CIS Tanium 7.x STIG Benchmark

v1.0.0 - 09-12-2025

Terms of Use

Please see the below link for our current terms of use:

https://www.cisecurity.org/cis-securesuite/cis-securesuite-membership-terms-of-use/

For information on referencing and/or citing CIS Benchmarks in 3rd party documentation (including using portions of Benchmark Recommendations) please contact CIS Legal (legalnotices@cisecurity.org) and request guidance on copyright usage.

NOTE: It is ***NEVER*** acceptable to host a CIS Benchmark in ***ANY*** format (PDF, etc.) on a 3rd party (non-CIS owned) site.

Table of Contents

Target Technology Details

Tanium 7.x Secure Technical Implementation Guide (STIG)

Version: 1 Release: 2 Benchmark

Date: 02 Sep 2022

Intended Audience

This benchmark is intended for system and application administrators, security specialists, auditors, help desk, and platform deployment personnel who plan to develop, deploy, assess, or secure solutions that incorporate Tanium 7.x and are looking to comply with the STIG guidance

Recommendation Definitions

The following defines the various components included in a CIS recommendation as applicable. If any of the components are not applicable it will be noted, or the component will not be included in the recommendation.

Title

Concise description for the recommendation's intended configuration.

Assessment Status

An assessment status is included for every recommendation. The assessment status indicates whether the given recommendation can be automated or requires manual steps to implement. Both statuses are equally important and are determined and supported as defined below:

Automated

Represents recommendations for which assessment of a technical control can be fully automated and validated to a pass/fail state. Recommendations will include the necessary information to implement automation.

Manual

Represents recommendations for which assessment of a technical control cannot be fully automated and requires all or some manual steps to validate that the configured state is set as expected. The expected state can vary depending on the environment.

Profile

A collection of recommendations for securing a technology or a supporting platform. Most benchmarks include at least a Level 1 and Level 2 Profile. Level 2 extends Level 1 recommendations and is not a standalone profile. The Profile Definitions section in the benchmark provides the definitions as they pertain to the recommendations included for the technology.

Description

The Rule Title from the STIG.

Rationale Statement

Detailed reasoning for the recommendation to provide the user a clear and concise understanding on the importance of the recommendation.

Audit Procedure

Systematic instructions for determining if the target system complies with the recommendation.

Remediation Procedure

Systematic instructions for applying recommendations to the target system to bring it into compliance according to the recommendation.

Additional Information

References from the STIG Rule if applicable.

Profile Definitions

The following configuration profiles are defined by this Benchmark:

- **SEVERITY: CAT I**

  Items in this profile exhibit one or more of the following characteristics:

  - are considered to be high severity
  - are intended for environments or use cases where following STIG based security guidance is paramount.
  - acts as defense in depth measure.
  - may negatively inhibit the utility or performance of the technology.

  This profile is intended for servers and workstations.

- **SEVERITY: CAT II**

  Items in this profile exhibit one or more of the following characteristics:

  - are considered to be medium severity
  - are intended for environments or use cases where following STIG based security guidance is paramount.
  - acts as defense in depth measure.
  - may negatively inhibit the utility or performance of the technology.

  This profile is intended for servers and workstations.

- **SEVERITY: CAT III**

  Items in this profile exhibit one or more of the following characteristics:

  - are considered to be low severity
  - are intended for environments or use cases where following STIG based security guidance is paramount.
  - acts as defense in depth measure.
  - may negatively inhibit the utility or performance of the technology.

  This profile is intended for servers and workstations.

Acknowledgements

This Benchmark exemplifies the great things a community of users, vendors, and subject matter experts can accomplish through consensus collaboration. The CIS community thanks the entire consensus team with special recognition to the following individuals who contributed greatly to the creation of this guide:

The Recommendations in this Benchmark are a representation of the Rules in the unclassified DISA STIG for Tanium 7.x

Contributor

Tim Harrison CISSP, ICP, KMP, Center for Internet Security, New York

Recommendations

1 STIG RULES

Tanium 7.x Operating System on TanOS

Tanium 7.x Secure Technical Implementation Guide (STIG)

Version: 1 Release: 2 Benchmark

Date: 02 Sep 2022

CLASSIFICATION unclassified

1.1 TANS-00-000155 (Manual)

Profile Applicability:

- SEVERITY: CAT II

Description:

The Tanium application must be configured to send audit records from multiple components within the system to a central location for review and analysis.

```
GROUP ID: V-253779
RULE ID: SV-253779r842365
```

Rationale:

Successful incident response and auditing relies on timely, accurate system information and analysis to allow the organization to identify and respond to potential incidents in a proficient manner. If the application does not provide the ability to centrally review the application logs, forensic analysis is negatively impacted.

Segregation of logging data to multiple disparate computer systems is counterproductive and makes log analysis and log event alarming difficult to implement and manage, particularly when the system or application has multiple logging components written to different locations or systems.

Automated mechanisms for centralized reviews and analyses include, for example, security information and event management (SIEM) products.

Audit:

1. Using a web browser on a system that has connectivity to the Tanium application, access the Tanium application web user interface (UI) and log on with multifactor authentication.
2. Click "Modules" on the top navigation banner.
3. Click "Connect".
4. Review the configured Connections under the "Connections" section.

If no Connection exists to send the "Tanium Audit Source" to a SIEM tool, this is a finding.

Remediation:

1. Using a web browser on a system that has connectivity to the Tanium application, access the Tanium application web UI and log on with multifactor authentication.
2. Click "Modules" on the top navigation banner.
3. Click "Connect".
4. Click "Create Connection".

5. In the "Configuration" section under "Source", select "Tanium Audit Source" as the source from the drop-down menu.
6. In the "Configuration" section under "Destination", select the desired Destination and fill in the respective fields.
7. In the "Configure Output" section under "Format", select the desired file format type.
8. In the "Schedule" section, select the desired schedule.
9. Click "Create Connection".

Additional Information:

CCI-000154

Provide the capability to centrally review and analyze audit records from multiple components within the system.

- NIST SP 800-53::AU-6 (4)
- NIST SP 800-53A::AU-6 (4).1
- NIST SP 800-53 Revision 4::AU-6 (4)
- NIST SP 800-53 Revision 5::AU-6 (4)

1.2 TANS-00-001025 (Manual)

Profile Applicability:

- SEVERITY: CAT II

Description:

The application must, at a minimum, offload interconnected systems in real time and offload standalone systems weekly.

```
GROUP ID: V-253780
RULE ID: SV-253780r850325
```

Rationale:

Information stored in one location is vulnerable to accidental or incidental deletion or alteration.

Offloading is a common process in information systems with limited audit storage capacity.

Audit:

1. Using a web browser on a system that has connectivity to the Tanium application, access the Tanium application web user interface (UI) and log on with multifactor authentication.
2. Click "Modules" on the top navigation banner.
3. Select "Connect".
4. Review the "Connections" sections for Source "Tanium Audit Source".

   If necessary, filter the connections by filtering by "Source" and the term "Audit".

5. Verify the "State" is "Enabled".

If no results are returned, this is a finding.

If results are returned but the state is not "Enabled", this is a finding.

Remediation:

1. Using a web browser on a system that has connectivity to the Tanium application, access the Tanium application web UI and log on with multifactor authentication.
2. Click "Modules" on the top navigation banner.
3. Select "Connect".
4. Click "Create Connection".
5. Enter "Name".
6. Enter "Description".

7. In the "Configuration" section, select Source: "Tanium Audit Source" and under "Basic" options, select appropriate audits.
8. In the "Destination" section, select a source from the drop-down menu.
9. Enter "Destination Name".
10. Enter "Host".
11. Select "Network Protocol": "TCP" or "UDP".
12. Enter "Port".
13. Select "Save".

Additional Information:

CCI-001851

Transfer audit logs per organization-defined frequency to a different system, system component, or media than the system or system component conducting the logging.

- NIST SP 800-53 Revision 4::AU-4 (1)
- NIST SP 800-53 Revision 5::AU-4 (1)

1.3 TANS-00-001055 (Manual)

Profile Applicability:

- SEVERITY: CAT II

Description:

Tanium Client processes must be excluded from On-Access scan.

```
GROUP ID: V-253781
RULE ID: SV-253781r842371
```

Rationale:

Similar to any other host-based applications, the Tanium Client is subject to the restrictions other system-level software may place on an operating environment. Antivirus, intrusion prevention system (IPS), encryption, or other security and management stack software may disallow the Client from working as expected.

For more information, refer to https://docs.tanium.com/platform_deployment_reference/platform_deployment_reference/security_exceptions.html?Highlight=exclusion.

Audit:

Review the settings of the antivirus software.

Verify exclusions exist that exclude the Tanium Client process interactions from On-Access scans and are treated as Low-Risk.

If exclusions do not exist, this is a finding.

Remediation:

Implement exclusion policies within the antivirus software to exclude the On-Access scanning of Tanium Client process interactions. These processes should be treated as Low-Risk and not scanned during read or write events.

Additional Information:

CCI-000366

Implement the security configuration settings.

- NIST SP 800-53::CM-6 b
- NIST SP 800-53A::CM-6.1 (iv)
- NIST SP 800-53 Revision 4::CM-6 b
- NIST SP 800-53 Revision 5::CM-6 b

1.4 TANS-00-001065 (Manual)

Profile Applicability:

- SEVERITY: CAT II

Description:

The Tanium application must be configured for LDAP user/group synchronization to map the authenticated identity to the individual user or group account for PKI-based authentication.

```
GROUP ID: V-253782
RULE ID: SV-253782r842374
```

Rationale:

Without mapping the certificate used to authenticate to the user account, the ability to determine the identity of the individual user or group will not be available for forensic analysis.

Audit:

Consult with the Tanium system administrator to review the documented list of Tanium users. The users' User Groups, Roles, Computer Groups, and correlated LDAP security groups must be documented.

If the documentation does not exist or is missing any Tanium users and their respective User Groups, Roles, Computer Groups, and correlated LDAP security groups, this is a finding.

Remediation:

1. Using a web browser on a system that has connectivity to the Tanium application, access the Tanium application web user interface (UI) and log on with multifactor authentication.
2. Click "Administration" on the top navigation banner.
3. Under "Permissions", select "Users".
4. Prepare and maintain documentation identifying the Tanium console users and their respective User Groups, Roles, Computer Groups, and associated LDAP security groups.

Additional Information:

CCI-000187

For public key-based authentication, map the authenticated identity to the account of the individual or group.

- NIST SP 800-53::IA-5 (2)

- NIST SP 800-53A::IA-5 (2).1
- NIST SP 800-53 Revision 4::IA-5 (2) (c)
- NIST SP 800-53 Revision 5::IA-5 (2) (a) (2)

1.5 TANS-00-001075 (Manual)

Profile Applicability:

- SEVERITY: CAT II

Description:

The Tanium application must uniquely identify and authenticate nonorganizational users (or processes acting on behalf of nonorganizational users).

```
GROUP ID: V-253783
RULE ID: SV-253783r842377
```

Rationale:

Lack of authentication and identification enables nonorganizational users to gain access to the application or possibly other information systems and provides an opportunity for intruders to compromise resources within the application or information system.

Nonorganizational users include all information system users other than organizational users, which includes organizational employees or individuals the organization deems to have equivalent status of employees (e.g., contractors and guest researchers).

Nonorganizational users must be uniquely identified and authenticated for all accesses other than those accesses explicitly identified and documented by the organization when related to the use of anonymous access, such as accessing a web server.

Audit:

1. Using a web browser on a system that has connectivity to the Tanium application, access the Tanium application web user interface (UI) and log on with multifactor authentication.
2. Click "Administration" on the top navigation banner.
3. Under "Permissions", select "Users".
4. Compare users listed to the prepared documentation.

If documentation identifying the Tanium console users and their respective User Groups, Roles, Computer Groups, and associated LDAP security groups does not exist, this is a finding.

Remediation:

Prepare and maintain documentation identifying the Tanium console users and their respective User Groups, Roles, Computer Groups, and associated LDAP security groups.

Additional Information:

CCI-000804

Uniquely identify and authenticate non-organizational users or processes acting on behalf of non-organizational users.

- NIST SP 800-53::IA-8
- NIST SP 800-53A::IA-8.1
- NIST SP 800-53 Revision 4::IA-8
- NIST SP 800-53 Revision 5::IA-8

1.6 TANS-00-001120 (Manual)

Profile Applicability:

- SEVERITY: CAT II

Description:

The Tanium application must separate user functionality (including user interface services) from information system management functionality.

```
GROUP ID: V-253784
RULE ID: SV-253784r842380
```

Rationale:

Application management functionality includes functions necessary for administration and requires privileged user access. Allowing nonprivileged users to access application management functionality capabilities increases the risk that nonprivileged users may obtain elevated privileges.

The separation of user functionality from information system management functionality is either physical or logical and is accomplished by using different computers, different central processing units, different instances of the operating system, different network addresses, different TCP/UDP ports, virtualization techniques, combinations of these methods, or other methods as appropriate.

An example of this type of separation is observed in web administrative interfaces that use separate authentication methods for users of any other information system resources. This may include isolating the administrative interface on a different security domain and with additional access controls.

Audit:

Consult with the Tanium system administrator to review the documented list of Tanium users. The users' User Groups, Roles, Computer Groups, and correlated LDAP security groups or Local Users must be documented.

Local users can be identified by the following:

1. Using a web browser on a system that has connectivity to the Tanium application, access the Tanium application web user interface (UI) and log on with multifactor authentication.
2. Click "Administration" on the top navigation banner.
3. Under "Permissions", select "Users".
4. Compare users that do not have a Domain listed to the prepared documentation.

If documentation identifying the Tanium console users and their respective User Groups, Roles, Computer Groups, and associated LDAP security groups does not exist, this is a finding.

Remediation:

Prepare and maintain documentation identifying the Tanium console users and their respective User Groups, Roles, Computer Groups, and associated LDAP security groups.

Additional Information:

CCI-001082

Separate user functionality, including user interface services, from system management functionality.

- NIST SP 800-53::SC-2
- NIST SP 800-53A::SC-2.1
- NIST SP 800-53 Revision 4::SC-2
- NIST SP 800-53 Revision 5::SC-2

1.7 TANS-00-001155 (Manual)

Profile Applicability:

- SEVERITY: CAT II

Description:

The Tanium Server and Client applications must have logging enabled.

```
GROUP ID: V-253785
RULE ID: SV-253785r842383
```

Rationale:

Failure to a known state can address safety or security in accordance with the mission/business needs of the organization. Failure to a known secure state helps prevent a loss of confidentiality, integrity, or availability in the event of a failure of the information system or a component of the system. Preserving application state information helps to facilitate application restart and return to the operational mode of the organization with less disruption to mission-essential processes.

Audit:

For Tanium Server:

1. Using a web browser on a system that has connectivity to the Tanium application, access the Tanium application web user interface (UI) and log on with multifactor authentication.
2. Click "Administration" on the top navigation banner.
3. Under "Configuration", select "Logging".
4. Select "Log Level".

If the value for the current level for "Tanium Server" and "Tanium Module Server" is not set to `1` or higher, this is a finding.

For Tanium Client:

1. Using a web browser on a system that has connectivity to the Tanium application, access the Tanium application web UI. Log on with multifactor authentication.
2. Click "Modules" on the top navigation banner.
3. Click "Interact".
4. In the "Explore Data" box, type the following question:

Get Tanium Client Explicit Setting`[LogVerbosityLevel] < 1` and Is Windows from all machines with Tanium Client Explicit Setting`[LogVerbosityLevel] < 1`

If any answers are returned that are `0`, this is a finding.

Remediation:

For Tanium Server:

1. Using a web browser on a system that has connectivity to the Tanium application, access the Tanium application web UI and log on with multifactor authentication.
2. Click "Administration" on the top navigation banner.
3. Under "Configuration", select "Logging".
4. In "Log Verbosity Level for Troubleshooting", set "Tanium Server" and "Tanium Module Server" to "1".

For Tanium Client:

1. Using a web browser on a system that has connectivity to the Tanium application, access the Tanium application web UI and log on with multifactor authentication.
2. Click "Modules" on the top navigation banner.
3. Click "Interact".
4. In the "Explore Data" box, type the following question:

   Get Tanium Client Explicit Setting`[LogVerbosityLevel] < 1` and Is Windows from all machines with Tanium Client Explicit Setting`[LogVerbosityLevel] < 1`

5. Select the row with "Is windows" set to "True" and deploy the following action and settings:

   a) Deployment Package: Modify Tanium Client Setting

   b) RegType: `REG_DWORD`

   c) ValueName: `LogVerbosityLevel`

   d) ValueData: `1` or higher

   Schedule Deployment

   a) Distribute over: 1 hour

6. Click "Show Preview to continue".
7. Click "Deploy Action".
8. Select the row with "Is windows" set to "False" and deploy the following action and settings:

   a) Deployment Package: Modify Tanium Client Setting [Non-Windows]

   b) RegType: `NUMERIC`

   c) ValueName: `LogVerbosityLevel`

d) ValueData: 1 or higher

Schedule Deployment

a) Distribute over: 1 hour

9. Click "Show Preview to continue".
10. Click "Deploy Action".

Additional Information:

CCI-001665

Preserve organization-defined system state information in the event of a system failure.

- NIST SP 800-53::SC-24
- NIST SP 800-53A::SC-24.1 (v)
- NIST SP 800-53 Revision 4::SC-24
- NIST SP 800-53 Revision 5::SC-2

1.8 TANS-00-001165 (Manual)

Profile Applicability:

- SEVERITY: CAT II

Description:

The Tanium application must restrict the ability of individuals to use information systems to launch organization-defined denial-of-service (DoS) attacks against other information systems.

```
GROUP ID: V-253786
RULE ID: SV-253786r842386
```

Rationale:

The Tanium Action Approval feature provides a two-person integrity control mechanism designed to achieve a high level of security and reduce the possibility of error for critical operations and DoS conditions.

When this feature is enabled, an action configured by one Tanium console user will require a second Tanium console user with a role of Action Approver (or higher) to approve the action before it is deployed to targeted computers.

Audit:

1. Using a web browser on a system that has connectivity to the Tanium application, access the Tanium application web user interface (UI) and log on with multifactor authentication.
2. Click "Administration" on the top navigation banner.
3. Under "Configuration", select "Platform Settings".
4. In the "Filter items" search box, type `require_action_approval`.
5. Click "Enter".

If no results are returned, this is a finding.

If results are returned for `require_action_approval`, but the value is not `1`, this is a finding.

Remediation:

1. Using a web browser on a system that has connectivity to the Tanium application, access the Tanium application web UI and log on with multifactor authentication.
2. Click "Administration" on the top navigation banner.
3. Under "Configuration", select "Platform Settings".
4. Click "Create Setting".
5. Select `Server` box for `Setting Type`.

6. In "Create Platform Setting" dialog box, enter `require_action_approval` does not exist: Flag for `Name`.
7. Select `Numeric` radio button for `Value Type`.
8. Enter `1` for `Value`.
9. Click "Save".

Additional Information:

CCI-001094

Restrict the ability of individuals to launch organization-defined denial of service attacks against other systems.

- NIST SP 800-53::SC-5 (1)
- NIST SP 800-53A::SC-5 (1).1
- NIST SP 800-53 Revision 4::SC-5 (1)
- NIST SP 800-53 Revision 5::SC-5 (1)

1.9 TANS-00-001170 (Manual)

Profile Applicability:

- SEVERITY: CAT II

Description:

The Tanium application must manage bandwidth throttles to limit the effects of information flooding types of denial-of-service (DoS) attacks.

```
GROUP ID: V-253787
RULE ID: SV-253787r842389
```

Rationale:

DoS is a condition when a resource is not available for legitimate users. When this occurs, the organization either cannot accomplish its mission or must operate at degraded capacity.

In the case of application DoS attacks, care must be taken when designing the application to ensure the application makes the best use of system resources. SQL queries have the potential to consume large amounts of CPU cycles if they are not tuned for optimal performance. Web services containing complex calculations requiring large amounts of time to complete can bog down if too many requests for the service are encountered within a short period of time.

The methods employed to meet this requirement will vary depending on the technology the application uses. However, a variety of technologies exist to limit or, in some cases, eliminate the effects of application-related DoS attacks. Employing increased capacity and bandwidth combined with specialized application layer protection devices and service redundancy may reduce the susceptibility to some DoS attacks.

Audit:

1. Using a web browser on a system that has connectivity to the Tanium application, access the Tanium application web user interface (UI) and log on with multifactor authentication.
2. Click "Administration" on the top navigation banner.
3. Under "Configuration", select "Bandwidth Throttles".
4. Work with the Tanium administrator to confirm settings.

For more information, refer to https://docs.tanium.com/platform_user/platform_user/console_bandwidth_throttling.html .

If the Bandwidth Throttles configuration is not accordance with organization's needs, this is a finding.

Remediation:

1. Using a web browser on a system that has connectivity to the Tanium Application, access the Tanium Application web user interface (UI) and log on with multifactor authentication.
2. Click "Administration" on the top navigation banner.
3. Under "Configuration", select "Bandwidth Throttles".
4. Click "Add" on the line for "Global Throttle for All Data".
5. Work with the Tanium administrator to configure the required bandwidth throttles.
6. Click "Save".
7. Work with the Tanium administrator to confirm or set the remaining options:
    - Global Throttle for Package Files.
    - Global Throttle for Sensors.
    - Site Throttles.

Additional Information:

CCI-001095

Manage capacity, bandwidth, or other redundancy to limit the effects of information flooding types of denial-of-service attacks.

- NIST SP 800-53::SC-5 (2)
- NIST SP 800-53A::SC-5 (2).1
- NIST SP 800-53 Revision 4::SC-5 (2)
- NIST SP 800-53 Revision 5::SC-5 (2)

1.10 TANS-00-001185 (Manual)

Profile Applicability:

- SEVERITY: CAT II

Description:

The Tanium application must generate error messages that provide information necessary for corrective actions without revealing information that could be exploited by adversaries.

```
GROUP ID: V-253788
RULE ID: SV-253788r842392
```

Rationale:

Any application providing too much information in error messages risks compromising the data and security of the application and system. The structure and content of error messages must be carefully considered by the organization and development team.

Organizations carefully consider the structure/content of error messages. The extent to which information systems are able to identify and handle error conditions is guided by organizational policy and operational requirements. Information that could be exploited by adversaries includes, for example, erroneous logon attempts with passwords entered by mistake as the username, mission/business information that can be derived from (if not stated explicitly by) information recorded, and personal information, such as account numbers, Social Security numbers, and credit card numbers.

Audit:

1. Access the Tanium Server.
2. Log on to the server with an account that has administrative privileges.
3. Open a File Explorer window.
4. Navigate to Program Files >> Tanium >> Tanium Server.
5. Right-click the "Logs" folder.
6. Select "Properties".
7. Select the "Security" tab.
8. Click the "Advanced" button.
    - Validate the owner of the directory is the [Tanium service account].
    - Validate the [Tanium service account] is the only account with modify permissions on the directory.
    - Validate the [Tanium Administrators] group has full permissions on the directory.
9. Right-click the `TDL_Logs` folder.
10. Select "Properties".
11. Select the "Security" tab.
12. Click the "Advanced" button.
    - Validate the owner of the directory is the [Tanium service account].

- Validate the [Tanium service account] is the only account with modify permissions on the directory.
- Validate the [Tanium Administrators] group has full permissions on the directory.

If any of the specified permissions are not set as required, this is a finding.

Remediation:

1. Access the Tanium Server.
2. Log on to the server with an account that has administrative privileges.
3. Open a File Explorer window.
4. Navigate to Program Files >> Tanium >> Tanium Server.
5. Right-click the "Logs" folder.
6. Select "Properties".
7. Select the "Security" tab.
8. Click the "Advanced" button.
9. Disable folder inheritance.
10. Change/verify the owner of the directory to the [Tanium service account].
11. Reduce [Tanium service account] privileges to modify permissions on the directory.
12. Ensure [Tanium Admins] group has full permissions on the directory.
13. Right-click the `TDL_Logs` folder.
14. Select "Properties".
15. Select the "Security" tab.
16. Click the "Advanced" button.
17. Disable folder inheritance.
18. Change/verify the owner of the directory to the [Tanium service account].
19. Reduce [Tanium service account] privileges to modify permissions on the directory.
20. Ensure [Tanium Admins] group has full permissions on the directory.

Additional Information:

CCI-001312

Generate error messages that provide information necessary for corrective actions without revealing information that could be exploited.

- NIST SP 800-53::SI-11 b
- NIST SP 800-53A::SI-11.1 (iii)
- NIST SP 800-53 Revision 4::SI-11 a
- NIST SP 800-53 Revision 5::SI-11 a

1.11 TANS-00-001190 (Manual)

Profile Applicability:

- SEVERITY: CAT II

Description:

The Tanium application must reveal error messages only to the information system security officer (ISSO), information system security manager (ISSM), and system administrator (SA).

```
GROUP ID: V-253789
RULE ID: SV-253789r842395
```

Rationale:

Only authorized personnel must be aware of errors and the details of the errors. Error messages are an indicator of an organization's operational state or can identify the application. Additionally, personally identifiable information (PII) and operational information must not be revealed through error messages to unauthorized personnel or their designated representatives.

The structure and content of error messages must be carefully considered by the organization and development team. The extent to which the information system is able to identify and handle error conditions is guided by organizational policy and operational requirements.

Audit:

1. Access the Tanium Server.
2. Log on to the server with an account that has administrative privileges.
3. Open a File Explorer window.
4. Navigate to Program Files >> Tanium >> Tanium Server.
5. Right-click the "Logs" folder.
6. Select "Properties".
7. Select the "Security" tab.
8. Click the "Advanced" button.
    - Validate the owner of the directory is the [Tanium service account].
    - Validate the [Tanium service account] is the only account with modify permissions on the directory.
    - Validate the [Tanium Administrators] group has full permissions on the directory.
9. Right-click the "TDL_Logs" folder.
10. Select "Properties".
11. Select the "Security" tab.
12. Click the "Advanced" button.
    - Validate the owner of the directory is the [Tanium service account].

- Validate the [Tanium service account] privileges is the only account with modify permissions on the directory.
- Validate the [Tanium Administrators] group has full permissions on the directory.

If any of the specified permissions are not set as required, this is a finding.

Remediation:

1. Access the Tanium Server.
2. Log on to the server with an account that has administrative privileges.
3. Open a File Explorer window.
4. Navigate to Program Files >> Tanium >> Tanium Server.
5. Right-click the "Logs" folder.
6. Select "Properties".
7. Select the "Security" tab.
8. Click the "Advanced" button.
9. Disable folder inheritance.
10. Change/verify the owner of the directory to the [Tanium service account].
11. Reduce [Tanium service account] privileges to modify permissions on the directory.
12. Ensure [Tanium Admins] group has full permissions on the directory.
13. Right-click the "TDL_Logs" folder.
14. Select "Properties".
15. Select the "Security" tab.
16. Click the "Advanced" button.
17. Disable folder inheritance.
18. Change/verify the owner of the directory to the [Tanium service account].
19. Reduce [Tanium service account] privileges to modify permissions on the directory.
20. Ensure [Tanium Admins] group has full permissions on the directory.

Additional Information:

CCI-001314

Reveal error messages only to organization-defined personnel or roles.

- NIST SP 800-53::SI-11 c
- NIST SP 800-53A::SI-11.1 (iv)
- NIST SP 800-53 Revision 4::SI-11 b
- NIST SP 800-53 Revision 5::SI-11 b

1.12 TANS-00-001195 (Manual)

Profile Applicability:

- SEVERITY: CAT II

Description:

The Tanium application must employ automated mechanisms to determine the state of information system components with regard to flaw remediation using the following frequency: continuously, where HBSS is used; 30 days, for any additional internal network scans not covered by HBSS; and annually, for external scans by Computer Network Defense Service Provider (CNDSP).

```
GROUP ID: V-253790
RULE ID: SV-253790r842661
```

Rationale:

Without the use of automated mechanisms to scan for security flaws on a continuous and/or periodic basis, the system components may remain vulnerable to the exploits presented by undetected software flaws.

To support this requirement, the flow remediation application may have automated mechanisms that perform automated scans for security-relevant software updates (e.g., patches, service packs, and hot fixes) and security vulnerabilities of the information system components being monitored. For example, a method of compliance would be an integrated solution incorporating continuous scanning using HBSS and periodic scanning using other tools as specified in the requirement.

Audit:

Note: If Tanium Patch is not licensed, another scanning solutions can be used.

1. Using a web browser on a system that has connectivity to the Tanium application, access the Tanium application web user interface (UI) and log on with multifactor authentication.
2. Click "Modules" at the top of the console.
3. Select "Patch".
4. On the left, expand the menu (three vertical dots).
5. Select "Scan Management".

If there is no "Scan Configurations" for all applicable operating systems, or if "Scan Configurations" are set with a Scan Frequency greater than 30 days, this is a finding.

Remediation:

Note: If Tanium Patch is not licensed, another scanning solutions can be used.

1. Using a web browser on a system that has connectivity to the Tanium application, access the Tanium application web UI and log on with multifactor authentication.
2. Click "Modules" on the top navigation banner.
3. Click "Patch".
4. Expand the left menu.
5. Select "Scan Management".
6. Work with the Tanium administrator to create Scan Configurations that run more often than 30 days.

Additional Information:

CCI-001233

The organization employs automated mechanisms on an organization-defined frequency to determine the state of information system components with regard to flaw remediation.

- NIST SP 800-53::SI-2 (2)
- NIST SP 800-53A::SI-2 (2).1 (ii)
- NIST SP 800-53 Revision 4::SI-2 (2)

1.13 TANS-00-001305 (Manual)

Profile Applicability:

- SEVERITY: CAT II

Description:

The Tanium application must allocate audit record storage capacity in accordance with organization-defined audit record storage requirements.

```
GROUP ID: V-253791
RULE ID: SV-253791r850192
```

Rationale:

To ensure applications have a sufficient storage capacity in which to write the audit logs, applications must be able to allocate audit record storage capacity.

The task of allocating audit record storage capacity is usually performed during initial installation of the application and is closely associated with the database administrator and system administrator roles. The database administrator or system administrator will usually coordinate the allocation of physical drive space with the application owner/installer, and the application will prompt the installer to provide the capacity information, the physical location of the disk, or both.

Audit:

Consult with the Tanium system administrator or database administrator to determine the volume on which the Tanium SQL databases are installed.

1. Using a web browser on a system that has connectivity to the Tanium application, access the Tanium application web user interface (UI) and log on with multifactor authentication.
2. Click "Modules" on the top navigation banner.
3. Select "Connect".
4. Review the configured Sources.

If none exist to send Disk Free Space of the Tanium SQL Server, this is a finding.

Work with the security information and event management (SIEM) administrator to determine if an alert is configured when Disk Free Space of the Tanium SQL Server reaches below 25%.

If no alert is configured, this is a finding.

Remediation:

Consult with the Tanium system administrator or database administrator to determine the volume on which the Tanium SQL databases are installed.

1. Using a web browser on a system that has connectivity to the Tanium application, access the Tanium application web UI and log on with multifactor authentication.
2. Click "Modules" in the top navigation banner.
3. Select "Interact".
4. Enter "Get Disk Free Space from all machines with Computer Name containing" [Your SQL Computer Name].
5. Press "Enter".
6. Select "Save this question" located under the Question box.
7. Enter a name (e.g., SQL Disk Free Space).
8. Select "Create Saved Question".
9. Click "Modules" in the top navigation banner.
10. Select "Connect".
11. Select "Create Connection".
12. In the "Configuration" section, select "Saved Question" from the Source drop-down menu.
13. Enter the "Saved Question Name" created above or select from the drop-down menu.
14. Select the "Computer Group" name from the drop-down menu.
15. Select the desired destination from the drop-down menu (must be a SIEM tool).
16. In the "General Information" section, provide a name and description.
17. Click "Save".

Work with the SIEM administrator to configure an alert when Disk Free Space of the Tanium SQL Server reaches below 25% of maximum.

Consult with the Tanium system administrator or database administrator to determine the volume on which the Tanium SQL databases are installed.

1. Using a web browser on a system that has connectivity to the Tanium Application, access the Tanium Application UI and log on with multifactor authentication.
2. Click "Modules" in the top navigation banner.
3. Select "Interact".
4. Enter "Get Disk Free Space from all machines with Computer Name containing" [Your SQL Computer Name].
5. Press "Enter".
6. Select "Save this question" located under the Question box.
7. Enter a name (e.g., SQL Disk Free Space).
8. Select "Create Saved Question".
9. Click "Modules" in the top navigation banner.
10. Select "Connect".
11. Select "Create Connection".
12. In the "Configuration" section, select "Saved Question" from the Source drop-down menu.
13. Enter the "Saved Question Name" created above or select from the drop-down menu.

14. Select the "Computer Group" name from the drop-down menu.
15. Select the desired destination from the drop-down menu (must be a SIEM tool).
16. In the "General Information" section, provide a name and description.
17. Click "Save".

Additional Information:

CCI-001849

Allocate audit log storage capacity to accommodate organization-defined audit log retention requirements.

- NIST SP 800-53 Revision 4::AU-4
- NIST SP 800-53 Revision 5::AU-4

1.14 TANS-00-001310 (Manual)

Profile Applicability:

- SEVERITY: CAT II

Description:

The Tanium application must offload audit records onto a different system or media than the system being audited.

```
GROUP ID: V-253792
RULE ID: SV-253792r850193
```

Rationale:

Information stored in one location is vulnerable to accidental or incidental deletion or alteration.

Offloading is a common process in information systems with limited audit storage capacity.

Audit:

1. Using a web browser on a system that has connectivity to the Tanium application, access the Tanium application web user interface (UI) and log in using multifactor authentication.
2. Click "Modules" on the top of the banner of the console.
3. Click "Connect".
4. Review the configured Connections under "Connections" section.

If no Connections exist to send the "Tanium Audit Source" to a security information and event management (SIEM) tool, this is a finding.

Remediation:

1. Using a web browser on a system that has connectivity to the Tanium application, access the Tanium application web UI and log in using multifactor authentication.
2. Click "Modules" on the top of the console.
3. Click "Connect".
4. Click "Create Connection".
5. In the "Configuration" section under "Source", select "Tanium Audit Source" as the source from the drop-down menu.
6. In the "Configuration" section under "Destination", select the desired Destination and fill in the respective fields.
7. In the "Configure Output" section under "Format", select the desired file format type.
8. In the "Schedule" section, select the desired schedule.

9. Click "Save".

Additional Information:

CCI-001851

Transfer audit logs per organization-defined frequency to a different system, system component, or media than the system or system component conducting the logging.

- NIST SP 800-53 Revision 4::AU-4 (1)
- NIST SP 800-53 Revision 5::AU-4 (1)

1.15 TANS-00-001315 (Manual)

Profile Applicability:

- SEVERITY: CAT II

Description:

The Tanium application must provide an immediate warning to the system administrator and information system security officer (at a minimum) when allocated audit record storage volume reaches 75% of repository maximum audit record storage capacity.

```
GROUP ID: V-253793
RULE ID: SV-253793r850194
```

Rationale:

If security personnel are not notified immediately upon storage volume utilization reaching 75%, they are unable to plan for storage capacity expansion.

Audit:

Consult with the Tanium system administrator or database administrator to determine the volume on which the Tanium SQL databases are installed.

1. Using a web browser on a system that has connectivity to the Tanium application, access the Tanium application web user interface (UI) and log on with multifactor authentication.
2. Click "Modules" on the top navigation banner.
3. Select "Connect".
4. Review the configured Connections under "Connections" section.

If none exist to send Disk Free Space of the Tanium SQL Server, this is a finding.

Work with the SIEM administrator to determine if an alert is configured when Disk Free Space of the Tanium SQL Server reaches below 25%.

If no alert is configured, this is a finding.

Remediation:

Consult with the Tanium system administrator or database administrator to determine the volume on which the Tanium SQL databases are installed.

1. Using a web browser on a system that has connectivity to the Tanium application, access the Tanium application web UI and log on with multifactor authentication.
2. Click "Modules" on the top navigation banner.
3. Select "Interact".

4. Enter "Get Disk Free Space from all machines with Computer Name containing" [Your SQL Computer Name].
5. Click "Enter".
6. Confirm question.
7. Select "Save" to the right of the Question Results.
8. Enter a name (e.g., SQL Disk Free Space).
9. Click "Save".
10. Click "Modules" on the top navigation banner.
11. Select "Connect".
12. Select "Create Connection".
13. In the Configuration section, select "Saved Question" from the Source drop-down menu.
14. Enter the "Saved Question Name" created above or select from the drop-down menu.
15. Select the "Computer Group" name from the drop-down menu.
16. Select the desired destination from the drop-down menu (must be a SIEM tool).
17. In the "General Information" section, provide a name and description.
18. Click "Save".

Work with the SIEM administrator to configure an alert when Disk Free Space of the Tanium SQL Server reaches below 25% of maximum.

Additional Information:

CCI-001855

Provide a warning to organization-defined personnel, roles, and/or locations within an organization-defined time period when allocated audit log storage volume reaches an organization-defined percentage of repository maximum audit log storage capacity.

- NIST SP 800-53 Revision 4::AU-5 (1)
- NIST SP 800-53 Revision 5::AU-5 (1)

1.16 TANS-00-001320 (Manual)

Profile Applicability:

- SEVERITY: CAT II

Description:

The Tanium application must provide an immediate real-time alert to the system administrator and information system security officer, at a minimum, of all audit failure events requiring real-time alerts.

```
GROUP ID: V-253794
RULE ID: SV-253794r850195
```

Rationale:

It is critical for the appropriate personnel to be aware if a system is at risk of failing to process audit logs as required. Without a real-time alert, security personnel may be unaware of an impending failure of the audit capability, and system operation may be adversely affected.

Alerts provide organizations with urgent messages. Real-time alerts provide these messages immediately (i.e., the time from event detection to alert occurs in seconds or less).

Audit:

1. Using a web browser on a system that has connectivity to the Tanium application, access the Tanium application web user interface (UI) and log on with multifactor authentication.
2. Click "Modules" on the top navigation banner.
3. Select "Connect".
4. Review the configured Tanium Sources listed.

   If an "Audit Log" source does not exist, this is a finding.

5. Select the "Audit Log" source.
6. Select the audit connection found in the lower half of the screen.
7. Verify the "Destination Type" is a security information and event management (SIEM) tool.

If the "Destination Type" is not a SIEM tool, this is a finding.

Remediation:

1. Using a web browser on a system that has connectivity to the Tanium application, access the Tanium application web UI and log on with multifactor authentication.

2. Click "Modules" on the top navigation banner.
3. Click "Connect".
4. Click "Create Connection".
5. In the Configuration section, select "Tanium Audit Source" as the "Event Source" from the "Source" drop-down menu.
6. In the "Destination" section, select "Socket Receiver" from the drop-down menu.
7. Enter "Destination Name".
8. Enter "Host".
9. Enter "Network Protocol".
10. Enter "Port".
11. Click "Save".

Consult documentation at https://docs.tanium.com/connect/connect/siem.html#siem for reference on configuring other applicable SIEM connections.

Work with the SIEM administrator to configure alerts based on audit failures.

Additional Information:

CCI-001858

Provide an alert in an organization-defined real-time-period to organization-defined personnel, roles, and/or locations when organization-defined audit failure events requiring real-time alerts occur.

- NIST SP 800-53 Revision 4::AU-5 (2)
- NIST SP 800-53 Revision 5::AU-5 (2)

1.17 TANS-00-001385 (Manual)

Profile Applicability:

- SEVERITY: CAT II

Description:

The Tanium application must prohibit user installation of software without explicit privileged status.

```
GROUP ID: V-253795
RULE ID: SV-253795r850213
```

Rationale:

Allowing regular users to install software, without explicit privileges, creates the risk that untested or potentially malicious software will be installed on the system. Explicit privileges (escalated or administrative privileges) provide the regular user with explicit capabilities and control that exceeds the rights of a regular user.

Application functionality will vary, and while users are not permitted to install unapproved applications, there may be instances where the organization allows the user to install approved software packages, such as from an approved software repository.

The application must enforce software installation by users based on what types of software installations are permitted (e.g., updates and security patches to existing software) and what types of installations are prohibited (e.g., software whose pedigree with regard to being potentially malicious is unknown or suspect) by the organization.

This requirement applies, for example, to applications that provide the ability to extend application functionality (e.g., plug-ins, add-ons) and software management applications.

Audit:

Consult with the Tanium system administrator to review the documented list of Tanium users.

1. Review the users' respective approved roles, as well as the correlated LDAP security group for the User Roles.
2. Validate LDAP security groups/Tanium roles are documented to assign least privileged access to the functions of the Tanium Server through the Tanium interface.

If the documentation does not reflect a granular, least-privileged-access approach to the LDAP Groups/Tanium Roles assignment, this is a finding.

Remediation:

1. Using a web browser on a system that has connectivity to the Tanium application, access the Tanium application web UI and log on with multifactor authentication.
2. Click "Administration" on the top navigation banner.
3. Under Permissions, select "Users".
4. Analyze the users configured in the Tanium interface.
5. Determine least privileged access required for each user to perform their respective duties.
6. Move users to the appropriate LDAP security group to ensure the user is synced to the appropriate Tanium User Role.
7. If the appropriate LDAP security groups are not already configured, create the groups and add the appropriate users.
8. Ensure LDAP sync repopulates the Tanium users' associated roles accordingly.

Additional Information:

CCI-001812

The information system prohibits user installation of software without explicit privileged status.

- NIST SP 800-53 Revision 4::CM-11 (2)

1.18 TANS-00-001395 (Manual)

Profile Applicability:

- SEVERITY: CAT II

Description:

The application must enforce access restrictions associated with changes to application configuration.

```
GROUP ID: V-253796
RULE ID: SV-253796r850215
```

Rationale:

Failure to provide logical access restrictions associated with changes to application configuration may have significant effects on the overall security of the system.

When dealing with access restrictions pertaining to change control, any changes to the hardware, software, and/or firmware components of the information system and/or application can have significant effects on the overall security of the system.

Accordingly, only qualified and authorized individuals should be allowed to obtain access to application components to initiate changes, including upgrades and modifications.

Logical access restrictions include, for example, controls that restrict access to workflow automation, media libraries, abstract layers (e.g., changes implemented into third-party interfaces rather than directly into information systems), and change windows (e.g., changes occur only during specified times, making unauthorized changes easy to discover).

Audit:

Consult with the Tanium system administrator to review the documented list of Tanium administrators.

Review the administrators' respective approved roles as the correlated LDAP security group for the User Roles.

If the documentation does not reflect a granular, least-privileged-access approach to the LDAP Groups/Tanium Roles assignment, this is a finding.

Remediation:

1. Using a web browser on a system that has connectivity to the Tanium application, access the Tanium application web user interface (UI) and log on with multifactor authentication.
2. Click "Administration" on the top navigation banner.
3. Under Permissions, select "Users".

4. Analyze the users configured in the Tanium interface.
5. Determine least privileged access required for each user to perform their respective duties.
6. Move users to the appropriate LDAP security group to ensure the user is synced to the appropriate Tanium User Role.
7. If the appropriate LDAP security groups are not already configured, create the groups and add the appropriate users.
8. Ensure LDAP sync repopulates the Tanium users' associated Roles accordingly.

Additional Information:

CCI-001813

Enforce access restrictions using organization-defined mechanisms.

- NIST SP 800-53 Revision 4::CM-5 (1)
- NIST SP 800-53 Revision 5::CM-5 (1) (a)

1.19 TANS-00-001405 (Manual)

Profile Applicability:

- SEVERITY: CAT II

Description:

The application must employ a deny-all, permit-by-exception (allowlist) policy to allow the execution of authorized software programs.

```
GROUP ID: V-253797
RULE ID: SV-253797r850221
```

Rationale:

Using an allowlist provides a configuration management method for allowing the execution of only authorized software. Using only authorized software decreases risk by limiting the number of potential vulnerabilities.

The organization must identify authorized software programs and permit execution of authorized software. The process used to identify software programs that are authorized to execute on organizational information systems is commonly referred to as allowlisting.

Verification of allowlisted software can occur either prior to execution or at system startup.

This requirement applies to configuration management applications or similar types of applications designed to manage system processes and configurations (e.g., HBSS and software wrappers).

Audit:

If Enforce is not used to manage allowlisting, this check is not applicable.

1. Using a web browser on a system that has connectivity to the Tanium application, access the Tanium application web user interface (UI) and log on with multifactor authentication.
2. Click "Modules" on the top navigation banner.
3. Select the "Enforce" module.
4. Click the three dots next to the "Enforce" header.
5. Click "Enforcements".
6. Verify an enforcement exists for allowlisting by looking for "AppLocker" in the "Policy" column.
7. Click each enforcement for allowlisting Policy type and verify the enforcement is applied to all applicable machines.

If an AppLocker Policy is not applied to all applicable machines, this is a finding.

Remediation:

If Enforce is not used to manage allowlisting, no fix is needed.

1. Using a web browser on a system that has connectivity to the Tanium application, access the Tanium application web UI and log on with multifactor authentication.
2. Click "Modules" on the top navigation banner.
3. Click "Enforce".
4. Expand the left menu.
5. From the Enforce menu, go to Policy Configurations.
6. Click "Action" and then "Create".
7. In the "General Information" section:
    - Enter a Name and Description for the policy.
    - Select AppLocker from the Policy Type options. Policy types can be filtered by operating system (All, Windows, Mac, Linux).
8. (Optional) If there is already a policy of this type, that policy can serve as the starting point for a new policy. Select the policy in the "Starting Point" pull-down menu.

    If requirements for this policy are missing, that information is displayed in the "Configuration Status" section. Refer to Configure Endpoint Encryption settings for BitLocker requirements.

9. In the "Settings" section:
    - Enter Support URL (optional).
    - Import Rules from XML (optional).
    - Select Rule Type (at least 1).
10. For each Rule Type:
    - Choose: Blocking.
    - Click "Create" under "Block" section.
11. Click "Create".

Additional Information:

CCI-001774

Employ a deny-all, permit-by-exception policy to allow the execution of authorized software programs on the system.

- NIST SP 800-53 Revision 4::CM-7 (5) (b)
- NIST SP 800-53 Revision 5::CM-7 (5) (b)

1.20 TANS-00-001420 (Manual)

Profile Applicability:

- SEVERITY: CAT II

Description:

The Tanium application must accept Personal Identity Verification (PIV) credentials.

```
GROUP ID: V-253798
RULE ID: SV-253798r850226
```

Rationale:

The use of PIV credentials facilitates standardization and reduces the risk of unauthorized access.

DoD has mandated the use of the CAC to support identity management and personal authentication for systems covered under HSPD 12 and as a primary component of layered protection for national security systems.

Audit:

1. Access the Tanium Server.
2. Log on to the server with an account that has administrative privileges.
3. Run regedit as Administrator.
4. Navigate to `HKEY_LOCAL_MACHINE >> SOFTWARE >> Wow6432Node >> Tanium >> Tanium Server`.
5. Validate the value for REG_DWORD `ForceSOAPSSLClientCert` is set to `1`.
6. Navigate to `HKEY_LOCAL_MACHINE >> SOFTWARE >> Wow6432Node >> Tanium >> Tanium Server`.
7. Validate the following keys exist and are configured:

```
REG_SZ "ClientCertificateAuthField"
For example:
X509v3 Subject Alternative Name.

REG_SZ "ClientCertificateAuthRegex"
For example-DoD:
.+?Name:\s*?(\S+@[._a-zA-Z0-9]+).*
Note: This regex may vary.

REG_SZ "ClientCertificateAuth"
For example:
C:\Program Files\Tanium\Tanium Server\dod.pem
```

If the value for `REG_DWORD ForceSOAPSSLClientCert` is not set to `1` and the remaining registry values are not configured, this is a finding.

Remediation:

1. Access the Tanium Server.
2. Log on to the server with an account that has administrative privileges.
3. Run regedit as Administrator.
4. Navigate to `HKEY_LOCAL_MACHINE >> SOFTWARE >> Wow6432Node >> Tanium >> Tanium Server`.
5. Validate the value for REG_DWORD `ForceSOAPSSLClientCert` is set to `1`.
6. Navigate to `HKEY_LOCAL_MACHINE >> SOFTWARE >> Wow6432Node >> Tanium >> Tanium Server`.
7. Configure the following keys:

```
REG_SZ "ClientCertificateAuthField"
For example:
X509v3 Subject Alternative Name.

REG_SZ "ClientCertificateAuthRegex"
For example-DoD:
.+?Name:\s*?(\S+@[._a-zA-Z0-9]+).*
Note: This regex may vary.

REG_SZ "ClientCertificateAuth"
For example:
C:\Program Files\Tanium\Tanium Server\dod.pem
```

Additional Information:

CCI-001953

Accept Personal Identity Verification-compliant credentials.

- NIST SP 800-53 Revision 4::IA-2 (12)
- NIST SP 800-53 Revision 5::IA-2 (12)

1.21 TANS-00-001425 (Manual)

Profile Applicability:

- SEVERITY: CAT II

Description:

The Tanium application must electronically verify Personal Identity Verification (PIV) credentials.

```
GROUP ID: V-253799
RULE ID: SV-253799r850227
```

Rationale:

The use of PIV credentials facilitates standardization and reduces the risk of unauthorized access.

DoD has mandated the use of the CAC to support identity management and personal authentication for systems covered under HSPD 12 and as a primary component of layered protection for national security systems.

Audit:

1. Access the Tanium Server.
2. Log on to the server with an account that has administrative privileges.
3. Run regedit as Administrator.
4. Navigate to `HKEY_LOCAL_MACHINE >> SOFTWARE >> Wow6432Node >> Tanium >> Tanium Server`.
5. Validate the value for `REG_DWORD ForceSOAPSSLClientCert` is set to `1`.
6. Navigate to `HKEY_LOCAL_MACHINE >> SOFTWARE >> Wow6432Node >> Tanium >> Tanium Server`.
7. Validate the following keys exist and are configured:

```
REG_SZ "ClientCertificateAuthField"
For example:
X509v3 Subject Alternative Name.

REG_SZ "ClientCertificateAuthRegex"
For example-DoD:
.+?Name:\s*?(\S+@[._a-zA-Z0-9]+).*
Note: This regex may vary and should be valid for any Subject Alternative Name
entry.

REG_SZ "ClientCertificateAuth"
For example:
C:\Program Files\Tanium\Tanium Server\dod.pem
```

If the value for `REG_DWORD ForceSOAPSSLClientCert` is not set to `1` and the remaining registry values are not configured, this is a finding.

Remediation:

1. Access the Tanium Server.
2. Log on to the server with an account that has administrative privileges.
3. Run regedit as Administrator.
4. Navigate to `HKEY_LOCAL_MACHINE >> SOFTWARE >> Wow6432Node >> Tanium >> Tanium Server`.
5. Validate the value for `REG_DWORD ForceSOAPSSLClientCert` is set to `1`.
6. Navigate to `HKEY_LOCAL_MACHINE >> SOFTWARE >> Wow6432Node >> Tanium >> Tanium Server`.
7. Configure the following keys:

```
REG_SZ "ClientCertificateAuthField"
For example:
X509v3 Subject Alternative Name.

REG_SZ "ClientCertificateAuthRegex"
For example-DoD:
.+?Name:\s*?(\S+@[._a-zA-Z0-9]+).*
Note: This regex may vary.

REG_SZ "ClientCertificateAuth"
For example:
C:\Program Files\Tanium\Tanium Server\dod.pem
```

Additional Information:

CCI-001954

Electronically verify Personal Identity Verification-compliant credentials.

- NIST SP 800-53 Revision 4::IA-2 (12)
- NIST SP 800-53 Revision 5::IA-2 (12)

1.22 TANS-00-001455 (Manual)

Profile Applicability:

- SEVERITY: CAT II

Description:

The Tanium application must accept Personal Identity Verification (PIV) credentials from other federal agencies.

```
GROUP ID: V-253800
RULE ID: SV-253800r850237
```

Rationale:

Access may be denied to authorized users if federal agency PIV credentials are not accepted.

PIV credentials are issued by federal agencies and conform to FIPS Publication 201 and supporting guidance documents. OMB Memorandum 11-11 requires federal agencies to continue implementing the requirements specified in HSPD-12 to enable agencywide use of PIV credentials.

Audit:

1. Access the Tanium Server.
2. Log on to the server with an account that has administrative privileges.
3. Run regedit as Administrator.
4. Navigate to `HKEY_LOCAL_MACHINE >> SOFTWARE >> Wow6432Node >> Tanium >> Tanium Server`.
5. Validate the value for `REG_DWORD ForceSOAPSSLClientCert` is set to `1`.
6. Navigate to `HKEY_LOCAL_MACHINE >> SOFTWARE >> Wow6432Node >> Tanium >> Tanium Server`.
7. Validate the following keys exist and are configured:

```
REG_SZ "ClientCertificateAuthField"
For example:
X509v3 Subject Alternative Name.

REG_SZ "ClientCertificateAuthRegex"
For example-DoD:
.+?Name:\s*?(\S+@[._a-zA-Z0-9]+).*
Note: This regex may vary.

REG_SZ "ClientCertificateAuth"
For example:
C:\Program Files\Tanium\Tanium Server\dod.pem
```

If the value for `REG_DWORD ForceSOAPSSLClientCert` is not set to `1` and the remaining registry values are not configured, this is a finding.

Remediation:

Use the vendor documentation titled "Smart card authentication" to implement correct configuration settings for this requirement.

Vendor documentation can be downloaded from the following URL:
https://docs.tanium.com/platform_deployment_reference/platform_deployment_reference/smart_card_authentication.html?Highlight=cac

1. Access the Tanium Server.
2. Log on to the server with an account that has administrative privileges.
3. Run regedit as Administrator.
4. Navigate to `HKEY_LOCAL_MACHINE >> SOFTWARE >> Wow6432Node >> Tanium >> Tanium Server`.
5. Validate the value for `REG_DWORD ForceSOAPSSLClientCert` is set to `1`.
6. Navigate to `HKEY_LOCAL_MACHINE >> SOFTWARE >> Wow6432Node >> Tanium >> Tanium Server`.
7. Configure the following keys:

```
REG_SZ "ClientCertificateAuthField"
For example:
X509v3 Subject Alternative Name.

REG_SZ "ClientCertificateAuthRegex"
For example-DoD:
.+?Name:\s*?(\S+@[._a-zA-Z0-9]+).*
Note: This regex may vary.

REG_SZ "ClientCertificateAuth"
For example:
C:\Program Files\Tanium\Tanium Server\dod.pem
```

Additional Information:

CCI-002009

Accept Personal Identity Verification-compliant credentials from other federal agencies.

- NIST SP 800-53 Revision 4::IA-8 (1)
- NIST SP 800-53 Revision 5::IA-8 (1)

1.23 TANS-00-001565 (Manual)

Profile Applicability:

- SEVERITY: CAT II

Description:

The Tanium application must install security-relevant software updates within the time period directed by an authoritative source (e.g., IAVM, CTOs, DTMs, and STIGs).

```
GROUP ID: V-253801
RULE ID: SV-253801r850286
```

Rationale:

Security flaws with software applications are discovered daily. Vendors are constantly updating and patching their products to address newly discovered security vulnerabilities. Organizations (including any contractor to the organization) are required to promptly install security-relevant software updates (e.g., patches, service packs, and hot fixes). Flaws discovered during security assessments, continuous monitoring, incident response activities, or information system error handling must also be addressed expeditiously.

Organization-defined time periods for updating security-relevant software may vary based on a variety of factors including, for example, the security category of the information system or the criticality of the update (i.e., severity of the vulnerability related to the discovered flaw).

This requirement will apply to software patch management solutions that are used to install patches across the enclave and also to applications that are not part of that patch management solution. For example, many browsers can install their own patch software. Patch criticality, as well as system criticality, will vary. Therefore, the tactical situations regarding the patch management process will also vary. This means the time period used must be a configurable parameter. Time frames for application of security-relevant software updates may depend on the Information Assurance Vulnerability Management (IAVM) process.

The application will be configured to check for and install security-relevant software updates within an identified time period from the availability of the update. The specific time period will be defined by an authoritative source (e.g., IAVM, CTOs, DTMs, and STIGs).

Audit:

Verify all components of the Tanium application have been updated within 60 days of vulnerability being announced by Tanium. Critical Vulnerabilities must be updated within 30 days.

Consult with the Tanium system administrator to review the documented time window designated for updates.

If a window of time is not defined or does not specify a reoccurring frequency, this is a finding.

1. Using a web browser on a system that has connectivity to the Tanium application, access the Tanium application web user interface (UI) and log on with multifactor authentication.
2. Click "Administration" on the top navigation banner.
3. Under "Configuration", select "Solutions".

If any module has the text "Update to" a newer (greater) version number compared to the installed version number in the Tanium Modules section of the page, this is a finding.

If the Tanium application is an "airgap" installation, work with the Tanium technical system administrator to determine if the modules are up to date.

Remediation:

Consult with the Tanium system administrator to review the documented time window designated for updates.

If a window of time is not defined or does not specify a reoccurring frequency, work with the Tanium administrator to document this.

1. Using a web browser on a system that has connectivity to the Tanium application, access the Tanium application web UI and log on with multifactor authentication.
2. Click "Administration" on the top navigation banner.
3. Under "Configuration", select "Solutions".

If any module has the text "Update to" a newer (greater) version number compared to the installed version number in the Tanium Modules section of the page, work with the Tanium administrator to update those modules or content.

If the Tanium application is an "airgap" installation, work with the Tanium technical system administrator to determine if the modules are up to date.

Additional Information:

CCI-002605

Install security-relevant software updates within an organization-defined time period of the release of the updates.

- NIST SP 800-53 Revision 4::SI-2 c
- NIST SP 800-53 Revision 5::SI-2 c

1.24 TANS-00-001600 (Manual)

Profile Applicability:

- SEVERITY: CAT II

Description:

Tanium must alert the ISSO, ISSM, and other individuals designated by the local organization when the following Indicators of Compromise (IOCs) or potential compromise are detected: real-time intrusion detection; threats identified by authoritative sources (e.g., CTOs); and Category I, II, IV, and VII incidents in accordance with CJCSM 6510.01B.

```
GROUP ID: V-253802
RULE ID: SV-253802r850301
```

Rationale:

When a security event occurs, the application that has detected the event must immediately notify the appropriate support personnel so they can respond appropriately.

Alerts may be generated from a variety of sources, including audit records or inputs from malicious code protection mechanisms, intrusion detection, or prevention mechanisms. Alerts may be transmitted, for example, telephonically, by electronic mail messages, or by text messaging. Individuals designated by the local organization to receive alerts may include, for example, system administrators, mission/business owners, or system owners.

IOCs are forensic artifacts from intrusions that are identified on organizational information systems (at the host or network level). IOCs provide organizations with valuable information on objects or information systems that have been compromised. These indicators reflect the occurrence of a compromise or a potential compromise.

This requirement applies to applications that provide monitoring capability for unusual/unauthorized activities including but are not limited to host-based intrusion detection, antivirus, and malware applications.

Audit:

Note: If THR is not licensed or used for detection, this is not applicable.

1. Using a web browser on a system that has connectivity to the Tanium application, access the Tanium application web user interface (UI) and log on with multifactor authentication.
2. Click "Modules" on the top navigation banner.
3. Click "Threat Response".
4. Expand the left menu.
5. Click "Alerts".
6. Filter on status "Unresolved".

If any alerts are unresolved, this is a finding.

Remediation:

1. Using a web browser on a system that has connectivity to the Tanium application, access the Tanium application web UI and log on with multifactor authentication.
2. Click "Modules" on the top navigation banner.
3. Click "Threat Response".
4. Expand the left menu.
5. Click "Alerts".
6. Filter on status "Unresolved".
7. Resolve any open IOC-based alerts and change status to applicable status.

Additional Information:

CCI-002664

Alert organization-defined personnel or roles when organization-defined compromise indicators generate the occurrence of a compromise or a potential compromise.

- NIST SP 800-53 Revision 4::SI-4 (5)
- NIST SP 800-53 Revision 5::SI-4 (5)

1.25 TANS-00-001750 (Manual)

Profile Applicability:

- SEVERITY: CAT II

Description:

Tanium Server processes must be excluded from On-Access scan.

```
GROUP ID: V-253803
RULE ID: SV-253803r842437
```

Rationale:

Similar to any other host-based applications, the Tanium Server is subject to the restrictions other system-level software may place on an operating environment. Antivirus, intrusion prevention system (IPS), encryption, or other security and management stack software may disallow the Tanium Server from working as expected.

For more information, refer to https://docs.tanium.com/platform_deployment_reference/platform_deployment_reference/security_exceptions.html?Highlight=exclusion.

Audit:

Review the settings of the antivirus software.

Validate exclusions exist that exclude the Tanium Server process interactions from On-Access scans and are treated as Low-Risk.

If exclusions do not exist, this is a finding.

Remediation:

Implement exclusion policies within the antivirus software solution to exclude the On-Access scanning of Tanium Server process interactions. These processes should be treated as Low-Risk and not scanned during read or write events.

Additional Information:

CCI-000366

Implement the security configuration settings.

- NIST SP 800-53::CM-6 b
- NIST SP 800-53A::CM-6.1 (iv)
- NIST SP 800-53 Revision 4::CM-6 b
- NIST SP 800-53 Revision 5::CM-6 b

1.26 TANS-00-001780 (Manual)

Profile Applicability:

- SEVERITY: CAT II

Description:

The Tanium application must authenticate endpoint devices (servers) before establishing a local, remote, and/or network connection using bidirectional authentication that is cryptographically based.

```
GROUP ID: V-253804
RULE ID: SV-253804r850330
```

Rationale:

Without authenticating devices, unidentified or unknown devices may be introduced, thereby facilitating malicious activity. Bidirectional authentication provides stronger safeguards to validate the identity of other devices for connections that are of greater risk, such as remote connections.

This requires device-to-device authentication. Information systems must use IEEE 802.1x, Extensible Authentication Protocol [EAP], Radius server with EAP-Transport Layer Security [TLS] authentication, or Kerberos to identify/authenticate devices on local and/or wide area networks.

Audit:

1. Using a web browser on a system that has connectivity to the Tanium application, access the Tanium application web user interface (UI) and log on with multifactor authentication.
2. Click "Administration" on the top navigation banner.
3. Under "Configuration", select "Platform Settings".
4. In the "Filter items" search box, type "TLSMode" and "ReportingTLSMode".
5. Click "Enter".

If results are returned and "TLSMode" = 0 and "ReportingTLSMode" = 0, this is a finding.

Remediation:

1. Using a web browser on a system that has connectivity to the Tanium application, access the Tanium application web UI and log on with multifactor authentication.
2. Click "Administration" on the top navigation banner.
3. Under "Configuration", select "Platform Settings".
4. In the "Filter items" search box, type "TLSMode" and "ReportingTLSMode".
5. Click "Enter".

6. Change the value for both "TLSMode" and "ReportingTLSMode" to "1".

Additional Information:

CCI-001967

Authenticate organization-defined devices and/or types of devices before establishing a local, remote, and/or network connection using bidirectional authentication that is cryptographically based.

- NIST SP 800-53 Revision 4::IA-3 (1)
- NIST SP 800-53 Revision 5::IA-3 (1)

1.27 TANS-CL-000001 (Manual)

Profile Applicability:

- SEVERITY: CAT II

Description:

The Tanium endpoint must have the Tanium Server's pki.db in its installation.

```
GROUP ID: V-253805
RULE ID: SV-253805r858416
```

Rationale:

Without cryptographic integrity protections in the Tanium Client, information could be altered by unauthorized users without detection.

Cryptographic mechanisms used for protecting the integrity of Tanium communications information include signed hash functions using asymmetric cryptography, enabling distribution of the public key to verify the hash information while maintaining the confidentiality of the secret key used to generate the hash.

Satisfies: SRG-APP-000158

Audit:

1. Using a web browser on a system that has connectivity to the Tanium application, access the Tanium application web user interface (UI) and log on with multifactor authentication.
2. Click "Administration" on the top navigation banner.
3. Under "Configuration", select "Client Status".
4. Change "Show systems that have reported in the last:"; enter 7 in the first field.
5. Select "Days" from the drop-down menu in the second field to determine if any endpoints connected with an invalid key.

If any systems are listed with "No" in the "Valid Key" column, this is a finding.

Remediation:

For systems that do not have a valid key for the Tanium Server, redeploy the client software from Tanium using Tanium Client Management or work with the Tanium system administrator to accomplish this.

1. Configure a deployment.
2. Deploy the package or installer.
3. Target appropriate systems.

Additional Information:

CCI-001453

Implement cryptographic mechanisms to protect the integrity of remote access sessions.

- NIST SP 800-53::AC-17 (2)
- NIST SP 800-53A::AC-17 (2).1
- NIST SP 800-53 Revision 4::AC-17 (2)
- NIST SP 800-53 Revision 5::AC-17 (2)

CCI-000778

Uniquely identify organization-defined devices and/or types of devices before establishing a local, remote, and/or network connection.

- NIST SP 800-53::IA-3
- NIST SP 800-53A::IA-3.1 (ii)
- NIST SP 800-53 Revision 4::IA-3
- NIST SP 800-53 Revision 5::IA-3

1.28 TANS-CL-000002 (Manual)

Profile Applicability:

- SEVERITY: CAT II

Description:

Access to Tanium logs on each endpoint must be restricted by permissions.

```
GROUP ID: V-253806
RULE ID: SV-253806r842446
```

Rationale:

For the Tanium Client software to run without impact from external negligent or malicious changes, the permissions on the Tanium log files and their directory must be restricted.

Tanium is deployed with a Client Hardening Solution. This solution, when applied, will ensure directory permissions are in place.

Audit:

1. Using a web browser on a system that has connectivity to the Tanium application, access the Tanium application web user interface (UI) and log on with multifactor authentication.
2. Click "Administration" on the top navigation banner.
3. Under "Actions", select "Scheduled Actions".
4. Look for a scheduled action titled "Client Service Hardening - Set SYSTEM only permissions on Tanium Client directory".

If a scheduled action titled "Client Service Hardening - Set SYSTEM only permissions on Tanium Client directory" does not exist, or there is a Scheduled Action contradicting the "Client Service Hardening - Set SYSTEM only permissions on Tanium Client directory" scheduled action, this is a finding.

If the scheduled action exists, select it. If it is not approved (the "Approve" button at the top of the section will be displayed if not approved), this is a finding.

Remediation:

1. Using a web browser on a system that has connectivity to the Tanium application, access the Tanium application web UI and log on with multifactor authentication.
2. Click "Modules" on the top navigation banner.
3. Click "Interact".
4. Within "Interact", under "Explore Data", ask the question "Get Tanium Client Directory Permissions from all machines".

Tanium will parse the script and return a row for "Restricted" and a row for "Not Restricted", with their respective client counts.

5. Click the "Not Restricted" row.
6. Select "Deploy Action".
    - In the "Deploy Action" dialog box, the package "Client Service Hardening - Set SYSTEM only permissions on Tanium Client directory" will be selected.
    - The clients, which have their Tanium Client directory "Not Restricted", will be displayed in the bottom window.
7. Choose a schedule to deploy the hardening.
8. Under "Targeting Criteria", in the "Action Group", select "All Computers" from the drop-down menu.
9. Click "Deploy Action".
10. Verify settings.
11. Click "Show Client Status Details".

Additional Information:

CCI-000163

Protect audit information from unauthorized modification.

- NIST SP 800-53::AU-9
- NIST SP 800-53A::AU-9.1
- NIST SP 800-53 Revision 4::AU-9
- NIST SP 800-53 Revision 5::AU-9 a

1.29 TANS-CL-000003 (Manual)

Profile Applicability:

- SEVERITY: CAT II

Description:

The Tanium cryptographic signing capabilities must be enabled on the Tanium Clients to safeguard the authenticity of communications sessions when answering requests from the Tanium Server.

```
GROUP ID: V-253807
RULE ID: SV-253807r858417
```

Rationale:

All of Tanium's signing capabilities should be enabled upon install. Tanium supports the cryptographic signing and verification before execution of all Sensors, Questions, Actions, Sensor Libraries, File Shards, etc.

Enabling signing removes the ability of an attacker to conduct man-in-the-middle (MitM) attacks for remote code execution and precludes the modification of the aforementioned data elements in transit. Additionally, Tanium supports object-level signing for content ingested into the Tanium platform. This allows for the detection and rejection of changes to objects (sensors, actions, etc.) by even a privileged user within Tanium.

Tanium has built-in signing capabilities enabled by default when installed. Cryptographic signing and verification of all Sensors, Questions, Actions, Sensor Libraries, File Shards, etc., before execution will be enforced by Tanium.

Signing will prevent MitM remote code execution attacks and will protect data element in transit. Tanium also supports object-level signing for content within the Tanium platform.

Satisfies: SRG-APP-000219

Audit:

1. Using a web browser on a system that has connectivity to the Tanium application, access the Tanium application web user interface (UI) and log on with multifactor authentication.
2. Click "Administration" on the top navigation banner.
3. Under "Configuration", select "Platform Settings".
4. In the "Filter Items" search box, type `AllQuestionsRequireSignatureFlag`.
5. Click "Enter".

If no results are returned, this is a finding.

If results are returned for "AllQuestionsRequireSignatureFlag" but the value is not "1", this is a finding.

Remediation:

1. Using a web browser on a system that has connectivity to the Tanium application, access the Tanium application web UI and log on with multifactor authentication.
2. Click "Administration" on the top navigation banner.
3. Under "Configuration", select "Platform Settings".
4. Click "Create Setting".
5. Select "Client" box for "Setting Type".
6. In "Create Platform Setting" dialog box, enter `AllQuestionsRequireSignatureFlag` for `Name`.
7. Select `Numeric` radio button for `Value Type`.
8. Enter `1` for `Value`.
9. Click "Save".

Additional Information:

CCI-001749

The information system prevents the installation of organization-defined software components without verification the software component has been digitally signed using a certificate that is recognized and approved by the organization.

- NIST SP 800-53 Revision 4::CM-5 (3)

CCI-001184

Protect the authenticity of communications sessions.

- NIST SP 800-53::SC-23
- NIST SP 800-53A::SC-23.1
- NIST SP 800-53 Revision 4::SC-23
- NIST SP 800-53 Revision 5::SC-23

1.30 TANS-CL-000004 (Manual)

Profile Applicability:

- SEVERITY: CAT II

Description:

Firewall rules must be configured on the Tanium endpoints for client-to-server communications.

```
GROUP ID: V-253808
RULE ID: SV-253808r842452
```

Rationale:

In addition to the client-to-server TCP communication that takes place over port 17472, Tanium Clients also communicate to other Tanium-managed computers over port 17472. Without proper firewall configurations, proper TCP communications may not take place as necessary for application functionality.

The Tanium environment can perform hundreds or thousands of times faster than other security or systems management tools because the Tanium Clients communicate in secure, linearly controlled peer-to-peer rings. Because clients dynamically communicate with other nearby agents based on proximity and latency, rings tend to form automatically to match a customer's topology. For example, endpoints in California will form one ring while endpoints in Germany will form a separate ring.

Audit:

Note: This check is performed for the Tanium endpoints and must be validated against the enterprise firewall solution (e.g., Endpoint Security Solution Firewall, Microsoft Windows Defender Firewall setting, Microsoft Advance Threat Protection Firewall, etc.) policies applied to the endpoints.

1. Consult with the personnel who maintain the Enterprise Security Suite configuration for assistance.
2. Validate a rule exists within the firewall policies for managed clients for the following:

   Port Needed: Tanium Clients or Zone Clients over TCP port 17472, bidirectionally.

   If a host-based firewall rule does not exist to allow TCP port 17472, bidirectionally, this is a finding.

3. Consult with the boundary network firewall administrator and validate rules exist for the following:

Allow TCP traffic on port 17472 from any computer to be managed on a local area network to any other computer to be managed on the same local area network.

If a network firewall rule does not exist to allow TCP port 17472 from any managed computer to any other managed computer on the same local area network, this is a finding.

Remediation:

1. Consult with the personnel who maintain the Enterprise Security Suite to configure host-based and network firewall rules to allow the following:

   Tanium Clients or Zone Clients over TCP port 17472, bidirectionally.

2. Consult with the boundary network firewall administrator to create a rule to allow the following:

TCP traffic on port 17472 from any computer to be managed on a local area network to any other computer to be managed on the same local area network.

Additional Information:

CCI-000382

Configure the system to prohibit or restrict the use of organization-defined prohibited or restricted functions, system ports, protocols, software, and/or services.

- NIST SP 800-53::CM-7
- NIST SP 800-53A::CM-7.1 (iii)
- NIST SP 800-53 Revision 4::CM-7 b
- NIST SP 800-53 Revision 5::CM-7 b

1.31 TANS-CL-000005 (Manual)

Profile Applicability:

- SEVERITY: CAT II

Description:

Control of the Tanium Client service must be restricted to SYSTEM access only for all managed clients.

```
GROUP ID: V-253809
RULE ID: SV-253809r850167
```

Rationale:

The reliability of the Tanium client's ability to operate depends on controlling access to the Tanium client service. By restricting access to SYSTEM access only, the non-Tanium system administrator will not have the ability to impact operability of the service.

Audit:

1. Using a web browser on a system that has connectivity to the Tanium application, access the Tanium application web user interface (UI) and log on with multifactor authentication.
2. Click "Administration" on the top navigation banner.
3. Under "Actions", select "Scheduled Actions".
4. Look for a scheduled action titled "Client Service Hardening - Allow Only Local SYSTEM to Control Service".

   If a scheduled action titled "Client Service Hardening - Allow Only Local SYSTEM to Control Service" does not exist, this is a finding.

5. If the scheduled action exists, select it. If it is not approved (the "Approve" button at the top of the section will be displayed if not approved), this is a finding.

If the scheduled action exists and has been approved but does not restrict control of the Tanium Client service to Allow Only Local SYSTEM to Control Service, this is a finding.

If the action is not configured to repeat at least every 12 hours, this is a finding.

If the scheduled action is not targeted at an "All Computers" Action Group, this is a finding.

Remediation:

1. Using a web browser on a system that has connectivity to the Tanium application, access the Tanium application web UI and log on with multifactor authentication.

2. Click "Modules" on the top navigation banner.
3. Click "Interact".
4. In "Categories" section, select box for "Client Service Hardening".
5. In "Dashboards" section, select "Control Service State Permissions".
6. The results will show a "Count" of clients matching the "Service Control is set to default permissions" query.
7. Select the result line for "Service Control is set to default permissions".
8. Choose "Deploy Action".
9. In the Deployment Package drop-down, select "Client Service Hardening - Allow Only Local SYSTEM to Control Service".
10. Configure the schedule to repeat at least every 12 hours for the requested action.
11. Under "Targeting Criteria", in the Action Group, select "All Computers" from the drop-down menu.
12. Click "Show preview to continue".
13. Noncompliant systems will be displayed at the bottom.
14. Click "Deploy Action".
15. Verify settings.
16. Click "Show Client Status Details".

Additional Information:

CCI-002165

Enforce organization-defined discretionary access control policies over defined subjects and objects.

- NIST SP 800-53 Revision 4::AC-3 (4)
- NIST SP 800-53 Revision 5::AC-3 (4)

1.32 TANS-CL-000006 (Manual)

Profile Applicability:

- SEVERITY: CAT II

Description:

The ability to uninstall the Tanium Client service must be disabled on all managed clients.

```
GROUP ID: V-253810
RULE ID: SV-253810r850167
```

Rationale:

By default, end users have the ability to uninstall software on their clients. In the event the Tanium Client software is uninstalled, the Tanium Server is unable to manage the client and must redeploy to the client. Preventing the software from being displayed in the client's Add/Remove Programs will lessen the risk of the software being uninstalled by non-Tanium system administrators.

Audit:

1. Using a web browser on a system that has connectivity to the Tanium application, access the Tanium application web user interface (UI) and log on with multifactor authentication.
2. Click "Administration" on the top navigation banner.
3. Under "Actions", select "Scheduled Actions".
4. Look for a scheduled action titled "Client Service Hardening - Hide Client from Add-Remove Programs".
5. If a scheduled action titled "Client Service Hardening - Hide Client from Add-Remove Programs" does not exist, this is a finding.

If the scheduled action exists, select it. If it is not approved (the "Approve" button at the top of the section will be displayed if not approved), this is a finding.

If the scheduled action exists and has been approved but does not disable the visibility of the client in Add-Remove Programs, this is a finding.

If the action is not configured to repeat at least every 12 hours, this is a finding.

If the scheduled action is not targeted at an "All Computers" Action Group, this is a finding.

Remediation:

1. Using a web browser on a system that has connectivity to the Tanium application, access the Tanium application web UI and log on with multifactor authentication.

2. Click "Modules" on the top navigation banner.
3. Click "Interact".
4. In "Categories" section, select box for "Client Service Hardening".
5. In "Dashboard" section, select "Hide From Add-Remove Program".
6. The results will show a "Count" of clients matching the "Tanium Client Visible in Add-Remove Programs" query.
7. Select the result line.
8. Choose "Deploy Action".
9. The "Deploy Action" dialog box will display "Client Service Hardening - Hide Client from Add-Remove Programs" as the package. The computer names comprising the "Count" of noncompliant systems will be displayed in the bottom.
10. From the Deployment Package drop-down, select "Client Service Hardening - Hide Client from Add-Remove Programs".
11. Configure the schedule to repeat at least every 12 hours for the requested action.
12. Under "Targeting Criteria", in the Action Group, select "All Computers" from the drop-down menu.
13. Click "Show preview to continue". Noncompliant systems will be displayed in the bottom.
14. Click "Deploy Action".
15. Verify settings.
16. Click "Show Client Status Details".

Additional Information:

CCI-002165

Enforce organization-defined discretionary access control policies over defined subjects and objects.

- NIST SP 800-53 Revision 4::AC-3 (4)
- NIST SP 800-53 Revision 5::AC-3 (4)

1.33 TANS-CL-000007 (Manual)

Profile Applicability:

- SEVERITY: CAT II

Description:

The permissions on the Tanium Client directory must be restricted to only the SYSTEM account on all managed clients.

```
GROUP ID: V-253811
RULE ID: SV-253811r850167
```

Rationale:

By restricting access to the Tanium Client directory on managed clients, the Tanium client's ability to operate and function as designed will be protected from malicious attack and unintentional modifications by end users.

Audit:

1. Using a web browser on a system that has connectivity to the Tanium application, access the Tanium application web user interface (UI) and log on with multifactor authentication.
2. Click "Administration" on the top navigation banner.
3. Under "Actions", select "Scheduled Actions".
4. Look for a scheduled action titled "Client Service Hardening - Set SYSTEM only permissions on the Tanium Client directory".

If a scheduled action titled "Client Service Hardening - Set SYSTEM only permissions on the Tanium Client directory" does not exist, this is a finding.

If the scheduled action exists, select it. If it is not approved (the "Approve" button at the top of the section will be displayed if not approved), this is a finding.

If the scheduled action exists and has been approved but does not disable the visibility of the client in Add-Remove Programs, this is a finding.

If the action is not configured to repeat at least every 12 hours, this is a finding.

If the scheduled action is not targeted at an "All Computers" Action Group, this is a finding.

Remediation:

1. Using a web browser on a system that has connectivity to the Tanium application, access the Tanium application web UI and log on with multifactor authentication.
2. Click "Modules" on the top navigation banner.

3. Click "Interact".
4. In "Categories" section, select box for "Client Service Hardening".
5. In "Dashboard" section, select "Set Client Directory Permissions".
    - The results will show a "Count" of clients' compliant and noncompliant hardening for the "Tanium Client Directory Permissions".
    - Noncompliant clients will have a count other than "0" for "Not Restricted" or "Error: No Permissions".
6. Select each of the "Not Restricted" or "Error: No Permissions" statuses.
7. Select "Deploy Action".
8. In the "Deploy Action" dialog box, change the package to "Client Service Hardening - Set SYSTEM only permissions on the Tanium Client directory" as the package.
9. Configure the schedule to repeat at least every 12 hours for the requested action.
10. Under "Targeting Criteria", in the Action Group, select "All Computers" from the drop-down menu.
11. Click "Show preview to continue". Noncompliant systems will be displayed in the bottom.
12. Click "Deploy Action".
13. Verify settings.
14. Click "Show Client Status Details".

Additional Information:

CCI-002165

Enforce organization-defined discretionary access control policies over defined subjects and objects.

- NIST SP 800-53 Revision 4::AC-3 (4)
- NIST SP 800-53 Revision 5::AC-3 (4)

1.34 TANS-CL-000008 (Manual)

Profile Applicability:

- SEVERITY: CAT II

Description:

Tanium Client directory and subsequent files must be excluded from On-Access scan.

```
GROUP ID: V-253812
RULE ID: SV-253812r842464
```

Rationale:

Similar to any other host-based applications, the Tanium Client is subject to the restrictions other system-level software may place on an operating environment. Antivirus, intrusion prevention system (IPS), encryption, or other security and management stack software may disallow the Client from working as expected.

For more information, refer to https://docs.tanium.com/platform_deployment_reference/platform_deployment_reference/security_exceptions.html?Highlight=exclusion.

Audit:

Review the settings of the antivirus software.

Validate exclusions exist that exclude the Tanium Client directory and subsequent file interactions from On-Access scans.

If exclusions do not exist, this is a finding.

Remediation:

Implement exclusion policies within the antivirus software solution to exclude the On-Access scanning of Tanium Client directory and subsequent file interactions.

Additional Information:

CCI-000366

Implement the security configuration settings.

- NIST SP 800-53::CM-6 b
- NIST SP 800-53A::CM-6.1 (iv)
- NIST SP 800-53 Revision 4::CM-6 b
- NIST SP 800-53 Revision 5::CM-6 b

1.35 TANS-CL-000014 (Manual)

Profile Applicability:

- SEVERITY: CAT II

Description:

Tanium endpoint files must be excluded from host-based intrusion prevention system (HIPS) intervention.

```
GROUP ID: V-253813
RULE ID: SV-253813r842467
```

Rationale:

Similar to any other host-based applications, the Tanium Client is subject to the restrictions other system-level software may place on an operating environment. Antivirus, intrusion prevention system (IPS), encryption, or other security and management stack software may disallow the Tanium Server from working as expected.

For more information, refer to https://docs.tanium.com/platform_deployment_reference/platform_deployment_reference/security_exceptions.html?Highlight=exclusion.

Audit:

Consult with the Tanium system administrator to determine the HIPS software used on the Tanium Clients.

Review the settings of the HIPS software.

Validate exclusions exist that exclude the Tanium program files from being restricted by HIPS.

If exclusions do not exist, this is a finding.

Remediation:

Implement exclusion policies within the HIPS software solution to exclude the Tanium client program files from HIPS intervention.

Additional Information:

CCI-000366

Implement the security configuration settings.

- NIST SP 800-53::CM-6 b
- NIST SP 800-53A::CM-6.1 (iv)
- NIST SP 800-53 Revision 4::CM-6 b
- NIST SP 800-53 Revision 5::CM-6 b

1.36 TANS-CN-000001 (Manual)

Profile Applicability:

- SEVERITY: CAT II

Description:

The Tanium application must retain the session lock until the user reestablishes access using established identification and authentication procedures.

```
GROUP ID: V-253814
RULE ID: SV-253814r842470
```

Rationale:

Unattended systems are susceptible to unauthorized use and should be locked when unattended. This protects critical and sensitive data from exposure to unauthorized personnel with physical access to the system.

Audit:

1. Access the Tanium Server.
2. Log on to the server with an account that has administrative privileges.
3. Run regedit as Administrator.
4. Navigate to `HKEY_LOCAL_MACHINE >> SOFTWARE >> Wow6432Node >> Tanium >> Tanium Server`.
5. Validate the value for `REG_DWORD ForceSOAPSSLClientCert` is set to `1`.
6. Navigate to `HKEY_LOCAL_MACHINE >> SOFTWARE >> Wow6432Node >> Tanium >> Tanium Server`.
7. Validate the following keys exist and are configured:

```
REG_SZ "ClientCertificateAuthField"
For example:
X509v3 Subject Alternative Name.

REG_SZ "ClientCertificateAuthRegex"
For example-DoD:
.+?Name:\s*?(\S+@[._a-zA-Z0-9]+).*
Note: This regex may vary.

REG_SZ "ClientCertificateAuth"
For example:
C:\Program Files\Tanium\Tanium Server\dod.pem
```

If the value for `REG_DWORD ForceSOAPSSLClientCert` is not set to `1` and the remaining registry values are not configured, this is a finding.

Remediation:

Use the vendor documentation titled "Smart card authentication" to implement correct configuration settings for this requirement.

Vendor documentation can be downloaded from https://docs.tanium.com/platform_deployment_reference/platform_deployment_reference/smart_card_authentication.html?Highlight=cac.

1. Access the Tanium Server.
2. Log on to the server with an account that has administrative privileges.
3. Run regedit as Administrator.
4. Navigate to `HKEY_LOCAL_MACHINE >> SOFTWARE >> Wow6432Node >> Tanium >> Tanium Server`.
5. Validate the value for `REG_DWORD ForceSOAPSSLClientCert` is set to `1`.
6. Navigate to `HKEY_LOCAL_MACHINE >> SOFTWARE >> Wow6432Node >> Tanium >> Tanium Server`.
7. Configure the following keys:

```
REG_SZ "ClientCertificateAuthField"
For example:
X509v3 Subject Alternative Name.

REG_SZ "ClientCertificateAuthRegex"
For example-DoD:
.+?Name:\s*?(\S+@[._a-zA-Z0-9]+).*
Note: This regex may vary.

REG_SZ "ClientCertificateAuth"
For example:
C:\Program Files\Tanium\Tanium Server\dod.pem
```

Additional Information:

CCI-000060

Conceal, via the device lock, information previously visible on the display with a publicly viewable image.

- NIST SP 800-53::AC-11 (1)
- NIST SP 800-53A::AC-11 (1).1
- NIST SP 800-53 Revision 4::AC-11 (1)
- NIST SP 800-53 Revision 5::AC-11 (1)

1.37 TANS-CN-000002 (Manual)

Profile Applicability:

- SEVERITY: CAT II

Description:

The Tanium Application Server must be configured with a connector to sync to Microsoft Active Directory for account management functions.

```
GROUP ID: V-253815
RULE ID: SV-253815r858409
```

Rationale:

By restricting access to the Tanium Server to only Microsoft Active Directory, user accounts and related permissions can be strictly monitored. Account management will be under the operational responsibility of the system administrator for the Windows Operating System Active Directory.

Satisfies: SRG-APP-000317

Audit:

1. Using a web browser on a system that has connectivity to the Tanium application, access the Tanium application web user interface (UI) and log on with multifactor authentication.
2. Click "Administration" on the top navigation banner.
3. Under "Configuration", select "LDAP/AD Sync Configurations".
4. Verify a sync exists under "Enabled Servers".

If no sync exists, this is a finding.

If sync exists under "Disabled Servers" and there are no Enabled Servers, this is a finding.

Remediation:

1. Using a web browser on a system that has connectivity to the Tanium application, access the Tanium application web UI and log on with multifactor authentication.
2. Click "Administration" on the top navigation banner.
3. Under "Configuration", select "LDAP/AD Sync Configurations".
4. Click "Add Server".
5. Complete the settings using guidance from https://docs.tanium.com/platform_user/platform_user/console_using_ldap.html.
6. Click "Show Preview to Continue".
7. Review the users and groups to be imported.

8. Click "Save".

Additional Information:

CCI-001084

Isolate security functions from nonsecurity functions.

- NIST SP 800-53::SC-3
- NIST SP 800-53A::SC-3.1 (ii)
- NIST SP 800-53 Revision 4::SC-3
- NIST SP 800-53 Revision 5::SC-3

CCI-002142

The information system terminates shared/group account credentials when members leave the group.

- NIST SP 800-53 Revision 4::AC-2 (10)

1.38 TANS-CN-000003 (Manual)

Profile Applicability:

- SEVERITY: CAT II

Description:

The Tanium Application Server must be configured to only use LDAP for account management functions.

```
GROUP ID: V-253816
RULE ID: SV-253816r842476
```

Rationale:

Enterprise environments make application account management challenging and complex. A manual process for account management functions adds the risk of a potential oversight or other error.

To reduce risk, the Tanium application must be configured to allow for LDAP to provide account management functions that immediately enforce the organization's current account policy.

Audit:

1. Using a web browser on a system that has connectivity to the Tanium application, access the Tanium application web user interface (UI) and log on with multifactor authentication.
2. Click "Administration" on the top navigation banner.
3. Under "Configuration", select "LDAP/AD Sync Configurations".
4. Ensure LDAP sync is enabled.

If LDAP is not enabled, this is a finding.

Remediation:

Vendor documentation can be downloaded from https://docs.tanium.com/platform_user/platform_user/console_using_ldap.html?Highlight=LDAP.

1. Using a web browser on a system that has connectivity to the Tanium application, access the Tanium application web UI and log on with multifactor authentication.
2. Click "Administration" on the top navigation banner.
3. Under "Configuration", select "LDAP/AD Sync Configurations".
4. Follow the vendor documentation titled "Integrating with LDAP Servers" to implement correct configuration settings for this requirement.

Additional Information:

CCI-000015

Support the management of system accounts using organization-defined automated mechanisms.

- NIST SP 800-53::AC-2 (1)
- NIST SP 800-53A::AC-2 (1).1
- NIST SP 800-53 Revision 4::AC-2 (1)
- NIST SP 800-53 Revision 5::AC-2 (1)

1.39 TANS-CN-000004 (Manual)

Profile Applicability:

- SEVERITY: CAT II

Description:

Tanium Computer Groups must be used to restrict console users from effecting changes to unauthorized computers.

```
GROUP ID: V-253817
RULE ID: SV-253817r842479
```

Rationale:

Computer Groups allow a site running Tanium to assign responsibility of specific Computer Groups to specific Tanium console users. By doing so, a desktop administrator, for example, will not have the ability to enforce an action against a high-visibility server.

For large sites, it is crucial to have the Computer Groups. While a smaller site might not seem to require Computer Groups, creating them provides for a cleaner implementation. All sites will be required to have some kind of Computer Groups configured other than the default "All Computers".

Audit:

1. Using a web browser on a system that has connectivity to the Tanium Application, access the Tanium Application web user interface (UI) and log on with multifactor authentication.
2. Click "Administration" on the top navigation banner.
3. Select the "Computer Groups" tab.
4. Under the "Name" column, verify organization-specific computer groups match organization-defined list in the system security plan (SSP).

If site- or organization-specific computer groups do not match or exist, this is a finding.

Remediation:

1. Using a web browser on a system that has connectivity to the Tanium Server, access the Tanium Server web UI and log on with multifactor authentication.
2. Click "Administration" on the top navigation banner.
3. Select the "Computer Groups" tab.
4. Configure specific Computer Groups to facilitate the management of computers by authorized individuals for those computers.

Note: Tanium offers two ways to define computer groups. Refer to the following documentation for explanation: https://docs.tanium.com/platform_user/platform_user/console_computer_groups.html#Computer_Group_types

Additional Information:

CCI-000213

Enforce approved authorizations for logical access to information and system resources in accordance with applicable access control policies.

- NIST SP 800-53::AC-3
- NIST SP 800-53A::AC-3.1
- NIST SP 800-53 Revision 4::AC-3
- NIST SP 800-53 Revision 5::AC-3

1.40 TANS-CN-000005 (Manual)

Profile Applicability:

- SEVERITY: CAT II

Description:

Documentation identifying Tanium console users, their respective User Groups, Computer Groups, and Roles must be maintained.

```
GROUP ID: V-253818
RULE ID: SV-253818r842482
```

Rationale:

System access should be reviewed periodically to verify that all Tanium users are assigned the appropriate functional role, with the least privileged access possible to perform assigned tasks being the recommended best practice to avoid unauthorized access.

Audit:

Consult with the Tanium system administrator to review the documented list of Tanium users. The users' User Groups, Roles, Computer Groups, and correlated LDAP security groups must be documented.

If the documentation does not exist or is missing any Tanium users and their respective User Groups, Roles, Computer Groups, and correlated LDAP security groups, this is a finding.

Remediation:

Prepare and maintain documentation identifying the Tanium console users and their respective User Groups, Roles, Computer Groups, and associated LDAP security groups.

Additional Information:

CCI-000213

Enforce approved authorizations for logical access to information and system resources in accordance with applicable access control policies.

- NIST SP 800-53::AC-3
- NIST SP 800-53A::AC-3.1
- NIST SP 800-53 Revision 4::AC-3
- NIST SP 800-53 Revision 5::AC-3

1.41 TANS-CN-000006 (Manual)

Profile Applicability:

- SEVERITY: CAT II

Description:

The Tanium application must be configured to use Tanium User Groups in a manner consistent with the model outlined in the environment's system documentation.

```
GROUP ID: V-253819
RULE ID: SV-253819r842485
```

Rationale:

It is important for information system owners to document authorized User Groups for the Tanium application to avoid unauthorized access to systems. Misaligned implementation of User Groups grants excessive access and results in potential compromise of "need-to-know" for information access.

Audit:

1. Consult with the Tanium system administrator to review the documented list of Tanium User Groups.
2. Using a web browser on a system that has connectivity to the Tanium application, access the Tanium application web user interface (UI) and log on with multifactor authentication.
3. Click "Administration" on the top navigation banner.
4. Under "Permissions", select "User Groups".
5. Click each User Group and compare both the User Group name and the assigned Role(s) to the system documentation.

If any users have access to Tanium and their User Group is not on the list of documented User Groups with the appropriate Role(s), this is a finding.

Remediation:

Consult the documentation identifying the Tanium User Groups and their respective Role(s).

1. Using a web browser on a system that has connectivity to the Tanium application, access the Tanium application web UI and log on with multifactor authentication.
2. Click "Administration" on the top navigation banner.
3. Under "Permissions", select "User Groups".
4. Click each User Group and add any missing Role(s).
5. For any missing User Groups, make the appropriate adjustments in LDAP.

Additional Information:

CCI-000213

Enforce approved authorizations for logical access to information and system resources in accordance with applicable access control policies.

- NIST SP 800-53::AC-3
- NIST SP 800-53A::AC-3.1
- NIST SP 800-53 Revision 4::AC-3
- NIST SP 800-53 Revision 5::AC-3

1.42 TANS-CN-000008 (Manual)

Profile Applicability:

- SEVERITY: CAT II

Description:

Documentation identifying Tanium console users and their respective Computer Group rights must be maintained.

```
GROUP ID: V-253820
RULE ID: SV-253820r842488
```

Rationale:

System access should be reviewed periodically to verify all Tanium users are assigned the appropriate computer groups, with the least privileged access possible to perform assigned tasks. Users who have been removed from the documentation should no longer be configured as a Tanium Console User.

Audit:

Consult with the Tanium system administrator to review the documented list of Tanium users and their respective, approved Computer Group rights.

If the documented list does not have the Tanium users and their respective, approved Computer Group rights documented, this is a finding.

Remediation:

Prepare and maintain documentation identifying the Tanium console users and their respective Computer Group rights.

Additional Information:

CCI-000213

Enforce approved authorizations for logical access to information and system resources in accordance with applicable access control policies.

- NIST SP 800-53::AC-3
- NIST SP 800-53A::AC-3.1
- NIST SP 800-53 Revision 4::AC-3
- NIST SP 800-53 Revision 5::AC-3

1.43 TANS-CN-000010 (Manual)

Profile Applicability:

- SEVERITY: CAT I

Description:

Multifactor authentication must be enabled on the Tanium Server for network access with privileged accounts.

```
GROUP ID: V-253821
RULE ID: SV-253821r858410
```

Rationale:

The Tanium application must be configured to use multifactor authentication. Without the use of multifactor authentication, the ease of access to privileged functions is greatly increased.

Multifactor authentication requires using two or more factors to achieve authentication.

Factors include:

1. Something a user knows (e.g., password/PIN);
2. Something a user has (e.g., cryptographic identification device, token); or
3. Something a user is (e.g., biometric).

A privileged account is defined as an information system account with authorizations of a privileged user.

Network access is defined as access to an information system by a user (or a process acting on behalf of a user) communicating through a network (e.g., local area network, wide area network, or the internet).

Satisfies: SRG-APP-000151

Audit:

1. Access the Tanium Server.
2. Log on to the server with an account that has administrative privileges.
3. Run regedit as Administrator.
4. Navigate to `HKEY_LOCAL_MACHINE >> SOFTWARE >> WOW6432Node >> Tanium >> Tanium Server`.
5. Validate the value for `REG_DWORD ForceSOAPSSLClientCert` is set to `1`.
6. Navigate to `HKEY_LOCAL_MACHINE >> SOFTWARE >> WOW6432Node >> Tanium >> Tanium Server`.
7. Validate the following keys exist and are configured:

```
REG_SZ "ClientCertificateAuthField"
```

```
For example:
X509v3 Subject Alternative Name

REG_SZ "ClientCertificateAuthRegex"
For example-DoD:
.+?Name:\s*?(\S+@[._a-zA-Z0-9]+).*
Note: This regex may vary.

REG_SZ "ClientCertificateAuth"
For example:
C:\Program Files\Tanium\Tanium Server\cac.pem

REG_SZ "TrustedHostList"
For example:
127.0.0.1 (for IPv4) and [::1] (for IPv6)
```

If the value for `REG_DWORD ForceSOAPSSLClientCert` is not set to `1` and the remaining registry values are not configured, this is a finding.

Remediation:

Use the vendor documentation titled "Smartcard authentication" to implement correct configuration settings for this requirement. The documentation is at https://docs.tanium.com/platform_deployment_reference/platform_deployment_reference/smart_card_authentication.html?Highlight=cac.

1. Access the Tanium Server.
2. Log on to the server with an account that has administrative privileges.
3. Run regedit as Administrator.
4. Navigate to `HKEY_LOCAL_MACHINE >> SOFTWARE >> WOW6432Node >> Tanium >> Tanium Server`.
5. Validate the value for `REG_DWORD ForceSOAPSSLClientCert` is set to `1`.
6. Navigate to `HKEY_LOCAL_MACHINE >> SOFTWARE >> WOW6432Node >> Tanium >> Tanium Server`.
7. Configure the following keys:

```
REG_SZ "ClientCertificateAuthField"
For example:
X509v3 Subject Alternative Name

REG_SZ "ClientCertificateAuthRegex"
For example-DoD:
.+?Name:\s*?(\S+@[._a-zA-Z0-9]+).*
Note: This regex may vary.

REG_SZ "ClientCertificateAuth"
For example:
C:\Program Files\Tanium\Tanium Server\cac.pem

REG_SZ "TrustedHostList"
For example:
Append 127.0.0.1 (for IPv4) and [::1] (for IPv6)
```

Additional Information:

CCI-000765

Implement multifactor authentication for access to privileged accounts.

- NIST SP 800-53::IA-2 (1)
- NIST SP 800-53A::IA-2 (1).1
- NIST SP 800-53 Revision 4::IA-2 (1)
- NIST SP 800-53 Revision 5::IA-2 (1)

CCI-000767

The information system implements multifactor authentication for local access to privileged accounts.

- NIST SP 800-53::IA-2 (3)
- NIST SP 800-53A::IA-2 (3).1
- NIST SP 800-53 Revision 4::IA-2 (3)

1.44 TANS-CN-000014 (Manual)

Profile Applicability:

- SEVERITY: CAT II

Description:

Firewall rules must be configured on the Tanium Server for Console-to-Server communications.

```
GROUP ID: V-253822
RULE ID: SV-253822r850218
```

Rationale:

An HTML5-based application, the Tanium Console runs from any device with a browser that supports HTML5. For security, the HTTP and SOAP communication to the Tanium Server is SSL encrypted, so the Tanium Server installer configures the server to listen for HTTP and SOAP requests on port 443. Without a proper connection to the Tanium Server, access to the system capabilities could be denied.

Port Needed: To Tanium Server over TCP port 443.

Network firewall rules:

Allow HTTP traffic on TCP port 443 from any computer on the internal network to the Tanium Server device.

For more information, refer to https://docs.tanium.com/platform_install/platform_install/reference_network_ports.html.

Audit:

Consult with the Tanium system administrator to verify which firewall is being used as a host-based firewall on the Tanium Server.

1. Access the Tanium Server.
2. Log on to the server with an account that has administrative privileges.
3. Access the host-based firewall configuration on the Tanium Server.
4. Validate a rule exists for the following:

Port Needed: From only designated Tanium console user clients to Tanium Server over TCP port 443.

If a host-based firewall rule does not exist to allow only designated Tanium console user clients to Tanium Server over TCP port 443, this is a finding.

Consult with the network firewall administrator and validate rules exist for the following: Allow TCP traffic from only designated Tanium console user clients to Tanium Server over TCP ports 443.

If a network firewall rule does not exist to allow traffic from only designated Tanium console user clients to Tanium Server over TCP port 443, this is a finding.

Remediation:

1. Configure host-based firewall rules on the Tanium Server to include the following required traffic:

Allow TCP traffic on port 433 to the Tanium Server from designated Tanium console user clients.

Configure the network firewall to allow the above traffic.

Additional Information:

CCI-001762

Disable or remove organization-defined functions, ports, protocols, software, and services within the system deemed to be unnecessary and/or nonsecure.

- NIST SP 800-53 Revision 4::CM-7 (1) (b)
- NIST SP 800-53 Revision 5::CM-7 (1) (b)

1.45 TANS-CN-000015 (Manual)

Profile Applicability:

- SEVERITY: CAT II

Description:

The publicly accessible Tanium application must display the Standard Mandatory DoD Notice and Consent Banner before granting access to the application.

```
GROUP ID: V-253823
RULE ID: SV-253823r858411
```

Rationale:

Display of a standardized and approved use notification before granting access to the publicly accessible application ensures privacy and security notification verbiage used is consistent with applicable federal laws, Executive Orders, directives, policies, regulations, standards, and guidance.

System use notifications are required only for access via logon interfaces with human users and are not required when such human interfaces do not exist.

The banner must be formatted in accordance with DTM-08-060. Use the following verbiage for desktops, laptops, and other devices accommodating banners of 1300 characters:

"You are accessing a U.S. Government (USG) Information System (IS) that is provided for USG-authorized use only.

By using this IS (which includes any device attached to this IS), you consent to the following conditions:

- The USG routinely intercepts and monitors communications on this IS for purposes including, but not limited to, penetration testing, COMSEC monitoring, network operations and defense, personnel misconduct (PM), law enforcement (LE), and counterintelligence (CI) investigations.
- At any time, the USG may inspect and seize data stored on this IS.
- Communications using, or data stored on, this IS are not private, are subject to routine monitoring, interception, and search, and may be disclosed or used for any USG-authorized purpose.
- This IS includes security measures (e.g., authentication and access controls) to protect USG interests--not for your personal benefit or privacy.
- Notwithstanding the above, using this IS does not constitute consent to PM, LE or CI investigative searching or monitoring of the content of privileged communications, or work product, related to personal representation or services by attorneys, psychotherapists, or clergy, and their assistants. Such communications and work product are private and confidential. See User Agreement for details."

Satisfies: SRG-APP-000069; SRG-APP-000070

Audit:

1. Using a web browser on a system that has connectivity to the Tanium application, access the Tanium application web user interface (UI) and log on with multifactor authentication.
2. Verify the DoD use notification displays prior to login:

```
"You are accessing a U.S. Government (USG) Information System (IS) that is
provided for USG-authorized use only. By using this IS (which includes any
device attached to this IS), you consent to the following conditions: The USG
routinely intercepts and monitors communications on this IS for purposes
including, but not limited to, penetration testing, COMSEC monitoring, network
operations and defense, personnel misconduct (PM), law enforcement (LE), and
counterintelligence (CI) investigations. At any time, the USG may inspect and
seize data stored on this IS. Communications using, or data stored on, this IS
are not private, are subject to routine monitoring, interception, and search,
and may be disclosed or used for any USG-authorized purpose. This IS includes
security measures (e.g., authentication and access controls) to protect USG
interests--not for your personal benefit or privacy. Notwithstanding the above,
using this IS does not constitute consent to PM, LE or CI investigative
searching or monitoring of the content of privileged communications, or work
product, related to personal representation or services by attorneys,
psychotherapists, or clergy, and their assistants. Such communications and work
product are private and confidential. See User Agreement for details."
```

If a DoD-approved use notification banner does not display prior to logon or cannot be acknowledged before granting access, this is a finding.

Remediation:

1. Create a .html file composed of the DoD-authorized warning banner verbiage:

```
"You are accessing a U.S. Government (USG) Information System (IS) that is
provided for USG-authorized use only. By using this IS (which includes any
device attached to this IS), you consent to the following conditions: The USG
routinely intercepts and monitors communications on this IS for purposes
including, but not limited to, penetration testing, COMSEC monitoring, network
operations and defense, personnel misconduct (PM), law enforcement (LE), and
counterintelligence (CI) investigations. At any time, the USG may inspect and
seize data stored on this IS. Communications using, or data stored on, this IS
are not private, are subject to routine monitoring, interception, and search,
and may be disclosed or used for any USG-authorized purpose. This IS includes
security measures (e.g., authentication and access controls) to protect USG
interests--not for your personal benefit or privacy. Notwithstanding the above,
using this IS does not constitute consent to PM, LE or CI investigative
searching or monitoring of the content of privileged communications, or work
product, related to personal representation or services by attorneys,
psychotherapists, or clergy, and their assistants. Such communications and work
product are private and confidential. See User Agreement for details."
```

2. Name the file `warning_banner.html`".
3. Copy the .html file to the Tanium Server's http folder `<drive>:\Program Files\Tanium\Tanium Server\http\`.

4. Using a web browser on a system that has connectivity to the Tanium application, access the Tanium application web UI and log on with multifactor authentication.
5. Click "Administration" on the top navigation banner.
6. Under "Configuration", select "Platform Settings".
7. Click "Create Setting".
8. Select "Server" box from "Setting Type".
9. In "Create Platform Setting" dialog box, enter `console_PreLoginBannerHTML` for `Name`.
10. Select `Text` radio button from `Value Type`.
11. Enter `warning_banner.html` for `Value:`.
12. Click "Save".

Additional Information:

CCI-000048

Display an organization-defined system use notification message or banner to users before granting access to the system that provides privacy and security notices consistent with applicable federal laws, Executive Orders, directives, policies, regulations, standards, and guidelines.

- NIST SP 800-53::AC-8 a
- NIST SP 800-53A::AC-8.1 (ii)
- NIST SP 800-53 Revision 4::AC-8 a
- NIST SP 800-53 Revision 5::AC-8 a

CCI-000050

Retain the notification message or banner on the screen until users acknowledge the usage conditions and take explicit actions to log on to or further access the system.

- NIST SP 800-53::AC-8 b
- NIST SP 800-53A::AC-8.1 (iii)
- NIST SP 800-53 Revision 4::AC-8 b
- NIST SP 800-53 Revision 5::AC-8 b

CCI-001384

For publicly accessible systems, display system use information with organization-defined conditions before granting further access to the publicly accessible system.

- NIST SP 800-53::AC-8 c
- NIST SP 800-53A::AC-8.2 (i)
- NIST SP 800-53 Revision 4::AC-8 c 1
- NIST SP 800-53 Revision 5::AC-8 c 1

CCI-001385

For publicly accessible systems, displays references, if any, to monitoring that are consistent with privacy accommodations for such systems that generally prohibit those activities.

- NIST SP 800-53::AC-8 c
- NIST SP 800-53A::AC-8.2 (ii)
- NIST SP 800-53 Revision 4::AC-8 c 2
- NIST SP 800-53 Revision 5::AC-8 c 2

CCI-001386

For publicly accessible systems, displays references, if any, to recording that are consistent with privacy accommodations for such systems that generally prohibit those activities.

- NIST SP 800-53::AC-8 c
- NIST SP 800-53A::AC-8.2 (ii)
- NIST SP 800-53 Revision 4::AC-8 c 2
- NIST SP 800-53 Revision 5::AC-8 c 2

CCI-001387

For publicly accessible systems, displays references, if any, to auditing that are consistent with privacy accommodations for such systems that generally prohibit those activities.

- NIST SP 800-53::AC-8 c
- NIST SP 800-53A::AC-8.2 (ii)
- NIST SP 800-53 Revision 4::AC-8 c 2
- NIST SP 800-53 Revision 5::AC-8 c 2

CCI-001388

For publicly accessible systems, includes a description of the authorized uses of the system.

- NIST SP 800-53::AC-8 c
- NIST SP 800-53A::AC-8.2 (iii)
- NIST SP 800-53 Revision 4::AC-8 c 3
- NIST SP 800-53 Revision 5::AC-8 c 3

1.46 TANS-CN-000016 (Manual)

Profile Applicability:

- SEVERITY: CAT II

Description:

The Tanium application must alert the information system security officer and system administrator (at a minimum) in the event of an audit processing failure.

```
GROUP ID: V-253824
RULE ID: SV-253824r842500
```

Rationale:

It is critical for the appropriate personnel to be aware if a system is at risk of failing to process audit logs as required. Without this notification, the security personnel may be unaware of an impending failure of the audit capability, and system operation may be adversely affected.

Audit processing failures include software/hardware errors, failures in the audit capturing mechanisms, and audit storage capacity being reached or exceeded.

This requirement applies to each audit data storage repository (i.e., distinct information system component where audit records are stored), the centralized audit storage capacity of organizations (i.e., all audit data storage repositories combined), or both.

Audit:

1. Using a web browser on a system that has connectivity to the Tanium application, access the Tanium application web user interface (UI) and log on with multifactor authentication.
2. Click "Modules" on the top navigation banner.
3. Click "Connect".
4. Review the configured Connections under "Connections" section.

Work with the security information and event management (SIEM) administrator to determine if an alert is configured when audit data is no longer received as expected.

If no alert is configured, this is a finding.

Remediation:

1. Using a web browser on a system that has connectivity to the Tanium application, access the Tanium application web UI and log on with multifactor authentication.
2. Click "Modules" on the top navigation banner.
3. Click "Connect".
4. Expand the left menu.

5. Click "Connections".
6. Configure a Connection for the "Tanium Audit Source" source from the Tanium Application to a SIEM tool.

Work with the SIEM administrator to configure an alert when no audit data is received from Tanium based on the defined schedule of connections.

Additional Information:

CCI-000139

Alert organization-defined personnel or roles within an organization-defined time period in the event of an audit logging process failure.

- NIST SP 800-53::AU-5 a
- NIST SP 800-53A::AU-5.1 (ii)
- NIST SP 800-53 Revision 4::AU-5 a
- NIST SP 800-53 Revision 5::AU-5 a

1.47 TANS-CN-000019 (Manual)

Profile Applicability:

- SEVERITY: CAT II

Description:

Tanium must notify system administrator and information system security officer (ISSO) when accounts are created.

```
GROUP ID: V-253825
RULE ID: SV-253825r842503
```

Rationale:

Once an attacker establishes initial access to a system, the attacker often attempts to create a persistent method of reestablishing access. One way to accomplish this is for the attacker to create a new account. Notification of account creation is one method for mitigating this risk. A comprehensive account management process will ensure an audit trail, which documents the creation of application user accounts and notifies administrators and ISSOs. Such a process greatly reduces the risk that accounts will be surreptitiously created and provides logging that can be used for forensic purposes.

To address access requirements, many application developers choose to integrate their applications with enterprise-level authentication/access/auditing mechanisms that meet or exceed access control policy requirements. Such integration allows the application developer to offload those access control functions and focus on core application features and functionality.

Audit:

1. Using a web browser on a system that has connectivity to the Tanium application, access the Tanium application web user interface (UI) and log on with multifactor authentication.
2. Click "Modules" on the top navigation banner.
3. Click "Connect".
4. Review the configured connections.

If no sources exist to send audit logs from Tanium to a security information and event management (SIEM) tool or email destination, this is a finding.

Work with the SIEM administrator to determine if an alert is configured when accounts are created.

If no alert is configured, this is a finding.

Remediation:

1. Using a web browser on a system that has connectivity to the Tanium application, access the Tanium application web UI and log on with multifactor authentication.
2. Click "Modules" on the top navigation banner.
3. Click "Connect".
4. Click "Create Connection" in the "Connections" section.
5. Configure sources to send audit logs from the Tanium SQL Server to a SIEM tool or email destination.
6. Work with the email administrator to configure an email destination.
7. Work with the SIEM administrator to configure an alert when accounts are created.

Additional Information:

CCI-001683

The information system notifies organization-defined personnel or roles for account creation actions.

- NIST SP 800-53::AC-2 (4)
- NIST SP 800-53 Revision 4::AC-2 (4)
- NIST SP 800-53A::AC-2 (4).1 (i and ii)

1.48 TANS-CN-000020 (Manual)

Profile Applicability:

- SEVERITY: CAT II

Description:

Tanium must notify system administrators and the information system security officer (ISSO) when accounts are modified.

```
GROUP ID: V-253826
RULE ID: SV-253826r842506
```

Rationale:

When application accounts are modified, user accessibility is affected. Accounts are utilized for identifying individual users or for identifying the application processes. Sending notification of account modification events to the system administrator and ISSO is one method for mitigating this risk. Such a capability greatly reduces the risk that application accessibility will be negatively affected for extended periods of time and also provides logging that can be used for forensic purposes.

To address access requirements, many operating systems can be integrated with enterprise-level authentication/access/auditing mechanisms that meet or exceed access control policy requirements.

Audit:

1. Using a web browser on a system that has connectivity to the Tanium application, access the Tanium application web user interface (UI) and log on with multifactor authentication.
2. Click "Modules" on the top navigation banner.
3. Click "Connect".
4. Review the configured connections.

If no sources exist to send audit logs from the Tanium Database to a security information and event management (SIEM) tool or email destination, this is a finding.

Work with the SIEM administrator to determine if an alert is configured when accounts are modified.

If no alert is configured, this is a finding.

Remediation:

1. Using a web browser on a system that has connectivity to the Tanium application, access the Tanium application web UI and log on with multifactor authentication.
2. Click "Modules" on the top navigation banner.

3. Click "Connect".
4. Click "Create Connection" in the "Connections" section.
5. Configure sources to send audit logs from the Tanium SQL Server to a SIEM tool or email destination.
6. Work with the email administrator to configure an email destination.
7. Work with the SIEM administrator to configure an alert when accounts are modified.

Additional Information:

CCI-001684

The information system notifies organization-defined personnel or roles for account modification actions.

- NIST SP 800-53::AC-2 (4)
- NIST SP 800-53 Revision 4::AC-2 (4)
- NIST SP 800-53A::AC-2 (4).1 (i and ii)

1.49 TANS-CN-000021 (Manual)

Profile Applicability:

- SEVERITY: CAT II

Description:

Tanium must notify the system administrator and information system security officer (ISSO) of account enabling actions.

```
GROUP ID: V-253827
RULE ID: SV-253827r850159
```

Rationale:

Once an attacker establishes access to an application, the attacker often attempts to create a persistent method of reestablishing access. One way to accomplish this is for the attacker to enable a new or disabled account. Sending notification of account enabling events to the system administrator and ISSO is one method for mitigating this risk. Such a capability greatly reduces the risk that application accessibility will be negatively affected for extended periods of time and also provides logging that can be used for forensic purposes.

To detect and respond to events that affect user accessibility and application processing, applications must notify the appropriate individuals so they can investigate the event.

To address access requirements, many application developers choose to integrate their applications with enterprise-level authentication/access/auditing mechanisms that meet or exceed access control policy requirements. Such integration allows the application developer to offload those access control functions and focus on core application features and functionality.

Audit:

1. Using a web browser on a system that has connectivity to the Tanium application, access the Tanium application web user interface (UI) and log on with multifactor authentication.
2. Click "Modules" on the top navigation banner.
3. Click "Connect".
4. Review the configured sources.

If no sources exists to send audit logs from the Tanium SQL Server to a security information and event management (SIEM) tool or email destination, this is a finding.

Work with the SIEM administrator to determine if an alert is configured when account-enabling actions are performed.

If no alert is configured, this is a finding.

Remediation:

1. Using a web browser on a system that has connectivity to the Tanium application, access the Tanium application web UI and log on with multifactor authentication.
2. Click "Modules" on the top navigation banner.
3. Click "Connect".
4. Configure sources to send audit logs from the Tanium SQL Server to a SIEM tool or email destination.
5. Work with the email administrator to configure an email destination.
6. Work with the SIEM administrator to configure an alert when account-enabling actions are performed.

Additional Information:

CCI-002132

The information system notifies organization-defined personnel or roles for account enabling actions.

- NIST SP 800-53 Revision 4::AC-2 (4)

1.50 TANS-CN-000027 (Manual)

Profile Applicability:

- SEVERITY: CAT II

Description:

Multifactor authentication must be enabled and enforced on the Tanium Server for all access and all accounts.

```
GROUP ID: V-253828
RULE ID: SV-253828r858412
```

Rationale:

To ensure accountability and prevent unauthenticated access, organizational users must be identified and authenticated to prevent potential misuse and compromise of the system.

Organizational users include organizational employees or individuals the organization deems to have equivalent status of employees (e.g., contractors). Organizational users (and any processes acting on behalf of users) must be uniquely identified and authenticated for all accesses, except the following.

1. Accesses explicitly identified and documented by the organization. Organizations document specific user actions that can be performed on the information system without identification or authentication; and
2. Accesses that occur through authorized use of group authenticators without individual authentication. Organizations may require unique identification of individuals in group accounts (e.g., shared privilege accounts) or for detailed accountability of individual activity.

Satisfies: SRG-APP-000080; SRG-APP-000403; SRG-APP-000156; SRG-APP-000005; SRG-APP-000150; SRG-APP-000152

Audit:

1. Access the Tanium Server.
2. Log on to the server with an account that has administrative privileges.
3. Run regedit as Administrator.
4. Navigate to `HKEY_LOCAL_MACHINE >> SOFTWARE >> WOW6432Node >> Tanium >> Tanium Server`.
5. Validate the value for `REG_DWORD ForceSOAPSSLClientCert` is set to `1`.
6. Navigate to `HKEY_LOCAL_MACHINE >> SOFTWARE >> WOW6432Node >> Tanium >> Tanium Server`.
7. Validate the following keys exist and are configured:

```
REG_SZ "ClientCertificateAuthField"
```

```
For example:
X509v3 Subject Alternative Name

REG_SZ "ClientCertificateAuthRegex"
For example-DoD:
.+?Name:\s*?(\S+@[._a-zA-Z0-9]+).*
Note: This regex may vary.

REG_SZ "ClientCertificateAuth"
For example:
E:\Program Files\Tanium\Tanium Server\cac.pem

REG_SZ "TrustedHostList"
For example:
127.0.0.1 (for IPv4) and [::1] (for IPv6)
```

If the value for `REG_DWORD ForceSOAPSSLClientCert` is not set to `1` and the remaining required registry values are not configured, this is a finding.

Remediation:

Use the vendor documentation titled "Smart card authentication" to implement correct configuration settings for this requirement.

Vendor documentation can be downloaded from https://docs.tanium.com/platform_deployment_reference/platform_deployment_reference/smart_card_authentication.html?Highlight=cac.

1. Access the Tanium Server.
2. Log on to the server with an account that has administrative privileges.
3. Run regedit as Administrator.
4. Navigate to `HKEY_LOCAL_MACHINE >> SOFTWARE >> WOW6432Node >> Tanium >> Tanium Server`.
5. Configure the value for `REG_DWORD ForceSOAPSSLClientCert` to `1`.
6. Navigate to `HKEY_LOCAL_MACHINE >> SOFTWARE >> WOW6432Node >> Tanium >> Tanium Server`.
7. Configure the following keys:

```
REG_SZ "ClientCertificateAuthField"
For example:
X509v3 Subject Alternative Name

REG_SZ "ClientCertificateAuthRegex"
For example-DoD:
.+?Name:\s*?(\S+@[._a-zA-Z0-9]+).*
Note: This regex may vary.

REG_SZ "ClientCertificateAuth"
For example:
E:\Program Files\Tanium\Tanium Server\cac.pem

REG_SZ "TrustedHostList"
For example:
Append 127.0.0.1 (for IPv4) and [::1] (for IPv6)
```

Additional Information:

CCI-000764 Uniquely identify and authenticate organizational users and associate that unique identification with processes acting on behalf of those users.

- NIST SP 800-53::IA-2
- NIST SP 800-53A::IA-2.1
- NIST SP 800-53 Revision 4::IA-2
- NIST SP 800-53 Revision 5::IA-2

CCI-000056 Retain the device lock until the user reestablishes access using established identification and authentication procedures.

- NIST SP 800-53::AC-11 b
- NIST SP 800-53A::AC-11.1 (iii)
- NIST SP 800-53 Revision 4::AC-11 b
- NIST SP 800-53 Revision 5::AC-11 b

CCI-000166 Provide irrefutable evidence that an individual (or process acting on behalf of an individual) falsely denying having performed organization-defined actions to be covered by non-repudiation.

- NIST SP 800-53::AU-10
- NIST SP 800-53A::AU-10.1
- NIST SP 800-53 Revision 4::AU-10
- NIST SP 800-53 Revision 5::AU-10

CCI-000766 Implement multifactor authentication for access to non-privileged accounts.

- NIST SP 800-53::IA-2 (2)
- NIST SP 800-53A::IA-2 (2).1
- NIST SP 800-53 Revision 4::IA-2 (2)
- NIST SP 800-53 Revision 5::IA-2 (2)

CCI-000768 The information system implements multifactor authentication for local access to non-privileged accounts.

- NIST SP 800-53::IA-2 (4)
- NIST SP 800-53A::IA-2 (4).1
- NIST SP 800-53 Revision 4::IA-2 (4)

CCI-001941 Implement replay-resistant authentication mechanisms for access to privileged accounts and/or non-privileged accounts.

- NIST SP 800-53 Revision 4::IA-2 (8)
- NIST SP 800-53 Revision 5::IA-2 (8)

CCI-002010 Electronically verify Personal Identity Verification-compliant credentials from other federal agencies.

- NIST SP 800-53 Revision 4::IA-8 (1)
- NIST SP 800-53 Revision 5::IA-8 (1)

1.51 TANS-CN-000032 (Manual)

Profile Applicability:

- SEVERITY: CAT II

Description:

Tanium must notify system administrators and the information system security officer (ISSO) for account disabling actions.

```
GROUP ID: V-253829
RULE ID: SV-253829r842515
```

Rationale:

When application accounts are disabled, user accessibility is affected. Accounts are utilized for identifying individual users or for identifying the application processes. Sending notification of account disabling events to the system administrator and ISSO is one method for mitigating this risk. Such a capability greatly reduces the risk that application accessibility will be negatively affected for extended periods of time and also provides logging that can be used for forensic purposes.

To address access requirements, many operating systems can be integrated with enterprise-level authentication/access/auditing mechanisms that meet or exceed access control policy requirements.

Audit:

1. Using a web browser on a system that has connectivity to the Tanium application, access the Tanium application web user interface (UI) and log on with multifactor authentication.
2. Click "Modules" on the top navigation banner.
3. Click "Connect".
4. Review the configured connections.

If no sources exist to send audit logs from the Tanium SQL Server to a security information and event management (SIEM) tool or email destination, this is a finding.

Work with the SIEM administrator to determine if an alert is configured when accounts are disabled.

If no alert is configured, this is a finding.

Remediation:

1. Using a web browser on a system that has connectivity to the Tanium application, access the Tanium application web UI and log on with multifactor authentication.
2. Click "Modules" on the top navigation banner.

3. Click "Connect".
4. Click "Create Connection" in the "Connections" section.
5. Configure sources to send audit logs from the Tanium SQL Server to a SIEM tool or email destination.
6. Work with the email administrator to configure an email destination.
7. Work with the SIEM administrator to configure an alert when accounts are modified.

Additional Information:

CCI-001685

The information system notifies organization-defined personnel or roles for account disabling actions.

- NIST SP 800-53::AC-2 (4)
- NIST SP 800-53 Revision 4::AC-2 (4)
- NIST SP 800-53A::AC-2 (4).1 (i and ii)

1.52 TANS-CN-000033 (Manual)

Profile Applicability:

- SEVERITY: CAT II

Description:

Tanium must notify system administrators and the information system security officer (ISSO) for account removal actions.

```
GROUP ID: V-253830
RULE ID: SV-253830r842518
```

Rationale:

When application accounts are removed, user accessibility is affected. Accounts are utilized for identifying users or for identifying the application processes. Sending notification of account removal events to the system administrator and ISSO is one method for mitigating this risk. Such a capability greatly reduces the risk that application accessibility will be negatively affected for extended periods of time and also provides logging that can be used for forensic purposes.

To address access requirements, many operating systems can be integrated with enterprise-level authentication/access/auditing mechanisms that meet or exceed access control policy requirements.

Audit:

1. Using a web browser on a system that has connectivity to the Tanium application, access the Tanium application web user interface (UI) and log on with multifactor authentication.
2. Click "Modules" on the top navigation banner.
3. Click "Connect".
4. Review the configured connections.

If no sources exist to send audit logs from the Tanium SQL Server to a security information and event management (SIEM) tool or email destination, this is a finding.

Work with the SIEM administrator to determine if an alert is configured when accounts are deleted.

If no alert is configured, this is a finding.

Remediation:

1. Using a web browser on a system that has connectivity to the Tanium application, access the Tanium application web UI and log on with multifactor authentication.
2. Click "Modules" on the top navigation banner.

3. Click "Connect".
4. Configure sources to send audit logs from the Tanium SQL Server to a SIEM tool or email destination.
5. Work with the email administrator to configure an email destination.
6. Work with the SIEM administrator to configure an alert when accounts are deleted.

Additional Information:

CCI-001686

The information system notifies organization-defined personnel or roles for account removal actions.

- NIST SP 800-53::AC-2 (4)
- NIST SP 800-53A::AC-2 (4).1 (i and ii)
- NIST SP 800-53 Revision 4::AC-2 (4)

1.53 TANS-CN-000036 (Manual)

Profile Applicability:

- SEVERITY: CAT II

Description:

The Tanium application must prohibit user installation, modification, or deletion of software without explicit privileged status.

```
GROUP ID: V-253831
RULE ID: SV-253831r858413
```

Rationale:

Allowing regular users to install, modify, or delete software, without explicit privileges, creates the risk that the application performs in a manner inconsistent with its design. Explicit privileges (escalated or administrative privileges) provide the regular user with explicit capabilities and control that exceed the rights of a regular user.

Application functionality will vary, and while users are not permitted to install unapproved applications, there may be instances where the organization allows the user to install approved software packages, such as from an approved software repository.

The application must enforce software installation by users based on what types of software installations are permitted (e.g., updates and security patches to existing software) and what types of installations are prohibited (e.g., software whose pedigree with regard to being potentially malicious is unknown or suspect) by the organization.

Satisfies: SRG-APP-000122; SRG-APP-000123

Audit:

1. Consult with the Tanium system administrator to review the documented list of Tanium users.
2. Using a web browser on a system that has connectivity to the Tanium application, access the Tanium application web user interface (UI) and log on with multifactor authentication.
3. Click "Administration" on the top navigation banner.
4. Under "Permissions", select "Users".
5. Review the users' respective approved roles, as well as the correlated LDAP security group for the User Roles.
6. Validate LDAP security groups/Tanium roles are documented to assign least privileged access to the functions of the Tanium Server through the Tanium interface.

If the documentation does not reflect a granular, least privileged access approach to the LDAP Groups/Tanium Roles assignment, this is a finding.

Remediation:

1. Using a web browser on a system that has connectivity to the Tanium application, access the Tanium application web UI and log on with multifactor authentication.
2. Click "Administration" on the top navigation banner.
3. Under "Permissions", select "Users".
4. Analyze the users configured in the Tanium interface.
5. Determine least privileged access required for each user to perform their respective duties.
6. Move users to the appropriate LDAP security group to ensure the user is synced to the appropriate Tanium User Role.
7. If the appropriate LDAP security groups are not already configured, create the groups and add the appropriate users.
8. Ensure LDAP sync repopulates the Tanium Users' associated Roles accordingly.

Additional Information:

CCI-001493

Protect audit tools from unauthorized access.

- NIST SP 800-53::AU-9
- NIST SP 800-53A::AU-9.1
- NIST SP 800-53 Revision 4::AU-9
- NIST SP 800-53 Revision 5::AU-9 a

CCI-001494

Protect audit tools from unauthorized modification.

- NIST SP 800-53::AU-9
- NIST SP 800-53A::AU-9.1
- NIST SP 800-53 Revision 4::AU-9
- NIST SP 800-53 Revision 5::AU-9 a

CCI-001495

Protect audit tools from unauthorized deletion.

- NIST SP 800-53::AU-9
- NIST SP 800-53A::AU-9.1
- NIST SP 800-53 Revision 4::AU-9
- NIST SP 800-53 Revision 5::AU-9 a

1.54 TANS-DB-000001 (Manual)

Profile Applicability:

- SEVERITY: CAT II

Description:

The Tanium database(s) must be installed on a separate system.

```
GROUP ID: V-253832
RULE ID: SV-253832r850162
```

Rationale:

Failure to protect organizational information from data mining may result in a compromise of information.

Data storage objects include, for example, databases, database records, and database fields. Data mining prevention and detection techniques include, for example, limiting the types of responses provided to database queries; limiting the number/frequency of database queries to increase the work factor needed to determine the contents of such databases; and notifying organizational personnel when atypical database queries or accesses occur.

Audit:

Note: If the customer is using a Tanium Appliance, this is not applicable.

Consult with the Tanium system administrator to determine the server to which the database has been installed and is configured.

1. Access the Tanium Server.
2. Log on to each Tanium Application Server with an account that has administrative privileges.
3. Verify Tanium Module Service is not running on both servers.
4. Verify SQL Server Services are not running on both servers.

If the Tanium Module Service is running on either server, this is a finding.

If SQL Server Services are running on either server, this is a finding.

If the database is installed on the same server as the Tanium Server or Tanium Module Server, this is a finding.

Remediation:

Move the Tanium database from the Tanium Server or Tanium Module Server to a separate server. Steps to move the Tanium database can be found at https://docs.tanium.com/platform_install/platform_install/installing_tanium_server.html#set_up_DB_server.

Additional Information:

CCI-002346

Employ organization-defined data mining prevention techniques for organization-defined data storage objects to protect against unauthorized data mining.

- NIST SP 800-53 Revision 4::AC-23
- NIST SP 800-53 Revision 5::AC-23

1.55 TANS-DB-000002 (Manual)

Profile Applicability:

- SEVERITY: CAT II

Description:

The Tanium application database must be dedicated to only the Tanium application.

```
GROUP ID: V-253833
RULE ID: SV-253833r850162
```

Rationale:

Failure to protect organizational information from data mining may result in a compromise of information.

Data storage objects include, for example, databases, database records, and database fields. Data mining prevention and detection techniques include, for example, limiting the types of responses provided to database queries; limiting the number/frequency of database queries to increase the work factor needed to determine the contents of such databases; and notifying organizational personnel when atypical database queries or accesses occur.

Audit:

With the Tanium system administrator's assistance, access the server on which the Tanium database(s) is installed.

1. Access the Tanium Server.
2. Log on to each Tanium Application Server with an account that has administrative privileges.
3. Verify SQL Server Services are not running on both servers.

If SQL Server Services are running on either server, this is a finding.

Review the Tanium database(s). If databases related to products other than Tanium exist in the Tanium database, this is a finding.

Remediation:

Move the Tanium database from the server hosting multiple databases for products other than Tanium or remove other product databases co-located with Tanium database(s).

Additional Information:

CCI-002346

Employ organization-defined data mining prevention techniques for organization-defined data storage objects to protect against unauthorized data mining.

- NIST SP 800-53 Revision 4::AC-23
- NIST SP 800-53 Revision 5::AC-23

1.56 TANS-DB-000003 (Manual)

Profile Applicability:

- SEVERITY: CAT II

Description:

The access to the Tanium SQL database must be restricted. Only the designated database administrator(s) can have elevated privileges to the Tanium SQL database.

```
GROUP ID: V-253834
RULE ID: SV-253834r850216
```

Rationale:

After the Tanium Server has been installed and the Tanium databases created, only the Tanium Server needs to access the SQL Server database.

Audit:

1. Access the Tanium SQL server interactively.
2. Log on to the server with an account that has administrative privileges.
3. Open SQL Server Management Studio.
4. Connect to a Tanium instance of SQL Server.
5. In the left pane, click "Databases".
6. Select the Tanium database.
7. Click "Security".
8. Click "Users".
9. In the "Users" pane, review the roles assigned to the user accounts. (Note: This does not apply to service accounts.)
10. Select the Tanium_archive database.
11. Click "Security".
12. Click "Users".
13. In the "Users" pane, review the roles assigned to the user accounts. (Note: This does not apply to service accounts.)

If any user account has an elevated privilege role other than the assigned database administrators, this is a finding.

Remediation:

1. Access the Tanium SQL server interactively.
2. Log on to the server with an account that has administrative privileges.
3. Open SQL Server Management Studio.
4. Connect to a Tanium instance of SQL Server.
5. In the left pane, click "Databases".
6. Select the Tanium database.
7. Click "Security".

8. Click "Users".
9. In the "Users" pane, review the roles assigned to the user accounts. (Note: This does not apply to service accounts.)
10. Select the Tanium_archive database.
11. Click "Security".
12. Click "Users".
13. Adjust user roles as necessary. (Note: This does not apply to service accounts.)

Additional Information:

CCI-001814

The Information system supports auditing of the enforcement actions.

- NIST SP 800-53 Revision 4::CM-5 (1)

1.57 TANS-DB-000004 (Manual)

Profile Applicability:

- SEVERITY: CAT II

Description:

The Tanium Server installer's account database permissions must be reduced to an appropriate level.

```
GROUP ID: V-253835
RULE ID: SV-253835r850216
```

Rationale:

Creating the "tanium" and "tanium_archive" databases through the Tanium Server installer program or using the database to create SQL scripts requires Sysadmin-level permissions. Once the databases have been created, the Tanium Server services must be configured to execute under an account that holds at least the Database Owner (dbo) role on both databases.

Post-installation, if the account used to configure the Tanium Server services to access the remote SQL database server holds only the Database Owner role, rather than the sysadmin role, grant this account the View Server State permission on the SQL Server. This dynamic management view enables the Tanium Server to access data faster than the dbo role alone.

Audit:

1. Access the Tanium SQL server interactively.
2. Log on to the server with an account that has administrative privileges.
3. Open SQL Server Management Studio.
4. Connect to Tanium instance of SQL Server.
5. In the left pane, click "Databases".
6. Select the Tanium database.
7. Click "Security".
8. Click "Users".
9. In the "Users" pane, review the role assigned to the Tanium Server service user account.
10. In the left pane, click "Databases".
11. Select the Tanium_archive database.
12. Click "Security".
13. Click "Users".
14. In the "Users" pane, review the role assigned to the Tanium Server service user account.
15. If the role assigned to the Tanium Server service account is not "db_owner", this is a finding.
16. If using Postgres:

Only owners of objects can change them. To view all functions, triggers, and trigger procedures, and their ownership and source, as the database administrator (shown here as "postgres"), run the following SQL:

```
$ sudo su - postgres
$ psql -x -c "\df+"
```

Remediation:

1. Access the Tanium SQL server interactively.
2. Log on to the server with an account that has administrative privileges.
3. Open SQL Server Management Studio.
4. Connect to Tanium instance of SQL Server.
5. In the left pane, click "Databases".
6. Select the Tanium database.
7. Click "Security".
8. Click "Users".
9. In the "Users" pane, right-click the Tanium Server service user account.
10. On the shortcut menu, click "Properties".
11. Under Database role membership, change role from "sysadmin" to "db_owner".
12. Click "OK".
13. In the left pane, click "Databases".
14. Select the Tanium_archive database.
15. Click "Security".
16. Click "Users".
17. In the "Users" pane, right-click the Tanium Server service user account.
18. On the shortcut menu, click "Properties".
19. Under Database role membership, change role from "sysadmin" to "db_owner".
20. Click "OK"
21. If using Postgres:

Configure PostgreSQL to enforce access restrictions associated with changes to the configuration of PostgreSQL or database(s).

Use ALTER ROLE to remove accesses from roles:

```
$ psql -c "ALTER ROLE <role_name> NOSUPERUSER"
```

Additional Information:

CCI-001814

The Information system supports auditing of the enforcement actions.

- NIST SP 800-53 Revision 4::CM-5 (1)

1.58 TANS-DB-000005 (Manual)

Profile Applicability:

- SEVERITY: CAT II

Description:

Firewall rules must be configured on the Tanium Server for server-to-database communications.

```
GROUP ID: V-253836
RULE ID: SV-253836r850218
```

Rationale:

The Tanium Server can use either a SQL Server relational database management system (RDBMS) installed locally to the same device as the Tanium Server application or a remote dedicated or shared SQL Server instance. Using a local SQL Server database typically requires no changes to network firewall rules since all communication remains on the Tanium application server device. To access database resources installed to a remote device, however, the Tanium Server service communicates over the port reserved for SQL, by default port 1433, to the database.

Port Needed: Tanium Server to Remote SQL Server over TCP port 1433.

Network firewall rules:

Allow TCP traffic on port 1433 from the Tanium Server device to the remote device hosting the SQL Server RDBMS.

For more information, refer to https://docs.tanium.com/platform_install/platform_install/reference_network_ports.html.

Audit:

Consult with the Tanium system administrator to verify which firewall is being used as a host-based firewall on the Tanium Server.

1. Access the Tanium Server.
2. Log on to the server with an account that has administrative privileges.
3. Access the host-based firewall configuration on the Tanium Server.
4. Validate a rule exists for the following:

Port Needed: Tanium Server to Remote SQL Server over TCP port 1433.

If a host-based firewall rule does not exist to allow Tanium Server to Remote SQL Server over TCP port 1433, this is a finding.

Consult with the network firewall administrator and validate rules exist for the following:

Allow traffic from Tanium Server to Remote SQL Server over TCP port 1433.

If a network firewall rule does not exist to allow traffic from Tanium Server to Remote SQL Server over TCP port 1433, this is a finding.

Remediation:

1. Configure host-based firewall rules on the Tanium Server to include the following required traffic: Allow TCP traffic on port 1433 from the Tanium Server to the Remote SQL Server.
2. Configure the network firewall to allow the above traffic.

Additional Information:

CCI-001762

Disable or remove organization-defined functions, ports, protocols, software, and services within the system deemed to be unnecessary and/or nonsecure.

- NIST SP 800-53 Revision 4::CM-7 (1) (b)
- NIST SP 800-53 Revision 5::CM-7 (1) (b)

1.59 TANS-SV-000002 (Manual)

Profile Applicability:

- SEVERITY: CAT II

Description:

The Tanium Application Server console must be configured to initiate a session lock after a 15-minute period of inactivity.

```
GROUP ID: V-253837
RULE ID: SV-253837r842539
```

Rationale:

When multifactor authentication is enabled, the Tanium Console will initiate a session lock based on the ActivClient or other smartcard software.

By initiating the session lock, the console will be locked and not allow unauthorized access by anyone other than the original user.

Although this setting does not apply when multifactor authentication is enabled, it should be explicitly disabled in the event multifactor authentication is ever broken or removed.

Audit:

1. Using a web browser on a system that has connectivity to the Tanium application, access the Tanium application web user interface (UI) and log on with multifactor authentication.
2. Click "Administration" on the top navigation banner.
3. Under "Configuration", select "Platform Settings".
4. In the "Filter items" search box, type `max_console_idle_seconds`.
5. Click "Enter".

If no results are returned, this is a finding.

If results are returned for `max_console_idle_seconds`, but the value is not between the range of `1 - 900`, this is a finding.

Remediation:

1. Using a web browser on a system that has connectivity to the Tanium application, access the Tanium application web UI and log on with multifactor authentication.
2. Click "Administration" on the top navigation banner.
3. Under "Configuration", select "Platform Settings".
4. Click "Create Setting".
5. Select "Server" box for "Setting Type".

6. In "Create Platform Setting" dialog box enter `max_console_idle_seconds` for `Name`.
7. Select `Numeric` radio button from `Value Type`.
8. Select `Value` and enter a value between the range of `1 - 900`.
9. Click "Save".
10. Add this setting to the system documentation for validation.

Additional Information:

CCI-000057

Prevent further access to the system by initiating a device lock after organization-defined time period of inactivity; and/or requiring the user to initiate a device lock before leaving the system unattended.

- NIST SP 800-53::AC-11 a
- NIST SP 800-53A::AC-11.1 (ii)
- NIST SP 800-53 Revision 4::AC-11 a
- NIST SP 800-53 Revision 5::AC-11 a

1.60 TANS-SV-000003 (Manual)

Profile Applicability:

- SEVERITY: CAT II

Description:

Tanium Trusted Content providers must be documented.

```
GROUP ID: V-253838
RULE ID: SV-253838r842542
```

Rationale:

A Tanium Sensor, also called content, enables an organization to gather real-time inventory, configuration, and compliance data elements from managed computers. Sensors gather specific information from the local device and then write the results to the computer's standard output channel. The Tanium Client captures that output and forwards the results through the platform's unique "ring" architecture for display in the Tanium Console.

The language used for Sensor development is based on the scripting engine available on the largest number of devices under management as well as the scripting experience and background of the people who will be responsible for creating new Sensors. VBScript and PowerShell are examples of common scripting languages used for developing sensors.

Because errors in scripting can and will provide errant feedback at best and will impact functionality of the endpoint to which the content is directed, it is imperative to ensure content is accepted only from trusted sources.

Audit:

Note: If only using Tanium-provided content and not accepting content from any other content providers, this is not applicable.

Consult with the Tanium system administrator to review the documented list of trusted content providers along with the hash for their respective public keys.

If the site does not have the Tanium trusted content providers documented along with the SHA-256 hash for their respective public keys, this is a finding.

Remediation:

Prepare and maintain documentation identifying the Tanium trusted content providers along with the SHA-256 hash from their respective public keys.

Additional Information:

CCI-001453

Implement cryptographic mechanisms to protect the integrity of remote access sessions.

- NIST SP 800-53::AC-17 (2)
- NIST SP 800-53A::AC-17 (2).1
- NIST SP 800-53 Revision 4::AC-17 (2)
- NIST SP 800-53 Revision 5::AC-17 (2)

1.61 TANS-SV-000004 (Manual)

Profile Applicability:

- SEVERITY: CAT II

Description:

Content providers must provide their public key to the Tanium administrator to import for validating signed content.

```
GROUP ID: V-253839
RULE ID: SV-253839r842545
```

Rationale:

A Tanium Sensor, also called content, enables an organization to gather real-time inventory, configuration, and compliance data elements from managed computers. Sensors gather specific information from the local device and then write the results to the computer's standard output channel. The Tanium Client captures that output and forwards the results through the platform's unique "ring" architecture for display in the Tanium Console.

The language used for Sensor development is based on the scripting engine available on the largest number of devices under management as well as the scripting experience and background of the people who will be responsible for creating new Sensors. VBScript and PowerShell are examples of common scripting languages used for developing sensors.

Because errors in scripting can and will provide errant feedback at best and will impact functionality of the endpoint to which the content is directed, it is imperative to ensure content is only accepted from trusted sources.

Audit:

Note: If only using Tanium-provided content and not accepting content from any other content providers, this is not applicable.

Obtain documentation that contains the public key validation data from the Tanium system administrator.

1. Access the Tanium Server.
2. Log on to the server with an account that has administrative privileges.
3. Open an Explorer window.
4. Navigate to the following folder: Program Files >> Tanium >> Tanium Server >> content_public_keys >> content folder.

If the Tanium default content-release.pub key is the only key in the folder, this is not a finding.

If documented content provider keys are in the content folder, this is not a finding.

If nondocumented content provider keys are in the content folder, this is a finding.

Remediation:

Obtain the public key from the content providers and validate the keys are present in the Tanium folders.

If the public keys are found for nontrusted content providers, remove the associated signing key and remove any content imported by that provider.

1. Access the Tanium Server.
2. Log on to the server with an account that has administrative privileges.
3. Open an Explorer window.
4. Navigate to the following folder: Program Files >> Tanium >> Tanium Server >> content_public_keys >> content folder.
5. Copy any trusted source's `.pub` keys into the folder and document them.
6. Remove any nontrusted source's `.pub` keys from the folder.

Additional Information:

CCI-001453

Implement cryptographic mechanisms to protect the integrity of remote access sessions.

- NIST SP 800-53::AC-17 (2)
- NIST SP 800-53A::AC-17 (2).1
- NIST SP 800-53 Revision 4::AC-17 (2)
- NIST SP 800-53 Revision 5::AC-17 (2)

1.62 TANS-SV-000005 (Manual)

Profile Applicability:

- SEVERITY: CAT II

Description:

Tanium public keys of content providers must be validated against documented trusted content providers.

```
GROUP ID: V-253840
RULE ID: SV-253840r842548
```

Rationale:

A Tanium Sensor, also called content, enables an organization to gather real-time inventory, configuration, and compliance data elements from managed computers. Sensors gather specific information from the local device and then write the results to the computer's standard output channel. The Tanium Client captures that output and forwards the results through the platform's unique "ring" architecture for display in the Tanium Console.

The language used for Sensor development is based on the scripting engine available on the largest number of devices under management as well as the scripting experience and background of the people who will be responsible for creating new Sensors. VBScript and PowerShell are examples of common scripting languages used for developing sensors.

Because errors in scripting can and will provide errant feedback at best and will impact functionality of the endpoint to which the content is directed, it is imperative to ensure content is only accepted from trusted sources.

Audit:

Note: If only using Tanium-provided content and not accepting content from any other content providers, this is not applicable.

Obtain documentation from the Tanium system administrator that contains the public key validation data.

1. Access the Tanium Server.
2. Log on to the server with an account that has administrative privileges.
3. Open an Explorer window.
4. Navigate to the following folder: Program Files >> Tanium >> Tanium Server >> content_public_keys >> content folder.
5. Verify the public keys listed in the content folder are documented.

If a public key, other than the default Tanium public key, is in the content folder and is not documented, this is a finding.

Remediation:

1. Access the Tanium Server.
2. Log on to the server with an account that has administrative privileges.
3. Open an Explorer window.
4. Navigate to the following folder: Program Files >> Tanium >> Tanium Server >> content_public_keys >> content folder.
5. If a public key, other than the default Tanium public key, resides in the content folder, use a hashing utility (e.g., `TaniumFileInfo.exe`) to determine the hash of the public key.
6. Document the owner, the name of the key, and the associated hash of the public key.

Additional Information:

CCI-001453

Implement cryptographic mechanisms to protect the integrity of remote access sessions.

- NIST SP 800-53::AC-17 (2)
- NIST SP 800-53A::AC-17 (2).1
- NIST SP 800-53 Revision 4::AC-17 (2)
- NIST SP 800-53 Revision 5::AC-17 (2)

1.63 TANS-SV-000006 (Manual)

Profile Applicability:

- SEVERITY: CAT II

Description:

The Tanium Action Approval feature must be enabled for two-person integrity when deploying actions to endpoints.

```
GROUP ID: V-253841
RULE ID: SV-253841r858414
```

Rationale:

The Tanium Action Approval feature provides a two-person integrity control mechanism designed to achieve a high level of security and reduce the possibility of error for critical operations.

When this feature is enabled, an action configured by one Tanium console user will require a second Tanium console user with a role of Action Approver (or higher) to approve the action before it is deployed to targeted computers.

While this system slows workflow, the reliability of actions deployed will be greater on the Packaging and Targeting.

Satisfies: SRG-APP-000488

Audit:

1. Using a web browser on a system that has connectivity to the Tanium application, access the Tanium application web user interface (UI) and log on with multifactor authentication.
2. Click "Administration" on the top navigation banner.
3. Under "Configuration", select "Platform Settings".
4. In the "Filter items" search box, type `require_action_approval`.
5. Click "Enter".

If no results are returned, this is a finding.

If results are returned for `require_action_approval`, but the value is not `1`, this is a finding.

Remediation:

1. Using a web browser on a system that has connectivity to the Tanium application, access the Tanium application web UI and log on with multifactor authentication.
2. Click "Administration" on the top navigation banner.

3. Under "Configuration", select "Platform Settings".
4. If "require_action_approval" does not exist: click "Create Setting".
5. Select `Server` box for `Setting Type`.
6. In "Create Platform Setting" dialog box, enter `require_action_approval` for `Name`.
7. Select `Numeric` radio button from `Value Type`.
8. Select `Value` and enter `1`.
9. Click "Save".

Additional Information:

CCI-000213

Enforce approved authorizations for logical access to information and system resources in accordance with applicable access control policies.

- NIST SP 800-53::AC-3
- NIST SP 800-53A::AC-3.1
- NIST SP 800-53 Revision 4::AC-3
- NIST SP 800-53 Revision 5::AC-3

CCI-002460

Enforce organization-defined actions prior to executing mobile code.

- NIST SP 800-53 Revision 4::SC-18 (4)
- NIST SP 800-53 Revision 5::SC-18 (4)

1.64 TANS-SV-000007 (Manual)

Profile Applicability:

- SEVERITY: CAT II

Description:

The Tanium documentation identifying recognized and trusted indicator of compromise (IOC) streams must be maintained.

```
GROUP ID: V-253842
RULE ID: SV-253842r842554
```

Rationale:

Using trusted and recognized IOC sources may detect compromise and prevent systems from becoming compromised. An IOC stream is a series or stream of IOCs that are imported from a vendor based on a subscription service. An IOC stream can be downloaded manually or on a scheduled basis. The items in an IOC stream can be manipulated separately after they are imported.

Audit:

Consult with the Tanium system administrator to determine if the Threat Response module is being used. If it is not, this is not applicable.

Review the documented list of IOC trusted stream sources.

If the site uses an external source for IOCs and the IOC trusted stream source is not documented, this is a finding.

Remediation:

Prepare and maintain documentation identifying the Threat Response trusted stream sources.

Additional Information:

CCI-001414

Enforce approved authorizations for controlling the flow of information between connected systems based on organization-defined information flow control policies.

- NIST SP 800-53::AC-4
- NIST SP 800-53A::AC-4.1 (iii)
- NIST SP 800-53 Revision 4::AC-4
- NIST SP 800-53 Revision 5::AC-4

1.65 TANS-SV-000008 (Manual)

Profile Applicability:

- SEVERITY: CAT II

Description:

Tanium Threat Response must be configured to receive IOC streams only from trusted sources.

```
GROUP ID: V-253843
RULE ID: SV-253843r842557
```

Rationale:

Using trusted and recognized IOC sources may detect compromise and prevent systems from becoming compromised. An IOC stream is a series or stream of intel that is imported from a vendor based on a subscription service or manually downloaded and placed in a folder. Threat Response can be configured to retrieve the IOC content on a regularly scheduled basis. The items in an IOC stream can be manipulated separately after they are imported.

Audit:

Consult with the Tanium system administrator to determine if the Threat Response module is being used. If it is not, this is not applicable.

1. Using a web browser on a system that has connectivity to the Tanium application, access the Tanium application web user interface (UI) and log on with multifactor authentication.
2. Click "Modules" on the top navigation banner.
3. Click "Threat Response".
4. Expand the left menu.
5. Click "Intel".
6. Select "Sources".
7. Verify all configured Threat Response Streams are configured to a documented trusted source.

If Threat Response is configured to a stream that has not been documented as trusted, this is a finding.

Remediation:

Consult the documentation on trusted intel subscription feeds.

1. Using a web browser on a system that has connectivity to the Tanium application, access the Tanium application web UI and log on with multifactor authentication.

2. Click "Modules" on the top navigation banner.
3. Click "Threat Response".
4. Expand the left menu.
5. Click "Intel".
6. Select "Sources".
7. Click "New Source".
8. Select the specified Source from the list.
9. Fill out the specified information based on the documented trusted intel feeds.
10. Select "Create".

Additional Information:

CCI-001414

Enforce approved authorizations for controlling the flow of information between connected systems based on organization-defined information flow control policies.

- NIST SP 800-53::AC-4
- NIST SP 800-53A::AC-4.1 (iii)
- NIST SP 800-53 Revision 4::AC-4
- NIST SP 800-53 Revision 5::AC-4

1.66 TANS-SV-000010 (Manual)

Profile Applicability:

- SEVERITY: CAT II

Description:

The Tanium applications must be configured to filter audit records for events of interest based on organization-defined criteria.

```
GROUP ID: V-253844
RULE ID: SV-253844r842560
```

Rationale:

The ability to specify the event criteria that are of interest enables those reviewing the logs to quickly isolate and identify these events without having to review entries that are of little or no consequence to the investigation. Without this capability, forensic investigations are impeded.

Events of interest can be identified by the content of specific audit record fields including, for example, identities of individuals, event types, event locations, event times, event dates, system resources involved, IP addresses involved, or information objects accessed. Organizations may define audit event criteria to any degree of granularity required, for example, locations selectable by general networking location (e.g., by network or subnetwork) or by specific information system component. This requires applications to provide the capability to customize audit record reports based on organization-defined criteria.

Audit:

1. Using a web browser on a system that has connectivity to the Tanium application, access the Tanium application web user interface (UI) and log on with multifactor authentication.
2. Click "Modules" on the top navigation banner.
3. Click "Connect".
4. Click "Connections" under "Connections" section.
5. Filter by source and review event-based sources.

If any event=based sources have a failed run for more than 72 hours, this is a finding.

Remediation:

1. Using a web browser on a system that has connectivity to the Tanium application, access the Tanium application web UI and log on with multifactor authentication.
2. Click "Modules" on the top navigation banner.
3. Click "Connect".

4. Expand the left menu.
5. Click "Connections".
6. Click "Create Connection" or if importing, click "Import".
7. Give the "Connection" a name and description.
8. In the "Configuration" section, select "Event" as the source.
9. Select appropriate source under "Event Group" - any source to generate interest-based events (Discover, Asset, IM, THR, etc).
10. Select the appropriate events to send. **Note:** Consult with the Tanium system administrator for the Destination.
11. Select "Listen for this Event".
12. Click "Save".

Additional Information:

CCI-000158

Provide the capability to process, sort, and search audit records for events of interest based on organization-defined audit fields within audit records.

- NIST SP 800-53::AU-7 (1)
- NIST SP 800-53A::AU-7 (1).1
- NIST SP 800-53 Revision 4::AU-7 (1)
- NIST SP 800-53 Revision 5::AU-7 (1)

1.67 TANS-SV-000014 (Manual)

Profile Applicability:

- SEVERITY: CAT II

Description:

The Tanium cryptographic signing capabilities must be enabled on the Tanium Server.

```
GROUP ID: V-253845
RULE ID: SV-253845r858415
```

Rationale:

All of Tanium's signing capabilities should be enabled upon install. Tanium supports the cryptographic signing and verification before execution of all Sensors, Questions, Actions, Sensor Libraries, File Shards, etc. Enabling signing does away with the ability of an attacker to conduct man-in-the-middle (MitM) attacks for remote code execution and precludes the modification of the aforementioned data elements in transit. Additionally, Tanium supports object level signing for content ingested into the Tanium platform. This allows for the detection and rejection of changes to objects (sensors, actions, etc.) by even a privileged user within Tanium.

Tanium has built-in signing capabilities enabled by default when installed. Cryptographic signing and verification of all Sensors, Questions, Actions, Sensor Libraries, File Shards, etc., before execution will be enforced by Tanium.

Signing will prevent MitM remote code execution attacks and will protect data elements in transit. Tanium also supports object-level signing for content within the Tanium platform.

Satisfies: SRG-APP-000233; SRG-APP-000317

Audit:

1. Using a web browser on a system that has connectivity to the Tanium application, access the Tanium application web user interface (UI) and log on with multifactor authentication.
2. Click "Administration" on the top navigation banner.
3. Under "Configuration", select "Platform Settings".
4. In the "Filter Items" search box, type `sign_all_questions_flag`.
5. Click "Enter".

If no results are returned, this is a finding.

If results are returned for `sign_all_questions_flag` but the value is not `1`, this is a finding.

Remediation:

1. Using a web browser on a system that has connectivity to the Tanium application, access the Tanium application web UI and log on with multifactor authentication.
2. Click "Administration" on the top navigation banner.
3. Under "Configuration", select "Platform Settings".
4. Click "Create Setting".
5. Select `Server` box for `Setting Type`.
6. In "Create Platform Setting" dialog box, enter `sign_all_questions_flag` for `Name`.
7. Select `Numeric` radio button for `Value Type`.
8. Enter `1` for `Value`.
9. Click "Save".

Additional Information:

CCI-001749

The information system prevents the installation of organization-defined software components without verification the software component has been digitally signed using a certificate that is recognized and approved by the organization.

- NIST SP 800-53 Revision 4::CM-5 (3)

CCI-001084

Isolate security functions from nonsecurity functions.

- NIST SP 800-53::SC-3
- NIST SP 800-53A::SC-3.1 (ii)
- NIST SP 800-53 Revision 4::SC-3
- NIST SP 800-53 Revision 5::SC-3

CCI-002142

The information system terminates shared/group account credentials when members leave the group.

- NIST SP 800-53 Revision 4::AC-2 (10)

1.68 TANS-SV-000015 (Manual)

Profile Applicability:

- SEVERITY: CAT II

Description:

The Tanium Server must be configured to allow only signed content to be imported.

```
GROUP ID: V-253846
RULE ID: SV-253846r850129
```

Rationale:

Changes to any software components can have significant effects on the overall security of the application. Verifying software components have been digitally signed using a certificate that is recognized and approved by the organization ensures the software has not been tampered with and that it has been provided by a trusted vendor.

Patches, service packs, or application components must be signed with a certificate recognized and approved by the organization.

Verifying the authenticity of the software prior to installation validates the integrity of the patch or upgrade received from a vendor. This ensures the software has not been tampered with and that it has been provided by a trusted vendor. Self-signed certificates are disallowed by this requirement. The application should not have to verify the software again. This requirement does not mandate DoD certificates for this purpose; however, the certificate used to verify the software is from an approved certificate authority (CA).

Audit:

Note: This requirement applies only to Tanium implementations in production. If implementation being evaluated is in development, this requirement is not applicable.

1. Access the Tanium Server through interactive logon.
2. Open Windows Explorer and browse to the installation drive of the Tanium Server (e.g., E:\Program Files\Tanium\Tanium Server).
3. Locate the "tanium.license" file and double-click it.
4. Select Notepad to open the "tanium.license" file.
5. Select "Edit" and then select "Find" from the menu in Notepad.
6. Type `allow_unsigned_import` in the search box and select "Find Next."

If `allow unsigned_import` is followed by `:true`, this is a finding.

If `allow unsigned_import` is followed by `:false`, this is not a finding.

Remediation:

Contact Tanium for a corrected license file.

1. Double-click the new `tanium.license` file and select Notepad to open the file.
   2.. Select "Edit" and then select "Find" from the menu in Notepad.
2. Type `allow_unsigned_import` in the search box and select "Find Next".
3. Verify `allow unsigned_import` is followed by `:false`.
4. Access the Tanium Server through interactive logon.
5. Open Windows Explorer and browse to the installation drive of the Tanium Server (e.g., `E:\Program Files\Tanium\Tanium Server`).
6. Locate the `tanium.license` file and copy it to a backup location.
7. Copy the new `tanium.license` file to the installation drive and directory of the Tanium Server (e.g., `E:\Program Files\Tanium\Tanium Server`).

Additional Information:

CCI-001749

The information system prevents the installation of organization-defined software components without verification the software component has been digitally signed using a certificate that is recognized and approved by the organization.

- NIST SP 800-53 Revision 4::CM-5 (3)

1.69 TANS-SV-000016 (Manual)

Profile Applicability:

- SEVERITY: CAT II

Description:

All installation files originally downloaded to the Tanium Server must be configured to download to a location other than the Tanium Server directory.

```
GROUP ID: V-253847
RULE ID: SV-253847r842569
```

Rationale:

Typically, the Tanium Server stores the Package Source Files that it downloads from the internet and server shares or files uploaded through the Tanium Console in a subdirectory of the server's installation directory called "Downloads". To ensure package files are not accessible to nonauthorized functions, the files must be relocated to outside of the server's installation directory.

Audit:

1. Access the Tanium Server.
2. Log on to the server with an account that has administrative privileges.
3. Run regedit as Administrator.
4. Navigate to `HKEY_LOCAL_MACHINE >> SOFTWARE >> WOW6432Node >> Tanium >> Tanium Server`.
5. Validate the value name `DownloadPath` with value type `REG_SZ` does not point to a location within the Tanium Server directory.

If the value name `DownloadPath` with value type `REG_SZ` does not exist or points to a location within the Tanium Server directory, this is a finding.

If the `DownloadPath REG_SZ` value points to a location within the Tanium Server directory, this is a finding.

Remediation:

1. Access the Tanium Server.
2. Log on to the server with an account that has administrative privileges.
3. Create a new folder outside of the Tanium Server directory (e.g., `E:\Stage\Downloads`).
4. Run regedit as Administrator.
5. Navigate to `HKEY_LOCAL_MACHINE >> SOFTWARE >> WOW6432Node >> Tanium >> Tanium Server`.

6. Add or change the value name `DownloadPath` with value type `REG_SZ` to point to the location of the relocated installation package files (e.g., `E:\Stage\Downloads`).
7. Move the files from the original directory (`E:\Program Files\Tanium\Tanium Server\Downloads`) to the location created for the installation package files.
8. Move the files from the original directory (`E:\Program Files\Tanium\Tanium Server\Downloads`) to the location created for the installation package files.

Additional Information:

CCI-001499

Limit privileges to change software resident within software libraries.

- NIST SP 800-53::CM-5 (6)
- NIST SP 800-53A::CM-5 (6).1
- NIST SP 800-53 Revision 4::CM-5 (6)
- NIST SP 800-53 Revision 5::CM-5 (6)

1.70 TANS-SV-000017 (Manual)

Profile Applicability:

- SEVERITY: CAT II

Description:

Firewall rules must be configured on the Tanium Server for client-to-server communications.

```
GROUP ID: V-253848
RULE ID: SV-253848r842572
```

Rationale:

In addition to the client-to-server TCP communication that takes place over port 17472, Tanium Clients also communicate to other Tanium-managed computers over port 17472. Without proper firewall configurations, proper TCP communications may not take place as necessary for application functionality. The Tanium environment can perform hundreds or thousands of times faster than other security or systems management tools because the Tanium Clients communicate in secure, linearly controlled peer-to-peer rings. Because clients dynamically communicate with other nearby agents based on proximity and latency, rings tend to form automatically to match a customer's topology. For example, endpoints in California will form one ring while endpoints in Germany will form a separate ring.

For more information, refer to https://docs.tanium.com/platform_deployment_reference/platform_deployment_reference/network_ports.html.

Audit:

Note: This check is performed for the Tanium endpoints and must be validated against the enterprise firewall solution (e.g., Endpoint Security Solution Firewall, Microsoft Windows Defender Firewall setting, Microsoft Advance Threat Protection Firewall, etc.) policies applied to the endpoints.

1. Consult with the personnel who maintain the Enterprise Security Suite configuration for assistance.
2. Validate a rule exists within the firewall policies for managed clients for the following:

   Port Needed: Tanium Clients or Zone Clients over TCP port 17472, bidirectionally.

   If a host-based firewall rule does not exist to allow TCP port 17472, bidirectionally, this is a finding.

3. Consult with the boundary network firewall administrator and validate rules exist for the following:

Allow TCP traffic on port 17472 from any computer to be managed on a local area network to any other computer to be managed on the same local area network.

If a network firewall rule does not exist to allow TCP port 17472 from any managed computer to any other managed computer on the same local area network, this is a finding.

Remediation:

1. Consult with the personnel who maintain the Enterprise Security Suite to configure host-based and network firewall rules to allow the following:

   Tanium Clients or Zone Clients over TCP port 17472, bidirectionally.

2. Consult with the boundary network firewall administrator to create a rule to allow the following:

TCP traffic on port 17472 from any computer to be managed on a local area network to any other computer to be managed on the same local area network.

Additional Information:

CCI-000382

Configure the system to prohibit or restrict the use of organization-defined prohibited or restricted functions, system ports, protocols, software, and/or services.

- NIST SP 800-53::CM-7
- NIST SP 800-53A::CM-7.1 (iii)
- NIST SP 800-53 Revision 4::CM-7 b
- NIST SP 800-53 Revision 5::CM-7 b

1.71 TANS-SV-000018 (Manual)

Profile Applicability:

- SEVERITY: CAT II

Description:

Firewall rules must be configured on the Tanium Zone Server for Client-to-Zone Server communications.

```
GROUP ID: V-253849
RULE ID: SV-253849r842575
```

Rationale:

In customer environments using the Tanium Zone Server, a Tanium Client may be configured to point to a Zone Server instead of a Tanium Server. The communication requirements for these Clients are identical to the Server-to-Client requirements. Without proper firewall configurations, proper TCP communications may not take place as necessary for application functionality. Additionally, without proper configuration, organizations may lose complete visibility into endpoints that cannot connect directly to the Tanium Server.

For more information, refer to https://docs.tanium.com/platform_deployment_reference/platform_deployment_reference/network_ports.html.

Audit:

Note: If a Zone Server is not being used, this is not applicable.

1. Consult with the Tanium system administrator to verify which firewall is being used as a host-based firewall on the Tanium Zone Server.
2. Access the host-based firewall configuration on the Tanium Zone Server.
3. Validate a rule exists for the following:

Port Needed: Tanium Clients to Zone Server over TCP port 17472, bidirectionally.

If a host-based firewall rule does not exist to allow TCP port 17472, bidirectionally, from Tanium Clients to the Tanium Zone Server, this is a finding.

Remediation:

Consult with the personnel who maintain the Enterprise Security Suite to configure host-based and network firewall rules to allow the following:

Tanium Clients or Zone Clients over TCP port 17472, bidirectionally.

Additional Information:

CCI-000382

Configure the system to prohibit or restrict the use of organization-defined prohibited or restricted functions, system ports, protocols, software, and/or services.

- NIST SP 800-53::CM-7
- NIST SP 800-53A::CM-7.1 (iii)
- NIST SP 800-53 Revision 4::CM-7 b
- NIST SP 800-53 Revision 5::CM-7 b

1.72 TANS-SV-000019 (Manual)

Profile Applicability:

- SEVERITY: CAT II

Description:

The Tanium Application Server must be configured to prohibit or restrict the use of organization-defined functions, ports, protocols, and/or services, as defined in the PPSM Category Assurance List (CAL) and vulnerability assessments.

```
GROUP ID: V-253850
RULE ID: SV-253850r842578
```

Rationale:

To prevent unauthorized connection of devices, unauthorized transfer of information, or unauthorized tunneling (i.e., embedding of data types within data types), organizations must disable or restrict unused or unnecessary physical and logical ports/protocols on information systems.

Applications are capable of providing a wide variety of functions and services. Some of the functions and services provided by default may not be necessary to support essential organizational operations. Additionally, it is sometimes convenient to provide multiple services from a single component (e.g., email and web services); however, doing so increases risk over limiting the services provided by any one component.

To support the requirements and principles of least functionality, the application must support the organizational requirements providing only essential capabilities and limiting the use of ports, protocols, and/or services to only those required, authorized, and approved to conduct official business or address authorized quality-of-life issues.

Audit:

Review the PPSM CAL to verify Tanium has been registered with all of the TCP ports required for functionality to include (but not limited to) TCP 17472, 17477, 17440, 17441, 443, and 1433.

If any TCP ports are being used on the Tanium Server that have been deemed as restricted by the PPSM CAL, this is a finding.

Remediation:

Submit a formal request to have the Tanium communication ports evaluated and added to the PPSM CAL.

Additional Information:

CCI-000382

Configure the system to prohibit or restrict the use of organization-defined prohibited or restricted functions, system ports, protocols, software, and/or services.

- NIST SP 800-53::CM-7
- NIST SP 800-53A::CM-7.1 (iii)
- NIST SP 800-53 Revision 4::CM-7 b
- NIST SP 800-53 Revision 5::CM-7 b

1.73 TANS-SV-000020 (Manual)

Profile Applicability:

- SEVERITY: CAT II

Description:

The Tanium Server certificates must have Extended Key Usage entries for the serverAuth object TLS Web Server Authentication and the clientAuth object TLS Web Client Authentication.

```
GROUP ID: V-253851
RULE ID: SV-253851r842581
```

Rationale:

Restricting this setting limits the user's ability to change their password. Passwords must be changed at specific policy-based intervals; however, if the application allows the user to immediately and continually change their password, it could be changed repeatedly in a short period of time to defeat the organization's policy regarding password reuse.

Audit:

1. Access the Tanium application server interactively.
2. Log on to the server with an account that has administrative privileges.
3. Navigate to Program Files >> Tanium >> Tanium Server.
4. Locate the `SOAPServer.crt` file.
5. Double-click the file to open the certificate.
6. Select the "Details" tab.
7. Scroll down through the details to find and select the "Enhanced Key Usage" field.

If there is no "Enhanced Key Usage" field, this is a finding.

In the bottom screen, verify "Server Authentication" and "Client Authentication" are both identified.

If "Server Authentication" and "Client Authentication" are not both identified, this is a finding.

Remediation:

Request or regenerate the certificate being used to include both the "Server Authentication" and "Client Authentication" objects.

Additional Information:

CCI-000185

For public key-based authentication, validate certificates by constructing and verifying a certification path to an accepted trust anchor including checking certificate status information.

- NIST SP 800-53::IA-5 (2)
- NIST SP 800-53A::IA-5 (2).1
- NIST SP 800-53 Revision 4::IA-5 (2) (a)
- NIST SP 800-53 Revision 5::IA-5 (2) (b) (1)

1.74 TANS-SV-000024 (Manual)

Profile Applicability:

- SEVERITY: CAT II

Description:

The Tanium Server directory must be restricted with appropriate permissions.

```
GROUP ID: V-253852
RULE ID: SV-253852r850167
```

Rationale:

Discretionary Access Control (DAC) is based on the notion that individual users are "owners" of objects and therefore have discretion over who should be authorized to access the object and in which mode (e.g., read or write). Ownership is usually acquired as a consequence of creating the object or via specified ownership assignment. DAC allows the owner to determine who will have access to objects they control. An example of DAC includes user-controlled file permissions.

When DAC policies are implemented, subjects are not constrained with regard to what actions they can take with information for which they have already been granted access. Thus, subjects that have been granted access to information are not prevented from passing (i.e., the subjects have the discretion to pass) the information to other subjects or objects.

A subject that is constrained in its operation by Mandatory Access Control policies is still able to operate under the less rigorous constraints of this requirement. Thus, while Mandatory Access Control imposes constraints preventing a subject from passing information to another subject operating at a different sensitivity level, this requirement permits the subject to pass the information to any subject at the same sensitivity level.

The policy is bounded by the information system boundary. Once the information is passed outside of the control of the information system, additional means may be required to ensure the constraints remain in effect. While the older, more traditional definitions of DAC require identity-based access control, that limitation is not required for this use of DAC.

Audit:

1. Access the Tanium Server.
2. Log on to the server with an account that has administrative privileges.
3. Open an Explorer window.
4. Navigate to Program Files >> Tanium.
5. Right-click the "Tanium Server" folder.
6. Select "Properties".
7. Select the "Security" tab.
8. Click the "Advanced" button.

- Validate the owner of the "Tanium Server" folder is the service account [Tanium service account].
- Validate the [Tanium service account] has full permissions to the "Tanium Server" folder.
- Validate the [Tanium Admins] group has full permissions to the "Tanium Server" folder.
- Validate Users have no permissions to the "Tanium Server" folder.

If any accounts other than the [Tanium service account] and the [Tanium Admins] group have any permission to the "Tanium Server" folder, this is a finding.

If the [Tanium service account] is not the owner of the "Tanium Server" folder, this is a finding.

Remediation:

1. Access the Tanium Server.
2. Log on to the server with an account that has administrative privileges.
3. Open an Explorer window.
4. Navigate to Program Files >> Tanium.
5. Right-click the "Tanium Server" folder.
6. Select "Properties".
7. Select the "Security" tab.
8. Click the "Advanced" button.
9. Disable folder inheritance.
10. Change the owner of the directory to the service account [Tanium service account].
11. Remove User permissions.
12. Give [Tanium service account] full permissions.
13. Give [Tanium Admins] group full permissions.

Additional Information:

CCI-002165

Enforce organization-defined discretionary access control policies over defined subjects and objects.

- NIST SP 800-53 Revision 4::AC-3 (4)
- NIST SP 800-53 Revision 5::AC-3 (4)

1.75 TANS-SV-000025 (Manual)

Profile Applicability:

- SEVERITY: CAT II

Description:

The Tanium Server http directory and subdirectories must be restricted with appropriate permissions.

```
GROUP ID: V-253853
RULE ID: SV-253853r850167
```

Rationale:

Discretionary Access Control (DAC) is based on the notion that individual users are "owners" of objects and therefore have discretion over who should be authorized to access the object and in which mode (e.g., read or write). Ownership is usually acquired as a consequence of creating the object or via specified ownership assignment. DAC allows the owner to determine who will have access to objects they control. An example of DAC includes user-controlled file permissions.

When DAC policies are implemented, subjects are not constrained with regard to what actions they can take with information for which they have already been granted access. Thus, subjects that have been granted access to information are not prevented from passing (i.e., the subjects have the discretion to pass) the information to other subjects or objects.

A subject that is constrained in its operation by Mandatory Access Control policies is still able to operate under the less rigorous constraints of this requirement. Thus, while Mandatory Access Control imposes constraints preventing a subject from passing information to another subject operating at a different sensitivity level, this requirement permits the subject to pass the information to any subject at the same sensitivity level.

The policy is bounded by the information system boundary. Once the information is passed outside of the control of the information system, additional means may be required to ensure the constraints remain in effect. While the older, more traditional definitions of DAC require identity-based access control, that limitation is not required for this use of DAC.

Audit:

1. Access the Tanium Server.
2. Log on to the server with an account that has administrative privileges.
3. Open an Explorer window.
4. Navigate to Program Files >> Tanium >> Tanium Server.
5. Right-click the "Tanium Server\http" folder.
6. Select "Properties".
7. Select the "Security" tab.

8. Click the "Advanced" button.
    - Validate Folder Inheritance is disabled.
    - Validate the owner of the directory is the [Tanium service account].
    - Validate the [Tanium Admins] group has full permissions.
    - Validate System has Read-Only permissions.
9. Right-click the `Tanium Server\http\libraries` folder.
10. Select the "Security" tab.
11. Click the "Advanced" button.
    - Validate Folder Inheritance is disabled.
    - Validate the owner of the directory is the [Tanium service account].
    - Validate System has Read-Only permissions.
    - Validate the [Tanium service account] has Read-Only permissions.
    - Validate the [Tanium Admins] group has full permissions.
12. Right-click the `Tanium Server\http\taniumjs` folder.
13. Select the "Security" tab.
14. Click the "Advanced" button.
    - Validate Folder Inheritance is disabled.
    - Validate the owner of the directory is the [Tanium service account].
    - Validate System has "Read-Only" permissions.
    - Validate the [Tanium service account] has "Read-Only" permissions.
    - Validate the [Tanium Admins] group has full permissions.
15. Right-click the `Tanium Server\http\tux` folder.
16. Select the "Security" tab.
17. Click the "Advanced" button.
    - Validate Folder Inheritance is disabled.
    - Validate the owner of the directory is the [Tanium service account].
    - Validate System has "Read-Only" permissions.
    - Validate the [Tanium service account] has "Read Only" permissions.
    - Validate the [Tanium Admins] group has full permissions.
18. Right-click the `Tanium Server\http\tux-console` folder.
19. Select the "Security" tab.
20. Click the "Advanced" button.
    - Validate Folder Inheritance is disabled.
    - Validate the owner of the directory is the [Tanium service account].
    - Validate System has "Read-Only" permissions.
    - Validate the [Tanium service account] has "Read-Only" permissions.
    - Validate the [Tanium Admins] group has full permissions.
21. Right-click the Tanium Server\Logs folder.
22. Select "Properties".
23. Select the "Security" tab.
24. Click the "Advanced" button.
    - Validate Folder Inheritance is disabled.
    - Validate the owner of the directory is the [Tanium service account].
    - Validate the [Tanium Service Account] has only "Modify" permissions.
    - Validate the [Tanium Admins] group has full permissions.
25. Right-click the Tanium Server\TDL_Logs folder.

26. Select "Properties".
27. Select the "Security" tab.
28. Click the "Advanced" button.
    - Validate Folder Inheritance is disabled.
    - Validate the owner of the directory is the [Tanium service account].
    - Validate the [Tanium Service Account] has only "Modify" permissions.
    - Validate the [Tanium Admins] group has full permissions.
29. Right-click the Tanium Server\Certs folder.
30. Select "Properties".
31. Select the "Security" tab.
32. Click the "Advanced" button.
    - Validate Folder Inheritance is disabled.
    - Validate the owner of the directory is the [Tanium service account].
    - Validate System has "Read-Only" permissions.
    - Validate the [Tanium Admins] group has full permissions.
33. Navigate to Tanium Server >> Certs.
34. For the following files, verify System and [Tanium Service Account] have "Read-Only" permissions:

```
installedcacert.crt
installed-server.crt
installed-server.key
SOAPServer.crt
SOAPServer.key
```

35. Right-click the `Tanium Server\content_public_keys` folder.
36. Select "Properties".
37. Select the "Security" tab.
38. Click the "Advanced" button.
    - Validate Folder Inheritance is disabled.
    - Validate the owner of the directory is the [Tanium service account].
    - Validate System has "Read-Only" permissions.
    - Validate the [Tanium Service Account] has "Read-Only" permissions.
    - Validate the [Tanium Admins] group has full permissions.

If any of the above permissions are not configured correctly, this is a finding.

Remediation:

1. Access the Tanium Server.
2. Log on to the server with an account that has administrative privileges.
3. Open an Explorer window.
4. Navigate to Program Files >> Tanium >> Tanium Server.
5. Right-click the "Tanium Server\http folder.
6. Select "Properties".
7. Select the "Security" tab.
8. Click the "Advanced" button.

9. Verify/Disable folder inheritance.
10. Change/verify the owner of the directory to the [Tanium service account].
11. Change/verify the [Tanium Admins] group has full permissions.
12. Reduce System to "Read-Only" permissions.
13. Right-click the `Tanium Server\http\libraries` folder.
14. Select the "Security" tab.
15. Click the "Advanced" button.
16. Verify/disable folder inheritance.
17. Change/verify the owner of the directory to the [Tanium service account].
18. Reduce System to "Read-Only" permissions.
19. Reduce [Tanium service account] to "Read-Only" permissions.
20. Change/verify the [Tanium Admins] group has full permissions.
21. Right-click the `Tanium Server\http\taniumjs` folder.
22. Select the "Security" tab.
23. Click the "Advanced" button.
24. Verify/disable folder inheritance.
25. Change/verify the owner of the directory to the [Tanium service account].
26. Reduce System to "Read-Only" permissions.
27. Reduce [Tanium service account] to "Read-Only" permissions.
28. Change/verify the [Tanium Admins] group has full permissions.
29. Right-click the `Tanium Server\http\tux` folder.
30. Select the "Security" tab.
31. Click the "Advanced" button.
32. Verify/disable folder inheritance.
33. Change/verify the owner of the directory to the [Tanium service account].
34. Reduce System to "Read-Only" permissions.
35. Reduce [Tanium service account] to "Read-Only" permissions.
36. Change/verify the [Tanium Admins] group has full permissions.
37. Right-click the `Tanium Server\http\tux-console` folder.
38. Select the "Security" tab.
39. Click the "Advanced" button.
40. Verify/disable folder inheritance.
41. Change/verify the owner of the directory to the [Tanium service account].
42. Reduce System to "Read-Only" permissions.
43. Reduce [Tanium service account] to "Read-Only" permissions.
44. Change/verify the [Tanium Admins] group has full permissions.
45. Right-click the `Tanium Server\Logs` folder.
46. Select the "Security" tab.
47. Click the "Advanced" button.
48. Verify/disable folder inheritance.
49. Change/verify the owner of the directory to the [Tanium service account].
50. Reduce [Tanium service account] to "Modify" permissions.
51. Change/verify the [Tanium Admins] group has full permissions.
52. Right-click the `Tanium Server\http\TDL_Logs` folder.
53. Select the "Security" tab.
54. Click the "Advanced" button.

55. Verify/disable folder inheritance.
56. Change/verify the owner of the directory to the [Tanium service account].
57. Reduce [Tanium service account] to "Modify" permissions.
58. Change/verify the [Tanium Admins] group has full permissions.
59. Right-click the "Tanium Server\Certs" folder.
60. Select the "Security" tab.
61. Click the "Advanced" button.
62. Verify/disable folder inheritance.
63. Change/verify the owner of the directory to the [Tanium service account].
64. Reduce System to "Read-Only" permissions.
65. Change/verify the [Tanium Admins] group has full permissions.
66. Navigate to Tanium Server >> Certs.
67. For the following files, verify/reduce System and [Tanium Service Account] to "Read-Only" permissions:

```
installedcacert.crt
installed-server.crt
installed-server.key
SOAPServer.crt
SOAPServer.key
```

68. Right-click the `Tanium Server\content_public_keys` folder.
69. Select the "Security" tab.
70. Click the "Advanced" button.
71. Verify/disable folder inheritance.
72. Change/verify the owner of the directory to the [Tanium service account].
73. Reduce System to "Read-Only" permissions - apply to child objects.
74. Reduce [Tanium service account] to "Read-Only" permissions - apply to child objects.
75. Change/verify the [Tanium Admins] group has full permissions.

Additional Information:

CCI-002165

Enforce organization-defined discretionary access control policies over defined subjects and objects.

- NIST SP 800-53 Revision 4::AC-3 (4)
- NIST SP 800-53 Revision 5::AC-3 (4)

1.76 TANS-SV-000026 (Manual)

Profile Applicability:

- SEVERITY: CAT II

Description:

The permissions on the Tanium Server registry keys must be restricted to only the Tanium service account and the [Tanium Admins] group.

```
GROUP ID: V-253854
RULE ID: SV-253854r850167
```

Rationale:

Discretionary Access Control (DAC) is based on the notion that individual users are "owners" of objects and therefore have discretion over who should be authorized to access the object and in which mode (e.g., read or write). Ownership is usually acquired as a consequence of creating the object or via specified ownership assignment. DAC allows the owner to determine who will have access to objects they control. An example of DAC includes user-controlled file permissions.

When DAC policies are implemented, subjects are not constrained with regard to what actions they can take with information for which they have already been granted access. Thus, subjects that have been granted access to information are not prevented from passing (i.e., the subjects have the discretion to pass) the information to other subjects or objects.

A subject that is constrained in its operation by Mandatory Access Control policies is still able to operate under the less rigorous constraints of this requirement. Thus, while Mandatory Access Control imposes constraints preventing a subject from passing information to another subject operating at a different sensitivity level, this requirement permits the subject to pass the information to any subject at the same sensitivity level.

The policy is bounded by the information system boundary. Once the information is passed outside of the control of the information system, additional means may be required to ensure the constraints remain in effect. While the older, more traditional definitions of DAC require identity-based access control, that limitation is not required for this use of DAC.

Audit:

1. Access the Tanium Server.
2. Log on to the server with an account that has administrative privileges.
3. Run regedit as Administrator.
4. Navigate to `HKEY_LOCAL_MACHINE >> SOFTWARE >> Wow6432Node >> Tanium >> Tanium Server`.
5. Right-click "Tanium Server".
6. Select "Permissions".

7. Click the "Security" tab.
8. Click the "Advanced" button.
    - Validate the [Tanium service account] has full permissions.
    - Validate the [Tanium Admins] group has full permissions.
    - Validate the SYSTEM account has full permissions.
    - Validate the User accounts do not have any permissions.

If any other account has full permissions and/or the User account has any permissions, this is a finding.

Remediation:

1. Access the Tanium Server.
2. Log on to the server with an account that has administrative privileges.
3. Run regedit as Administrator.
4. Navigate to `HKEY_LOCAL_MACHINE >> SOFTWARE >> Wow6432Node >> Tanium >> Tanium Server`.
5. Right-click "Tanium Server".
6. Select "Properties".
7. Click the "Security" tab.
8. Click the "Advanced" button.
9. Provide the [Tanium service account] with full permissions.
10. Provide the [Tanium Admins] group with full permissions.
11. Reduce permissions for any other accounts with full permissions.
12. Remove permissions for User accounts.

Additional Information:

CCI-002165

Enforce organization-defined discretionary access control policies over defined subjects and objects.

- NIST SP 800-53 Revision 4::AC-3 (4)
- NIST SP 800-53 Revision 5::AC-3 (4)

1.77 TANS-SV-000027 (Manual)

Profile Applicability:

- SEVERITY: CAT II

Description:

The Tanium Server Logs and TDL_Logs directories must be restricted with appropriate permissions.

```
GROUP ID: V-253855
RULE ID: SV-253855r850167
```

Rationale:

Discretionary Access Control (DAC) is based on the notion that individual users are "owners" of objects and therefore have discretion over who should be authorized to access the object and in which mode (e.g., read or write). Ownership is usually acquired as a consequence of creating the object or via specified ownership assignment. DAC allows the owner to determine who will have access to objects they control. An example of DAC includes user-controlled file permissions.

When discretionary access control policies are implemented, subjects are not constrained with regard to what actions they can take with information for which they have already been granted access. Thus, subjects that have been granted access to information are not prevented from passing (i.e., the subjects have the discretion to pass) the information to other subjects or objects.

A subject that is constrained in its operation by Mandatory Access Control policies is still able to operate under the less rigorous constraints of this requirement. Thus, while Mandatory Access Control imposes constraints preventing a subject from passing information to another subject operating at a different sensitivity level, this requirement permits the subject to pass the information to any subject at the same sensitivity level.

The policy is bounded by the information system boundary. Once the information is passed outside of the control of the information system, additional means may be required to ensure the constraints remain in effect. While the older, more traditional definitions of DAC require identity-based access control, that limitation is not required for this use of DAC.

Audit:

1. Access the Tanium Server.
2. Log on to the server with an account that has administrative privileges.
3. Open an Explorer window.
4. Navigate to Program Files >> Tanium >> Tanium Server.
5. Right-click the `Logs` folder.
6. Select "Properties".
7. Click the "Security" tab.

8. Click the "Advanced" button.
    - Validate the owner of the directory is the [Tanium service account].
    - Validate the [Tanium service account] privileges is the only account with modify permissions on the directory.
    - Validate the [Tanium Administrators] group has full permissions on the directory.
9. Right-click the `TDL_Logs` folder.
10. Select "Properties".
11. Click the "Security" tab.
12. Click the "Advanced" button.
    - Validate the owner of the directory is the [Tanium service account].
    - Validate the [Tanium service account] privileges is the only account with modify permissions on the directory.
    - Validate the [Tanium Administrators] group has full permissions on the directory.

If any of the specified permissions are not set as required, this is a finding.

Remediation:

1. Access the Tanium Server.
2. Log on to the server with an account that has administrative privileges.
3. Open an Explorer window.
4. Navigate to Program Files >> Tanium >> Tanium Server.
5. Right-click the `Logs` folder.
6. Select "Properties".
7. Click the "Security" tab.
8. Click the "Advanced" button.
9. Disable folder inheritance.
10. Change/verify the owner of the directory to the [Tanium service account].
11. Reduce [Tanium service account] privileges to modify permissions on the directory.
12. Ensure [Tanium Admins] group has full permissions on the directory.
13. Right-click the `TDL_Logs` folder.
14. Select "Properties".
15. Click the "Security" tab.
16. Click the "Advanced" button.
17. Disable folder inheritance.
18. Change/verify the owner of the directory to the [Tanium service account].
19. Reduce [Tanium service account] privileges to modify permissions on the directory.
20. Ensure [Tanium Admins] group has full permissions on the directory.

Additional Information:

CCI-002165

Enforce organization-defined discretionary access control policies over defined subjects and objects.

- NIST SP 800-53 Revision 4::AC-3 (4)
- NIST SP 800-53 Revision 5::AC-3 (4)

1.78 TANS-SV-000031 (Manual)

Profile Applicability:

- SEVERITY: CAT II

Description:

Firewall rules must be configured on the Tanium module server to allow Server-to-Module Server communications from the Tanium Server.

```
GROUP ID: V-253856
RULE ID: SV-253856r850218
```

Rationale:

The Tanium Module Server is used to extend the functionality of Tanium through the use of various workbenches. The Tanium Module Server requires communication with the Tanium Server on port 17477. Without a proper connection from the Tanium Server to the Tanium Module Server, access to the system capabilities could be denied.

For more information, refer to https://docs.tanium.com/platform_install/platform_install/reference_network_ports.html.

Audit:

Consult with the Tanium system administrator to verify which firewall is being used as a host-based firewall on the Tanium Module Server.

1. Access the Tanium Server.
2. Log on to the server with an account that has administrative privileges.
3. Access the host-based firewall configuration on the Tanium Module Server.
4. Validate a rule exists for the following:

Port Needed: Tanium Server to Tanium Module Server over TCP port 17477.

If a host-based firewall rule does not exist to allow TCP port 17477 from the Tanium Server to the Tanium Module Server, this is a finding.

Consult with the network firewall administrator and validate rules exist for the following:

Allow TCP traffic on port 17477 from the Tanium Server to the Tanium Module Server.

If a network firewall rule does not exist to allow TCP traffic on port 17477 from the Tanium Server to the Tanium Module Server, this is a finding.

Remediation:

1. Configure host-based firewall rules on the Tanium Module Server to include the following required traffic:

Allow TCP traffic on port 17477 from the Tanium Server to the Tanium Module Server.

2. Configure the network firewall to allow the above traffic.

Additional Information:

CCI-001762

Disable or remove organization-defined functions, ports, protocols, software, and services within the system deemed to be unnecessary and/or nonsecure.

- NIST SP 800-53 Revision 4::CM-7 (1) (b)
- NIST SP 800-53 Revision 5::CM-7 (1) (b)

1.79 TANS-SV-000032 (Manual)

Profile Applicability:

- SEVERITY: CAT II

Description:

Firewall rules must be configured on the Tanium Server for Server-to-Module Server communications.

```
GROUP ID: V-253857
RULE ID: SV-253857r850218
```

Rationale:

The Tanium Module Server is used to extend the functionality of Tanium through the use of various workbenches. The Tanium Module Server requires communication with the Tanium Server on port 17477. Without a proper connection from the Tanium Server to the Tanium Module Server, access to the system capabilities could be denied.

For more information, refer to https://docs.tanium.com/platform_install/platform_install/reference_network_ports.html.

Audit:

Consult with the Tanium system administrator to verify which firewall is being used as a host-based firewall on the Tanium Server.

1. Access the Tanium Server.
2. Log on to the server with an account that has administrative privileges.
3. Access the host-based firewall configuration on the Tanium Server.
4. Validate a rule exists for the following:

Port Needed: Tanium Server to Tanium Module Server over TCP port 17477.

If a host-based firewall rule does not exist to allow TCP port 17477 from the Tanium Server to the Tanium Module Server, this is a finding.

Consult with the network firewall administrator and validate rules exist for the following:

Allow TCP traffic on port 17477 from the Tanium Server to the Tanium Module Server.

If a network firewall rule does not exist to allow TCP traffic on port 17477 from the Tanium Server to the Tanium Module Server, this is a finding.

Remediation:

1. Configure host-based firewall rules on the Tanium Server to allow the following required traffic:

Allow TCP traffic on port 17477 to the Tanium Module Server from the Tanium Server.

2. Configure the network firewall to allow the above traffic.

Additional Information:

CCI-001762

Disable or remove organization-defined functions, ports, protocols, software, and services within the system deemed to be unnecessary and/or nonsecure.

- NIST SP 800-53 Revision 4::CM-7 (1) (b)
- NIST SP 800-53 Revision 5::CM-7 (1) (b)

1.80 TANS-SV-000033 (Manual)

Profile Applicability:

- SEVERITY: CAT II

Description:

Firewall rules must be configured on the Tanium Server for Server-to-Zone Server communications.

```
GROUP ID: V-253858
RULE ID: SV-253858r850218
```

Rationale:

If using the Tanium Zone Server to proxy traffic from Tanium-managed computers on less trusted network segments to the Tanium Server on the core network, the Tanium Zone Server Hub, typically installed to the Tanium Server device, must be able to connect to the Zone Server(s) in the DMZ. This is the only configuration that requires allowing outbound traffic on port 17472 from the Tanium Server device. The ZoneServerList.txt configuration file in the Tanium Zone Server Hub's installation folder identifies the addresses of the destination Zone Servers. Refer to the Zone Server Configuration page for more details.

Port Needed: Tanium Server to Zone Server over TCP port 17472.

Network firewall rules:

Allow TCP traffic on port 17472 from the Zone Server Hub, usually the Tanium Server device, to the destination DMZ devices(s) hosting the Zone Server(s).

Endpoint firewall rules: For additional security, configure the following endpoint firewall rules:

Allow TCP traffic outbound on port 17472 from only the Zone Server Hub process running on the Tanium Server device.

Allow TCP traffic inbound on port 17472 to only the Zone Server process running on the designated Zone Server device(s).

For more information, refer to ttps://docs.tanium.com/platform_install/platform_install/reference_network_ports.html.

Audit:

Note: If a Zone Server is not being used, this is not applicable.

Consult with the Tanium system administrator to verify which firewall is being used as a host-based firewall on the Tanium Server.

1. Access the Tanium Server.

2. Log on to the server with an account that has administrative privileges.
3. Access the host-based firewall configuration on the Tanium Server.
4. Validate a rule exists for the following:

Port Needed: Tanium Server to Zone Server over TCP port 17472.

Note: By default, the Zone Server uses 17472 for traffic from Zone Server Hubs and Tanium Clients. However, as a best practice to improve the security of the Zone Server, different ports can be configured for the hubs and clients.

If a host-based firewall rule does not exist to allow TCP port 17472 or other defined port, bidirectionally, from the Tanium Server to the Tanium Zone Server, this is a finding.

Remediation:

1. Configure host-based firewall rules on the Tanium Zone server to include the following required traffic:

   Allow Tanium Server to Zone Server over TCP port 17472.

2. Configure the network firewall to allow the above traffic.

Note: By default, the Zone Server uses 17472 for traffic from Zone Server Hubs and Tanium Clients. However, as a best practice to improve the security of the Zone Server, different ports can be configured for the hubs and clients.

Additional Information:

CCI-001762

Disable or remove organization-defined functions, ports, protocols, software, and services within the system deemed to be unnecessary and/or nonsecure.

- NIST SP 800-53 Revision 4::CM-7 (1) (b)
- NIST SP 800-53 Revision 5::CM-7 (1) (b)

1.81 TANS-SV-000035 (Manual)

Profile Applicability:

- SEVERITY: CAT II

Description:

The SSLHonorCipherOrder must be configured to disable weak encryption algorithms on the Tanium Server.

```
GROUP ID: V-253859
RULE ID: SV-253859r850365
```

Rationale:

Use of weak or untested encryption algorithms undermines the purposes of using encryption to protect data. The application must implement cryptographic modules adhering to the higher standards approved by the federal government since this provides assurance they have been tested and validated.

Audit:

1. Access the Tanium Server.
2. Log on to the server with an account that has administrative privileges.
3. Access the server's registry by typing: `regedit <enter>`.
4. Navigate to `HKEY_LOCAL_MACHINE >> SOFTWARE >> Wow6432Node >> Tanium >> Tanium Server`.
5. Verify the existence of a `DWORD SSLHonorCipherOrder` with a value of `0x00000001 (hex)`.

If the `DWORD SSLHonorCipherOrder` does not exist with a value of `0x00000001 (hex)`, this is a finding.

Remediation:

1. Access the Tanium Server.
2. Log on to the server with an account that has administrative privileges.
3. Access the server's registry by typing: regedit .
4. Navigate to `HKEY_LOCAL_MACHINE >> SOFTWARE >> Wow6432Node >> Tanium >> Tanium Server`.
5. Add or modify the `DWORD SSLHonorCipherOrder` to have a value of `0x00000001 (hex)`.

Additional Information:

CCI-002450

Implement organization-defined types of cryptography for each specified cryptography use.

- NIST SP 800-53 Revision 4::SC-13
- NIST SP 800-53 Revision 5::SC-13 b

1.82 TANS-SV-000036 (Manual)

Profile Applicability:

- SEVERITY: CAT II

Description:

The Tanium Server certificate must be signed by a DoD certificate authority (CA).

```
GROUP ID: V-253860
RULE ID: SV-253860r850257
```

Rationale:

The Tanium Server has the option to use a "self-signed" certificate or a trusted CA signed certificate for SSL connections. During evaluations of Tanium in lab settings, customers often conclude that a "self-signed" certificate is an acceptable risk. However, in production environments it is critical that an SSL certificate signed by a trusted CA be used on the Tanium Server in lieu of an untrusted and insecure "self-signed" certificate.

Audit:

1. Using a web browser on a system that has connectivity to the Tanium application, access the Tanium application web user interface (UI) and log on with multifactor authentication.
2. When connected, review the certificate for the Tanium Server as noted below.
3. In the web browser, view the certificate and verify it was issued by a DoD root CA. Also verify the certification path's top level is a DoD root CA.

If the certificate authority is not DoD Root CA, this is a finding.

Remediation:

Request or regenerate the certificate from a DoD root CA.

Additional Information:

CCI-002470

Only allow the use of organization-defined certificate authorities for verification of the establishment of protected sessions.

- NIST SP 800-53 Revision 4::SC-23 (5)
- NIST SP 800-53 Revision 5::SC-23 (5)

1.83 TANS-SV-000040 (Manual)

Profile Applicability:

- SEVERITY: CAT II

Description:

Tanium Server directory and subsequent files must be excluded from On-Access scan.

```
GROUP ID: V-253861
RULE ID: SV-253861r842611
```

Rationale:

Similar to any other host-based applications, the Tanium Server is subject to the restrictions other system-level software may place on an operating environment. Antivirus, intrusion prevention system (IPS), encryption, or other security and management stack software may disallow the Tanium Server from working as expected.

For more information, refer to:
https://docs.tanium.com/platform_deployment_reference/platform_deployment_reference/security_exceptions.html?Highlight=exclusion

Audit:

Review the settings of the antivirus software.

Validate exclusions exist that exclude the Tanium Server directory and subsequent file interactions from On-Access scans.

If exclusions do not exist, this is a finding.

Remediation:

Implement exclusion policies within the antivirus software solution to exclude the On-Access scanning of Tanium Server directory and subsequent file interactions.

Additional Information:

CCI-000366

Implement the security configuration settings.

- NIST SP 800-53::CM-6 b
- NIST SP 800-53A::CM-6.1 (iv)
- NIST SP 800-53 Revision 4::CM-6 b
- NIST SP 800-53 Revision 5::CM-6 b

1.84 TANS-SV-000044 (Manual)

Profile Applicability:

- SEVERITY: CAT II

Description:

The SSLCipherSuite must be configured to disable weak encryption algorithms on the Tanium Server.

```
GROUP ID: V-253862
RULE ID: SV-253862r850365
```

Rationale:

Use of weak or untested encryption algorithms undermines the purposes of using encryption to protect data. The application must implement cryptographic modules adhering to the higher standards approved by the federal government since this provides assurance they have been tested and validated.

Audit:

1. Access the Tanium Server.
2. Log on to the server with an account that has administrative privileges.
3. Access the server's registry by typing: `regedit`.
4. Click "Enter".
5. Navigate to `HKEY_LOCAL_MACHINE >> SOFTWARE >> Wow6432Node >> Tanium >> Tanium Server`.
6. Verify the existence of the string `SSLCipherSuite` with a value of:

```
ECDHE-RSA-AES256-GCM-SHA384:ECDHE-RSA-AES128-GCM-SHA256:ECDHE-RSA-AES256-
SHA384:ECDHE-RSA-AES128-SHA256:!aNULL:!eNULL:!EXPORT:!DES:!RC4:!MD5:!PSK
```

If the string "SSLCipherSuite" does not exist with the appropriate list values, this is a finding.

Remediation:

1. Access the Tanium Server.
2. Log on to the server with an account that has administrative privileges.
3. Access the server's registry by typing: `regedit <enter>`.
4. Navigate to `HKEY_LOCAL_MACHINE >> SOFTWARE >> Wow6432Node >> Tanium >> Tanium Server`.
5. Add a new string `(REG_SZ)` or modify the string `SSLCipherSuite` to have a value of:

```
ECDHE-RSA-AES256-GCM-SHA384:ECDHE-RSA-AES128-GCM-SHA256:ECDHE-RSA-AES256-
SHA384:ECDHE-RSA-AES128-SHA256:!aNULL:!eNULL:!EXPORT:!DES:!RC4:!MD5:!PSK
```

Additional Information:

CCI-002450

Implement organization-defined types of cryptography for each specified cryptography use.

- NIST SP 800-53 Revision 4::SC-13
- NIST SP 800-53 Revision 5::SC-13 b

1.85 TANS-SV-000045 (Manual)

Profile Applicability:

- SEVERITY: CAT II

Description:

The Tanium "max_soap_sessions_total" setting must be explicitly enabled to limit the number of simultaneous sessions.

```
GROUP ID: V-253863
RULE ID: SV-253863r842617
```

Rationale:

Application management includes the ability to control the number of users and user sessions that utilize an application. Limiting the number of allowed users and sessions per user is helpful in limiting risks related to denial-of-service attacks.

This requirement may be met via the application or by using information system, session control provided by a web server with specialized session management capabilities. If it has been specified that this requirement will be handled by the application, the capability to limit the maximum number of concurrent single user sessions must be designed and built into the application.

This requirement addresses concurrent sessions for information system accounts and does not address concurrent sessions by single users via multiple system accounts. The maximum number of concurrent sessions should be defined based on mission needs and the operational environment for each system.

Audit:

1. Using a web browser on a system that has connectivity to the Tanium application, access the Tanium application web user interface (UI) and log on with multifactor authentication.
2. Click "Administration" on the top navigation banner.
3. Under "Configuration", select "Platform Settings".
4. In the "Filter items" search box, type `max_soap_sessions_total`.
5. Click "Enter".

If no results are returned, this is a finding.

If results are returned for `max_soap_sessions_total` but the value does not follow `{(Number of Users) * 1024}` formula, this is a finding.

Remediation:

1. Using a web browser on a system that has connectivity to the Tanium application, access the Tanium application web UI and log on with multifactor authentication.
2. Click "Administration" on the top navigation banner.
3. Under "Configuration", select "Platform Settings".
4. Click "Create Setting".
5. Select `Server` box for `Setting Type`.
6. In "Create Platform Setting" dialog box, enter `max_soap_sessions_total` for `Name`.
7. Select `Numeric` radio button from `Value Type`.
8. Use this formula for determining `"Setting Value": {(Number of Users) * 1024 = max_soap_sessions_total}`
9. Click "Save".
10. Add this setting to the system documentation for validation.

Additional Information:

CCI-000054

Limit the number of concurrent sessions for each organization-defined account and/or account type to an organization-defined number.

- NIST SP 800-53::AC-10
- NIST SP 800-53A::AC-10.1 (ii)
- NIST SP 800-53 Revision 4::AC-10
- NIST SP 800-53 Revision 5::AC-10

1.86 TANS-SV-000046 (Manual)

Profile Applicability:

- SEVERITY: CAT II

Description:

The Tanium "max_soap_sessions_per_user" setting must be explicitly enabled to limit the number of simultaneous sessions.

```
GROUP ID: V-253864
RULE ID: SV-253864r842620
```

Rationale:

Application management includes the ability to control the number of users and user sessions that utilize an application. Limiting the number of allowed users and sessions per user is helpful in limiting risks related to denial-of-service attacks.

This requirement may be met via the application or by using information system session control provided by a web server with specialized session management capabilities. If it has been specified that this requirement will be handled by the application, the capability to limit the maximum number of concurrent single user sessions must be designed and built into the application.

This requirement addresses concurrent sessions for information system accounts and does not address concurrent sessions by single users via multiple system accounts. The maximum number of concurrent sessions should be defined based on mission needs and the operational environment for each system.

Audit:

1. Using a web browser on a system that has connectivity to the Tanium application, access the Tanium application web user interface (UI) and log on with multifactor authentication.
2. Click "Administration" on the top navigation banner.
3. Under "Configuration", select "Platform Settings".
4. In the "Filter items" search box, type `max_soap_sessions_per_user`.
5. Click "Enter".

If no results are returned, this is a finding.

If results are returned for `max_soap_sessions_per_user` but the value is not `1024`, this is a finding.

Remediation:

1. Using a web browser on a system that has connectivity to the Tanium application, access the Tanium application web UI and log on with multifactor authentication.
2. Click "Administration" on the top navigation banner.
3. Under "Configuration", select "Platform Settings".
4. Click "Create Setting".
5. Select `Server` box for `Setting Type`.
6. In "Create Platform Setting" dialog box, enter `max_soap_sessions_per_user` for `Name`.
7. Select `Numeric` radio button from `Value Type`.
8. Enter `1024` for the `Value:`.
9. Click "Save".
10. Add this setting to the system documentation for validation.

Additional Information:

CCI-000054

Limit the number of concurrent sessions for each organization-defined account and/or account type to an organization-defined number.

- NIST SP 800-53::AC-10
- NIST SP 800-53A::AC-10.1 (ii)
- NIST SP 800-53 Revision 4::AC-10
- NIST SP 800-53 Revision 5::AC-10

1.87 TANS-SV-000048 (Manual)

Profile Applicability:

- SEVERITY: CAT II

Description:

The Tanium documentation identifying recognized and trusted folders for Threat Response Local Directory Source must be maintained.

```
GROUP ID: V-253865
RULE ID: SV-253865r842623
```

Rationale:

Using trusted and recognized indicator of compromise (IOC) sources may detect and prevent systems from becoming compromised. An IOC stream is a series or stream of IOCs that are imported from a vendor based on a subscription service or manually downloaded and placed in a folder. Threat Response can be configured to retrieve the IOC content on a regularly scheduled basis. The items in an IOC stream can be manipulated separately after they are imported.

Audit:

Consult with the Tanium system administrator to review the documented list of folder maintainers for Threat Response Local Directory Source.

If the site does not leverage Local Directory Source to import IOCs, this finding is not applicable.

If the site does use Local Directory Source to import IOCs and the folder maintainers are not documented, this is a finding.

Remediation:

Prepare and maintain documentation identifying the Tanium Threat Response Local Directory Source maintainers.

Additional Information:

CCI-001414

Enforce approved authorizations for controlling the flow of information between connected systems based on organization-defined information flow control policies.

- NIST SP 800-53::AC-4
- NIST SP 800-53A::AC-4.1 (iii)
- NIST SP 800-53 Revision 4::AC-4
- NIST SP 800-53 Revision 5::AC-4

1.88 TANS-SV-000049 (Manual)

Profile Applicability:

- SEVERITY: CAT II

Description:

The Tanium Threat Response Local Directory Source must be configured to restrict access to only authorized maintainers of threat intel.

```
GROUP ID: V-253866
RULE ID: SV-253866r842626
```

Rationale:

Using trusted and recognized indicator of compromise (IOC) sources may detect and prevent systems from becoming compromised. An IOC stream is a series or stream of intel that is imported from a vendor based on a subscription service or manually downloaded and placed in a folder. Threat Response can be configured to retrieve the IOC content on a regularly scheduled basis. The items in an IOC stream can be manipulated separately after they are imported.

Audit:

Consult with the Tanium system administrator to determine if the Tanium Threat Response module is being used. If it is not, his finding is not applicable.

If the Local Directory Source type is being used, determine where they get their IOC stream.

1. Access the Tanium Module Server interactively.
2. Log on to the server with an account that has administrative privileges.
3. Open an Explorer window.
4. Navigate to Program Files >> Tanium >> Tanium Module Server >> services >> threat-response-files.
5. Right-click the folder and choose "Properties".
6. Select the "Security" tab.
7. Click the "Advanced" button.

If the accounts listed in the "Security" tab do not match the list of accounts in the Tanium documentation, this is a finding.

Remediation:

1. Access the Tanium Module Server interactively.
2. Log on to the server with an account that has administrative privileges.
3. Open an Explorer window.

4. Navigate to Program Files >> Tanium >> Tanium Module Server >> services >> threat-response-files.
5. Right-click the folder and choose "Properties".
6. Select the "Security" tab.
7. Click the "Advanced" button.

If the accounts listed in the "Security" tab do not match the list of accounts, with the exception of SYSTEM, remove the additionally listed accounts.

If the accounts listed in the "Security" tab are missing accounts from the documentation, with the exception of SYSTEM, add the additionally listed accounts with a minimum of READ permission.

Additional Information:

CCI-001414

Enforce approved authorizations for controlling the flow of information between connected systems based on organization-defined information flow control policies.

- NIST SP 800-53::AC-4
- NIST SP 800-53A::AC-4.1 (iii)
- NIST SP 800-53 Revision 4::AC-4
- NIST SP 800-53 Revision 5::AC-4

1.89 TANS-SV-000050 (Manual)

Profile Applicability:

- SEVERITY: CAT II

Description:

The Tanium documentation identifying recognized and trusted Security Content Automation Protocol (SCAP) sources must be maintained.

```
GROUP ID: V-253867
RULE ID: SV-253867r842629
```

Rationale:

SCAP XML documents validated by the National Institute of Standards and Technology (NIST) are provided from several possible sources such as DISA, NIST, and nongovernment entities. These documents are used as the basis of compliance definitions leveraged to automate compliance auditing of systems. These documents are updated on different frequencies and must be downloaded manually at regular intervals and imported in order to be current. Nonapproved SCAP definitions lead to a false sense of security when evaluating an enterprise environment.

Audit:

Consult with the Tanium system administrator to review the documented list of trusted SCAP sources.

If the site does not have the "Tanium Comply" module or does not use "Tanium Comply" for compliance validation, this finding is not applicable.

If the site does use Tanium Comply and the source for SCAP content is not documented, this is a finding.

Remediation:

If the site does not have the "Tanium Comply" module or does not use "Tanium Comply" for compliance validation, this finding is not applicable.

Prepare and maintain documentation identifying the source of SCAP sources that will be used by the "Tanium Comply" module.

Additional Information:

CCI-001414

Enforce approved authorizations for controlling the flow of information between connected systems based on organization-defined information flow control policies.

- NIST SP 800-53::AC-4

- NIST SP 800-53A::AC-4.1 (iii)
- NIST SP 800-53 Revision 4::AC-4
- NIST SP 800-53 Revision 5::AC-4

1.90 TANS-SV-000051 (Manual)

Profile Applicability:

- SEVERITY: CAT II

Description:

The Tanium documentation identifying recognized and trusted Open Vulnerability and Assessment Language (OVAL) feeds must be maintained.

```
GROUP ID: V-253868
RULE ID: SV-253868r842632
```

Rationale:

OVAL XML documents are provided from several possible sources such as the Community Intercomparison Suite (CIS) open-source repository and vendor/third-party paid repositories. These documents are used to automate the passive validation of vulnerabilities on systems and therefore require a reasonable level of confidence in their origin. Nonapproved OVAL definitions lead to a false sense of security when evaluating an enterprise environment.

Audit:

Consult with the Tanium system administrator to review the documented list of trusted OVAL feeds.

If the site does not have the "Tanium Comply" module or does not use "Tanium Comply" for passive vulnerability scanning, this finding is not applicable.

If the site does use "Tanium Comply" and the source for OVAL content is not documented, this is a finding.

Remediation:

If the site does not have the "Tanium Comply" module or does not use "Tanium Comply" for passive vulnerability scanning, this finding is not applicable.

Prepare and maintain documentation identifying the source of OVAL feeds that will be used by the "Tanium Comply" module.

Additional Information:

CCI-001414

Enforce approved authorizations for controlling the flow of information between connected systems based on organization-defined information flow control policies.

- NIST SP 800-53::AC-4
- NIST SP 800-53A::AC-4.1 (iii)

- NIST SP 800-53 Revision 4::AC-4
- NIST SP 800-53 Revision 5::AC-4

1.91 TANS-SV-000052 (Manual)

Profile Applicability:

- SEVERITY: CAT II

Description:

Tanium Comply must be configured to receive Security Content Automation Protocol (SCAP) content only from trusted sources.

```
GROUP ID: V-253869
RULE ID: SV-253869r842635
```

Rationale:

SCAP XML documents validated by the National Institute of Standards and Technology (NIST) are provided from several possible sources such as DISA, NIST, and other nongovernment entities. These documents are used as the basis of compliance definitions leveraged to automate compliance auditing of systems. These documents are updated on different frequencies and must be downloaded manually at regular intervals and imported in order to be current. Nonapproved SCAP definitions lead to a false sense of security when evaluating an enterprise environment.

Audit:

1. Using a web browser on a system that has connectivity to the Tanium application, access the Tanium application web user interface (UI) and log on with multifactor authentication.
2. Click "Modules" on the top banner of the console.
3. Click "Comply".
4. Click the menu on the left side of the interface. Under "Standards", click "Compliance".

Verify all imported compliance benchmarks are from a documented trusted source.

If any compliance benchmark is found that does not come from a documented trusted source, this is a finding.

Remediation:

1. Using a web browser on a system that has connectivity to the Tanium application, access the Tanium application web UI and log on with multifactor authentication.
2. Click "Modules" on the top banner of the console.
3. Click "Comply".
4. Click the menu on the left side of the interface. Under "Standards", click "Compliance".
5. Delete any compliance benchmarks that come from nontrusted sources.

Additional Information:

CCI-001414

Enforce approved authorizations for controlling the flow of information between connected systems based on organization-defined information flow control policies.

- NIST SP 800-53::AC-4
- NIST SP 800-53A::AC-4.1 (iii)
- NIST SP 800-53 Revision 4::AC-4
- NIST SP 800-53 Revision 5::AC-4

1.92 TANS-SV-000053 (Manual)

Profile Applicability:

- SEVERITY: CAT II

Description:

Tanium Comply must be configured to receive Open Vulnerability and Assessment Language (OVAL) feeds only from trusted sources.

```
GROUP ID: V-253870
RULE ID: SV-253870r842638
```

Rationale:

OVAL XML documents are provided from several possible sources such as the Community Intercomparison Suite (CIS) open-source repository and vendor/third-party paid repositories. These documents are used to automate the passive validation of vulnerabilities on systems and therefore require a reasonable level of confidence in their origin. Nonapproved OVAL definitions lead to a false sense of security when evaluating an enterprise environment.

Audit:

1. Using a web browser on a system that has connectivity to the Tanium application, access the Tanium application web user interface (UI) and log on with multifactor authentication.
2. Click "Modules" on the top navigation banner.
3. Click "Comply".
4. Expand the left menu.
5. Under "Standards", click "Vulnerability".
6. Verify all imported vulnerability sources are from a documented trusted source.

If any vulnerability sources are found that do not come from a documented trusted source, this is a finding.

Remediation:

1. Using a web browser on a system that has connectivity to the Tanium application, access the Tanium application web UI and log on with multifactor authentication.
2. Click "Modules" on the top navigation banner.
3. Click "Comply".
4. Expand the left menu.
5. Under "Standards", click "Vulnerability".
6. Delete any vulnerability sources configured to nontrusted sources or reconfigure them to point to trusted sources.

Additional Information:

CCI-001414

Enforce approved authorizations for controlling the flow of information between connected systems based on organization-defined information flow control policies.

- NIST SP 800-53::AC-4
- NIST SP 800-53A::AC-4.1 (iii)
- NIST SP 800-53 Revision 4::AC-4
- NIST SP 800-53 Revision 5::AC-4

1.93 TANS-SV-000062 (Manual)

Profile Applicability:

- SEVERITY: CAT II

Description:

The Tanium application must limit the bandwidth used in communicating with endpoints to prevent a denial-of-service (DoS) condition at the server.

```
GROUP ID: V-253871
RULE ID: SV-253871r850265
```

Rationale:

DoS is a condition when a resource is not available for legitimate users. When this occurs, the organization either cannot accomplish its mission or must operate at degraded capacity.

This requirement addresses the configuration of applications to mitigate the impact of DoS attacks that have occurred or are ongoing on application availability. For each application, known and potential DoS attacks must be identified and solutions for each type implemented. A variety of technologies exist to limit or, in some cases, eliminate the effects of DoS attacks (e.g., limiting processes or restricting the number of sessions the application opens at one time). Employing increased capacity and bandwidth, combined with service redundancy, may reduce the susceptibility to some DoS attacks.

Audit:

1. Using a web browser on a system that has connectivity to the Tanium application, access the Tanium application web user interface (UI) and log on with multifactor authentication.
2. Click "Administration" on the top navigation banner.
3. Under "Configuration", select "Bandwidth Throttles".
4. Work with the Tanium administrator to confirm settings.

If settings are not based on organization needs, this is a finding.

For more information, refer to https://docs.tanium.com/platform_user/platform_user/console_bandwidth_throttling.html .

Remediation:

1. Using a web browser on a system that has connectivity to the Tanium application, access the Tanium application web UI and log on with multifactor authentication.
2. Click "Administration" on the top navigation banner.

3. Under "Configuration", select "Bandwidth Throttles".
4. Click "Add" on the line for "Global Throttle for All Data".
5. Work with the Tanium administrator to configure the required bandwidth throttles.
6. Click "Save".
7. Work with the Tanium administrator to confirm or set settings for the remaining options:
    - Global Throttle for Package Files.
    - Global Throttle for Sensors.
    - Site Throttles.

Additional Information:

CCI-002385

Protect against or limit the effects of organization-defined types of denial-of-service events.

- NIST SP 800-53 Revision 4::SC-5
- NIST SP 800-53 Revision 5::SC-5 a

1.94 TANS-SV-000065 (Manual)

Profile Applicability:

- SEVERITY: CAT II

Description:

Tanium Server files must be excluded from host-based intrusion prevention intervention.

```
GROUP ID: V-253872
RULE ID: SV-253872r842644
```

Rationale:

Similar to any other host-based applications, the Tanium Server is subject to the restrictions other system-level software may place on an operating environment. Antivirus, intrusion prevention system (IPS), encryption, or other security and management stack software may disallow the Tanium Server from working as expected.

For more information, refer to https://docs.tanium.com/platform_deployment_reference/platform_deployment_reference/security_exceptions.html?Highlight=exclusion.

Audit:

Consult with the Tanium system administrator to determine the HIPS software used on the Tanium Server.

Review the settings of the HIPS software.

Validate exclusions exist that exclude the Tanium program files from being restricted by HIPS.

If exclusions do not exist, this is a finding.

Remediation:

Implement exclusion policies within the HIPS software solution to exclude the Tanium Server program files from HIPS intervention.

Additional Information:

CCI-000366

Implement the security configuration settings.

- NIST SP 800-53::CM-6 b
- NIST SP 800-53A::CM-6.1 (iv)
- NIST SP 800-53 Revision 4::CM-6 b
- NIST SP 800-53 Revision 5::CM-6 b

1.95 TANS-SV-000067 (Manual)

Profile Applicability:

- SEVERITY: CAT II

Description:

The Tanium application must set an inactive timeout for sessions.

```
GROUP ID: V-253873
RULE ID: SV-253873r850135
```

Rationale:

Leaving sessions open indefinitely is a major security risk. An attacker can easily use an already authenticated session to access the hosted application as the previously authenticated user. By closing sessions after a set period of inactivity, the web server can ensure sessions that are not closed when the user logs out of an application are eventually closed.

Acceptable values are 5 minutes for high-value applications, 10 minutes for medium-value applications, and 20 minutes for low-value applications.

Audit:

1. Using a web browser on a system that has connectivity to the Tanium application, access the Tanium application web user interface (UI) and log on with multifactor authentication.
2. Click "Administration" at top center of the screen.
3. Under "Configuration", select "Platform Settings".
4. In the "Filter Items" box, enter `max_console_idle_seconds`.

If no results are returned, this is a finding.

If results are returned for `max_console_idle_seconds` but the value is not `900` or less, this is a finding.

Remediation:

If the "max_console_idle_seconds" setting exists but is not `900` or less:

1. Using a web browser on a system that has connectivity to the Tanium application, access the Tanium application web UI and log on with multifactor authentication.
2. Click "Administration" on the top navigation banner.
3. Under "Configuration", select "Platform Settings".
4. In the "Filter Items" box, enter `max_console_idle_seconds`.
5. Select the `max_console_idle_seconds` setting.

6. For `Value`, enter `900` or less.
7. Click the "Save" button.

If the "max_console_idle_seconds" setting does not exist:

1. Using a web browser on a system that has connectivity to the Tanium application, access the Tanium application web UI and log on with multifactor authentication.
2. Click "Administration" on the top navigation banner.
3. Under "Configuration", select "Platform Settings".
4. Click the "Create Setting" button at the top right.
5. Select `Server` box for `Setting Type`.
6. In `Create Platform Setting` dialog box, enter `max_console_idle_seconds` for `Name`.
7. Select `Numeric` for the `Value Type`.
8. For the `Value`, enter `900` or less.
9. Click "Save".

Additional Information:

CCI-002361

Automatically terminate a user session after organization-defined conditions or trigger events requiring session disconnect.

- NIST SP 800-53 Revision 4::AC-12
- NIST SP 800-53 Revision 5::AC-12

1.96 TANS-SV-000068 (Manual)

Profile Applicability:

- SEVERITY: CAT II

Description:

The Tanium application service must be protected from being stopped by a nonprivileged user.

```
GROUP ID: V-253874
RULE ID: SV-253874r850265
```

Rationale:

Denial of service (DoS) is a condition when a resource is not available for legitimate users. When this occurs, the organization either cannot accomplish its mission or must operate at degraded capacity.

This requirement addresses the configuration of applications to mitigate the impact of DoS attacks that have occurred or are ongoing on application availability. For each application, known and potential DoS attacks must be identified and solutions for each type implemented. A variety of technologies exist to limit or, in some cases, eliminate the effects of DoS attacks (e.g., limiting processes or restricting the number of sessions the application opens at one time). Employing increased capacity and bandwidth, combined with service redundancy, may reduce the susceptibility to some DoS attacks.

A web server not properly tuned may become overwhelmed and cause a DoS condition even with expected traffic from users. To avoid a DoS, the web server must be tuned to handle the expected traffic for the hosted applications.

Audit:

Verify that to prevent a nonprivileged user from affecting the Tanium Server's ability to operate, the control of the service is restricted to the local administrators.

1. Access the Tanium Server.
2. Log on to the server with an account that has administrative privileges.
3. Open the CMD prompt as admin.
4. Run `sc sdshow "Tanium Server"`.

If the string does not match `D:(A;;CCDCLCSWRPWPDTLOCRSDRCWDWO;;;BA)(A;;CCLCSWRPWPDTLOCRRC;;;SY)(A;;CCLCSWLOCRRC;;;AU)S:(AU;FA;CCDCLCSWRPWPDTLOCRSDRCWDWO;;;WD)`, this is a finding.

Note: Run the above on all other Tanium Servers, including Tanium Servers in an Active-Active pair.

Remediation:

1. Access the Tanium Server.
2. Log on to the server with an account that has administrative privileges.
3. Open the CMD prompt as admin.
4. Run `sc sdset "Tanium Server" D:(A;;CCDCLCSWRPWPDTLOCRSDRCWDWO;;;BA)(A;;CCLCSWRPWPDTLOCRRC;;;SY)(A;;CCLCSWLOCRRC;;;AU)S:(AU;FA;CCDCLCSWRPWPDTLOCRSDRCWDWO;;;WD)`.
5. Run the above on all other Tanium Servers, including Tanium Servers in an Active-Active pair.

Additional Information:

CCI-002385

Protect against or limit the effects of organization-defined types of denial-of-service events.

- NIST SP 800-53 Revision 4::SC-5
- NIST SP 800-53 Revision 5::SC-5 a

1.97 TANS-SV-000070 (Manual)

Profile Applicability:

- SEVERITY: CAT I

Description:

The Tanium Application, SQL, and Module servers must all be configured to communicate using TLS 1.2 Strict Only.

```
GROUP ID: V-253875
RULE ID: SV-253875r850269
```

Rationale:

Disabling feedback to senders when there is a failure in protocol validation format prevents adversaries from obtaining information that would otherwise be unavailable.

Audit:

1. Access the Tanium Servers (Application, SQL and Module) interactively.
2. Log on to the server with an account that has administrative privileges.
3. Access the server's registry by typing `regedit`.
4. Press "Enter".
5. Confirm the following settings are in place:

   a) Navigate to: `HKEY_LOCAL_MACHINE >> SYSTEM >> CurrentControlSet >> Control >> SecurityProviders >> SCHANNEL >> Protocols >> SSL 2.0 >> Client`.

   ```
   Name: DisabledByDefault
   Type: REG_DWORD
   Data: 0x0000001 (hex)
   ```

   If the value for `DisabledByDefault` is not set to `1` and `Type` is not configured to `REG_DWORD` or does not exist, this is a finding.

   ```
   Name: Enabled
   Type: REG_DWORD
   Data: 0x00000000 (hex)
   ```

   If the value for `Enabled` is not set to `0` and `Type` is not configured to `REG_DWORD` or does not exist, this is a finding.

   b) Navigate to: `HKEY_LOCAL_MACHINE >> SYSTEM >> CurrentControlSet >> Control >> SecurityProviders >> SCHANNEL >> Protocols >> SSL 2.0 >> Server`.

   ```
   Name: DisabledByDefault
   Type: REG_DWORD
   Data: 0x0000001 (hex)
   ```

If the value for DisabledByDefault is not set to 1 and Type is not configured to REG_DWORD or does not exist, this is a finding.

```
Name: Enabled
Type: REG_DWORD
Data: 0x00000000 (hex)
```

If the value for Enabled is not set to 0 and Type is not configured to REG_DWORD or does not exist, this is a finding.

c) Repeat the steps above for SSL 3.0, TLS 1.0, and TLS 1.1.

d) Navigate to: HKEY_LOCAL_MACHINE >> SYSTEM >> CurrentControlSet >> Control >> SecurityProviders >> SCHANNEL >> Protocols >> TLS 1.2 >> Client.

```
Name: DisabledByDefault
Type: REG_DWORD
Data: 0x0000000 (hex)
```

If the value for DisabledByDefault is not set to 0 and Type is not configured to REG_DWORD or does not exist, this is a finding.

```
Name: Enabled
Type: REG_DWORD
Data: 0x00000001 (hex)
```

If the value for Enabled is not set to 1 and Type is not configured to REG_DWORD or does not exist, this is a finding.

e) Navigate to: HKEY_LOCAL_MACHINE >> SYSTEM >> CurrentControlSet >> Control >> SecurityProviders >> SCHANNEL >> Protocols >> SSL 2.0 >> Server.

```
Name: DisabledByDefault
Type: REG_DWORD
Data: 0x0000000 (hex)
```

If the value for DisabledByDefault is not set to 0 and Type is not configured to REG_DWORD or does not exist, this is a finding.

```
Name: Enabled
Type: REG_DWORD
Data: 0x00000001 (hex)
```

If the value for Enabled is not set to 1 and Type is not configured to REG_DWORD or does not exist, this is a finding.

Remediation:

1. Access the Tanium Server.
2. Log on to the server with an account that has administrative privileges.
3. Access the server's registry by typing regedit.
4. Press "Enter".

5. Navigate to: `HKEY_LOCAL_MACHINE >> SYSTEM >> CurrentControlSet >> Control >> SecurityProviders >> SCHANNEL >> Protocols >> SSL 2.0 >> Client`.
6. Right-click in the right window pane.
7. Select: `New >> DWORD (32-bit) Value`.
8. In the `Name` field, enter `DisabledByDefault`.
9. Press "Enter".
10. Right-click the newly created `Name`.
11. Select "Modify...".
12. Enter `1` in `Value data:` and ensure that under `Base`, the `Hexadecimal` radio button is selected.
13. Click "OK".
14. Right-click in the right window pane.
15. Select: `New >> DWORD (32-bit) Value`.
16. In the `Name` field, enter `Enabled`.
17. Press "Enter".
18. Right-click the newly created `Name`.
19. Select "Modify...".
20. Leave default value of `0` in `Value data:`.
21. Ensure that under `Base`, the `Hexadecimal` radio button is selected.
22. Click "OK".
23. Navigate to: `HKEY_LOCAL_MACHINE >> SYSTEM >> CurrentControlSet >> Control >> SecurityProviders >> SCHANNEL >> Protocols >> SSL 2.0 >> Server`.
24. Right-click in the right window pane.
25. Select: `New >> DWORD (32-bit) Value`.
26. In the `Name` field, enter `DisabledByDefault`.
27. Press "Enter".
28. Right-click the newly created `Name`.
29. Select "Modify...".
30. Enter `1` in `Value data:` and ensure that under `Base`, the `Hexadecimal` radio button is selected.
31. Click "OK".
32. Right-click in the right window pane.
33. Select: `New >> DWORD (32-bit) Value`.
34. In the `Name` field, enter `Enabled`.
35. Press "Enter".
36. Right-click the newly created `Name`.
37. Select "Modify...".
38. Leave default value of `0` in `Value data:`.
39. Ensure that under `Base`, the `Hexadecimal` radio button is selected.
40. Click "OK".
41. Repeat the above steps for SSL 3.0, TLS 1.0, and TLS 1.1.

42. Navigate to: `HKEY_LOCAL_MACHINE >> SYSTEM >> CurrentControlSet >> Control >> SecurityProviders >> SCHANNEL >> Protocols >> TLS 1.2 >> Client`.
43. Right-click in the right window pane.
44. Select: `New >> DWORD (32-bit) Value`.
45. In the `Name` field, enter `DisabledByDefault`.
46. Press "Enter".
47. Right-click the newly created `Name`.
48. Select "Modify...".
49. Enter `0` in `Value data:` and ensure that under `Base`, the `Hexadecimal` radio button is selected.
50. Click "OK".
51. Right-click in the right window pane.
52. Select: `New >> DWORD (32-bit) Value`.
53. In the `Name` field, enter `Enabled`.
54. Press "Enter".
55. Right-click the newly created "Name".
56. Select "Modify...".
57. Leave default value of `1` in `Value data:`.
58. Ensure that under `Base`, the `Hexadecimal` radio button is selected.
59. Click "OK".
60. Navigate to: `HKEY_LOCAL_MACHINE >> SYSTEM >> CurrentControlSet >> Control >> SecurityProviders >> SCHANNEL >> Protocols >> TLS 1.2 >> Server`.
61. Right-click in the right window pane.
62. Select: `New >> DWORD (32-bit) Value`.
63. In the `Name` field, enter `DisabledByDefault`.
64. Press "Enter".
65. Right-click the newly created `Name`.
66. Select "Modify...".
67. Enter `0` in `Value data:` and ensure that under `Base`, the `Hexadecimal` radio button is selected.
68. Click "OK".
69. Right-click in the right window pane.
70. Select: `New >> DWORD (32-bit) Value`.
71. In the `Name` field, enter `Enabled`.
72. Press "Enter".
73. Right-click the newly created `Name`.
74. Select "Modify...".
75. Leave default value of `1` in `Value data:`.
76. Ensure that under `Base`, the `Hexadecimal` radio button is selected.
77. Click "OK".

Additional Information:

CCI-002418

Protect the confidentiality and/or integrity of transmitted information.

- NIST SP 800-53 Revision 4::SC-8
- NIST SP 800-53 Revision 5::SC-8

1.98 TANS-SV-000101 (Manual)

Profile Applicability:

- SEVERITY: CAT I

Description:

The SchUseStrongCrypto registry value must be set.

```
GROUP ID: V-253876
RULE ID: SV-253876r850269
```

Rationale:

Without protection of the transmitted information, confidentiality and integrity may be compromised since unprotected communications can be intercepted and either read or altered.

This requirement applies only to applications that are either distributed or can allow access to data nonlocally. Use of this requirement will be limited to situations where the data owner has a strict requirement for ensuring data integrity and confidentiality is maintained at every step of the data transfer and handling process. When transmitting data, applications must leverage transmission protection mechanisms, such as TLS, SSL VPNs, or IPsec. FIPS 140-2 approved TLS versions must be enabled, and non-FIPS-approved SSL versions must be disabled. NIST SP 800-52 defines the approved TLS versions for government applications.

Communication paths outside the physical protection of a controlled boundary are exposed to the possibility of interception and modification. Protecting the confidentiality and integrity of organizational information can be accomplished by physical means (e.g., employing physical distribution systems) or by logical means (e.g., employing cryptographic techniques). If physical means of protection are employed, then logical means (cryptography) do not have to be employed, and vice versa.

Audit:

1. Access the Tanium Server, Tanium Module Server, and Tanium SQL Server.
2. Log on to the server with an account that has administrative privileges.
3. Run `regedit` as Administrator.
4. Navigate to the following and confirm the setting `SchUseStrongCrypto` is present and configured as follows:

   Navigate to: `HKEY_LOCAL_MACHINE >> SOFTWARE >> Wow6432Node >> Microsoft >> .NETFramework >> v4.0.xxxxx` (the subversion number may vary, but it is a 4.0 version; example: `4.0.30319`) for Tanium Application Server.

Navigate to: HKEY_LOCAL_MACHINE >> SOFTWARE >> Microsoft >> .NETFramework >> v4.0.xxxxx (the subversion number may vary, but it is a 4.0 version; example: 4.0.30319) for Tanium SQL Server.

Navigate to: HKEY_LOCAL_MACHINE >> SOFTWARE >> Microsoft >> .NETFramework >> v4.0.xxxxx (the subversion number may vary, but it is a 4.0 version; example: 4.0.30319) for Tanium Module Server.

```
Name: SchUseStrongCrypto
Type: REG_DWORD
Data: 0x0000001 (hex)
```

If the value for SchUseStrongCrypto is not set to 0x00000001 (hex) and Type is not configured to REG_DWORD or does not exist, this is a finding.

Remediation:

1. Access the Tanium Server, Tanium Module Server, and Tanium SQL Server.
2. Log on to the server with an account that has administrative privileges.
3. Run regedit as Administrator.
4. Use the following locations for steps 5-13.

   Navigate to: HKEY_LOCAL_MACHINE >> SOFTWARE >> Wow6432Node >> Microsoft >> .NETFramework >> v4.0.xxxxx (the subversion number may vary, but it is a 4.0 version; example: 4.0.30319) for Tanium Application Server.

   Navigate to: HKEY_LOCAL_MACHINE >> SOFTWARE >> Microsoft >> .NETFramework >> v4.0.xxxxx (the subversion number may vary, but it is a 4.0 version; example: 4.0.30319) for Tanium SQL Server.

   Navigate to: HKEY_LOCAL_MACHINE >> SOFTWARE >> Microsoft >> .NETFramework >> v4.0.xxxxx (the subversion number may vary, but it is a 4.0 version; example: 4.0.30319) for Tanium Module Server.

5. Right-click in the right window pane.
6. Select: New >> DWORD (32-bit) Value.
7. In the Name field, enter SchUseStrongCrypto.
8. Press "Enter".
9. Right-click the newly created Name.
10. Select "Modify...".
11. Enter 1 in Value data:.
12. Ensure that under Base, the Hexadecimal radio button is selected.
13. Click "OK".

Additional Information:

CCI-002418

Protect the confidentiality and/or integrity of transmitted information.

- NIST SP 800-53 Revision 4::SC-8
- NIST SP 800-53 Revision 5::SC-8

1.99 TANS-SV-000107 (Manual)

Profile Applicability:

- SEVERITY: CAT I

Description:

The SSLCipherSuite registry value must be set.

```
GROUP ID: V-253877
RULE ID: SV-253877r850269
```

Rationale:

Without protection of the transmitted information, confidentiality and integrity may be compromised since unprotected communications can be intercepted and either read or altered.

This requirement applies only to applications that are either distributed or can allow access to data nonlocally. Use of this requirement will be limited to situations where the data owner has a strict requirement for ensuring data integrity and confidentiality is maintained at every step of the data transfer and handling process. When transmitting data, applications must leverage transmission protection mechanisms, such as TLS, SSL VPNs, or IPsec. FIPS 140-2 approved TLS versions must be enabled, and non-FIPS-approved SSL versions must be disabled. NIST SP 800-52 defines the approved TLS versions for government applications.

Communication paths outside the physical protection of a controlled boundary are exposed to the possibility of interception and modification. Protecting the confidentiality and integrity of organizational information can be accomplished by physical means (e.g., employing physical distribution systems) or by logical means (e.g., employing cryptographic techniques). If physical means of protection are employed, logical means (cryptography) do not have to be employed, and vice versa.

Audit:

1. Access the Tanium Server.
2. Log on to the server with an account that has administrative privileges.
3. Run `regedit` as Administrator.
4. Navigate to: `HKEY_LOCAL_MACHINE >> SOFTWARE >> Wow6432Node >> Tanium >> Tanium Server`.

```
Name: SSLCipherSuite
Type: String
Value:ECDHE-RSA-AES256-GCM-SHA384:ECDHE-RSA-AES256-SHA384:ECDHE-RSAAES128-GCM-
SHA256:ECDHE-RSA-AES128-SHA256:!aNULL:!eNULL:!EXPORT:!DES:!RC4:!MD5:!PSK
```

If the String `SSLCipherSuite` does not exist with the appropriate list values, this is a finding.

Remediation:

1. Access the Tanium Server.
2. Log on to the server with an account that has administrative privileges.
3. Run `regedit` as Administrator.
4. Navigate to: `HKEY_LOCAL_MACHINE >> Software >> Wow6432Node >> Tanium >> Tanium Server`.
5. Right-click in the right window pane.
6. Select: New >> String Value.
7. In the `Name` field, enter `SSLCipherSuite`.
8. Press "Enter".
9. Right-click the newly created `Name`.
10. Select "Modify".
11. Add the following: `ECDHE-RSA-AES256-GCM-SHA384:ECDHE-RSA-AES256-SHA384:ECDHE-RSAAES128-GCM-SHA256:ECDHE-RSA-AES128-SHA256:!aNULL:!eNULL:!EXPORT:!DES:!RC4:!MD5:!PSK`
12. Click "OK".

Additional Information:

CCI-002418

Protect the confidentiality and/or integrity of transmitted information.

- NIST SP 800-53 Revision 4::SC-8
- NIST SP 800-53 Revision 5::SC-8

Appendix: Summary Table

CIS Benchmark Recommendation		Set Correctly	
		Yes	No
1	**STIG RULES**		
1.1	TANS-00-000155 (Manual)	☐	☐
1.2	TANS-00-001025 (Manual)	☐	☐
1.3	TANS-00-001055 (Manual)	☐	☐
1.4	TANS-00-001065 (Manual)	☐	☐
1.5	TANS-00-001075 (Manual)	☐	☐
1.6	TANS-00-001120 (Manual)	☐	☐
1.7	TANS-00-001155 (Manual)	☐	☐
1.8	TANS-00-001165 (Manual)	☐	☐
1.9	TANS-00-001170 (Manual)	☐	☐
1.10	TANS-00-001185 (Manual)	☐	☐
1.11	TANS-00-001190 (Manual)	☐	☐
1.12	TANS-00-001195 (Manual)	☐	☐
1.13	TANS-00-001305 (Manual)	☐	☐
1.14	TANS-00-001310 (Manual)	☐	☐
1.15	TANS-00-001315 (Manual)	☐	☐
1.16	TANS-00-001320 (Manual)	☐	☐
1.17	TANS-00-001385 (Manual)	☐	☐
1.18	TANS-00-001395 (Manual)	☐	☐
1.19	TANS-00-001405 (Manual)	☐	☐

CIS Benchmark Recommendation		Set Correctly	
		Yes	No
1.20	TANS-00-001420 (Manual)	☐	☐
1.21	TANS-00-001425 (Manual)	☐	☐
1.22	TANS-00-001455 (Manual)	☐	☐
1.23	TANS-00-001565 (Manual)	☐	☐
1.24	TANS-00-001600 (Manual)	☐	☐
1.25	TANS-00-001750 (Manual)	☐	☐
1.26	TANS-00-001780 (Manual)	☐	☐
1.27	TANS-CL-000001 (Manual)	☐	☐
1.28	TANS-CL-000002 (Manual)	☐	☐
1.29	TANS-CL-000003 (Manual)	☐	☐
1.30	TANS-CL-000004 (Manual)	☐	☐
1.31	TANS-CL-000005 (Manual)	☐	☐
1.32	TANS-CL-000006 (Manual)	☐	☐
1.33	TANS-CL-000007 (Manual)	☐	☐
1.34	TANS-CL-000008 (Manual)	☐	☐
1.35	TANS-CL-000014 (Manual)	☐	☐
1.36	TANS-CN-000001 (Manual)	☐	☐
1.37	TANS-CN-000002 (Manual)	☐	☐
1.38	TANS-CN-000003 (Manual)	☐	☐
1.39	TANS-CN-000004 (Manual)	☐	☐
1.40	TANS-CN-000005 (Manual)	☐	☐
1.41	TANS-CN-000006 (Manual)	☐	☐

CIS Benchmark Recommendation		Set Correctly	
		Yes	No
1.42	TANS-CN-000008 (Manual)	☐	☐
1.43	TANS-CN-000010 (Manual)	☐	☐
1.44	TANS-CN-000014 (Manual)	☐	☐
1.45	TANS-CN-000015 (Manual)	☐	☐
1.46	TANS-CN-000016 (Manual)	☐	☐
1.47	TANS-CN-000019 (Manual)	☐	☐
1.48	TANS-CN-000020 (Manual)	☐	☐
1.49	TANS-CN-000021 (Manual)	☐	☐
1.50	TANS-CN-000027 (Manual)	☐	☐
1.51	TANS-CN-000032 (Manual)	☐	☐
1.52	TANS-CN-000033 (Manual)	☐	☐
1.53	TANS-CN-000036 (Manual)	☐	☐
1.54	TANS-DB-000001 (Manual)	☐	☐
1.55	TANS-DB-000002 (Manual)	☐	☐
1.56	TANS-DB-000003 (Manual)	☐	☐
1.57	TANS-DB-000004 (Manual)	☐	☐
1.58	TANS-DB-000005 (Manual)	☐	☐
1.59	TANS-SV-000002 (Manual)	☐	☐
1.60	TANS-SV-000003 (Manual)	☐	☐
1.61	TANS-SV-000004 (Manual)	☐	☐
1.62	TANS-SV-000005 (Manual)	☐	☐
1.63	TANS-SV-000006 (Manual)	☐	☐

CIS Benchmark Recommendation		Set Correctly	
		Yes	No
1.64	TANS-SV-000007 (Manual)	☐	☐
1.65	TANS-SV-000008 (Manual)	☐	☐
1.66	TANS-SV-000010 (Manual)	☐	☐
1.67	TANS-SV-000014 (Manual)	☐	☐
1.68	TANS-SV-000015 (Manual)	☐	☐
1.69	TANS-SV-000016 (Manual)	☐	☐
1.70	TANS-SV-000017 (Manual)	☐	☐
1.71	TANS-SV-000018 (Manual)	☐	☐
1.72	TANS-SV-000019 (Manual)	☐	☐
1.73	TANS-SV-000020 (Manual)	☐	☐
1.74	TANS-SV-000024 (Manual)	☐	☐
1.75	TANS-SV-000025 (Manual)	☐	☐
1.76	TANS-SV-000026 (Manual)	☐	☐
1.77	TANS-SV-000027 (Manual)	☐	☐
1.78	TANS-SV-000031 (Manual)	☐	☐
1.79	TANS-SV-000032 (Manual)	☐	☐
1.80	TANS-SV-000033 (Manual)	☐	☐
1.81	TANS-SV-000035 (Manual)	☐	☐
1.82	TANS-SV-000036 (Manual)	☐	☐
1.83	TANS-SV-000040 (Manual)	☐	☐
1.84	TANS-SV-000044 (Manual)	☐	☐
1.85	TANS-SV-000045 (Manual)	☐	☐

CIS Benchmark Recommendation		Set Correctly	
		Yes	No
1.86	TANS-SV-000046 (Manual)	☐	☐
1.87	TANS-SV-000048 (Manual)	☐	☐
1.88	TANS-SV-000049 (Manual)	☐	☐
1.89	TANS-SV-000050 (Manual)	☐	☐
1.90	TANS-SV-000051 (Manual)	☐	☐
1.91	TANS-SV-000052 (Manual)	☐	☐
1.92	TANS-SV-000053 (Manual)	☐	☐
1.93	TANS-SV-000062 (Manual)	☐	☐
1.94	TANS-SV-000065 (Manual)	☐	☐
1.95	TANS-SV-000067 (Manual)	☐	☐
1.96	TANS-SV-000068 (Manual)	☐	☐
1.97	TANS-SV-000070 (Manual)	☐	☐
1.98	TANS-SV-000101 (Manual)	☐	☐
1.99	TANS-SV-000107 (Manual)	☐	☐

Appendix: Change History

Date	Version	Changes for this version
Sep 12, 2025	1.0.0	Initial CIS Release