CIS Dragos Platform 2.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

Dragos Platform 2.x Secure Technical Implementation Guide (STIG)

Version: 1 Release: 3 Benchmark

Date: 02 Jul 2025

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 Dragos Platform 2.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 (or rules) for securing a technology or a supporting platform. STIG Benchmark profiles are used to identify which Vulnerability Severity Category Code (CAT) each rule is associated with.

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

The Recommendations in this Benchmark are a representation of the Rules in the unclassified DISA STIG for Dragos Platform 2.x

Recommendations

1 STIG RULES

Dragos Platform 2.*

Dragos Platform 2.x Secure Technical Implementation Guide (STIG)

Version: 1 Release: 3 Benchmark

Date: 02 Jul 2025

CLASSIFICATION unclassified

1.1 DRAG-OT-000020 (Manual)

Profile Applicability:

- SEVERITY: CAT II

Description:

Dragos must configure idle timeouts at 10 minutes.

```
GROUP ID: V-270904
RULE ID: SV-270904r1058027
```

Rationale:

A session time-out lock is a temporary action taken when a user stops work and moves away from the immediate physical vicinity of the information system but does not log out because of the temporary nature of the absence.

The session lock is implemented at the point where session activity can be determined. This is typically at the operating system level but may be at Dragos level.

When Dragos design specifies Dragos rather than the operating system will determine when to lock the session, Dragos session lock event must include an obfuscation of the display screen to prevent other users from reading what was previously displayed.

Publicly viewable images can include static or dynamic images, for example, patterns used with screen savers, photographic images, solid colors, a clock, a battery life indicator, or a blank screen, with the additional caveat that none of the images convey sensitive information.

Satisfies: SRG-APP-000002, SRG-APP-000003, SRG-APP-000190, SRG-APP-000295, SRG-APP-000389

Audit:

Verify session timeout is configured.

In the UI, navigate to Admin >> SiteStore Management >> Advanced Settings.

Click "Configurations".

If Idle Auto-Logout Minutes is not set to `10` minutes, this is a finding.

If Re-Authenticate User Device (Inactive) is not set to `1h`, this is a finding.

Remediation:

Set session timeout configurations.

In the UI, navigate to Admin >> SiteStore Management >> Advanced Settings.

Click "Configurations".

Set Idle Auto-Logout Minutes to `10`.

Set Re-Authenticate User Device (Inactive) to `1h`.

Click "Save & Apply".

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)

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

CCI-001133

Terminate the network connection associated with a communications session at the end of the session or after an organization-defined time period of inactivity.

- NIST SP 800-53::SC-10
- NIST SP 800-53A::SC-10.1 (ii)
- NIST SP 800-53 Revision 4::SC-10
- NIST SP 800-53 Revision 5::SC-10

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

CCI-002038

The organization requires users to reauthenticate upon organization-defined circumstances or situations requiring reauthentication.

- NIST SP 800-53 Revision 4::IA-11
- NIST SP 800-53 Revision 5::IA-11

1.2 DRAG-OT-000090 (Manual)

Profile Applicability:

- SEVERITY: CAT II

Description:

Dragos Platform must use an Identity Provider (IDP) for authentication and authorization processes.

```
GROUP ID: V-270910
RULE ID: SV-270910r1057994
```

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.

A comprehensive application account management process that includes automation helps to ensure accounts designated as requiring attention are consistently and promptly addressed. Examples include, but are not limited to, using automation to take action on multiple accounts designated as inactive, suspended, or terminated or by disabling accounts located in noncentralized account stores such as multiple servers. This requirement applies to all account types, including individual/user, shared, group, system, guest/anonymous, emergency, developer/manufacturer/vendor, temporary, and service.

Dragos Platform must be configured to automatically provide account management functions and these functions must immediately enforce the organization's current account policy. The automated mechanisms may reside within Dragos Platform itself or may be offered by the operating system or other infrastructure providing automated account management capabilities. Automated mechanisms may be comprised of differing technologies that when placed together contain an overall automated mechanism supporting an organization's automated account management requirements.

Account management functions include: assignment of group or role membership; identifying account type; specifying user access authorizations (i.e., privileges); account removal, update, or termination; and administrative alerts. The use of automated mechanisms can include, for example: using email or text messaging to automatically notify account managers when users are terminated or transferred; using the information system to monitor account usage; and using automated telephonic notification to report atypical system account usage.

Satisfies: SRG-APP-000023, SRG-APP-000025, SRG-APP-000065, SRG-APP-000149, SRG-APP-000150, SRG-APP-000151, SRG-APP-000152, SRG-APP-000163, SRG-APP-000165, SRG-APP-000170, SRG-APP-000173, SRG-APP-000233, SRG-APP-000345, SRG-APP-000317, SRG-APP-000318

Audit:

Review the authentication method being used by the Platform.

In the UI, navigate to Admin >> SiteStore Management >> Authentication Providers.

If the Platform does not have an Authentication Provider configured, this is a finding.

Remediation:

Configure LDAP.

In the UI, navigate to Admin >> SiteStore Management >> Authentication Providers.

Next to LDAP/Active Directory, click "ADD PROVIDER".

Fill in the configuration in the "Add New LDAP Provider" form.

Click "Save".

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)

CCI-000017

Disable accounts when the accounts have been inactive for the organization-defined time-period.

- NIST SP 800-53::AC-2 (3)
- NIST SP 800-53A::AC-2 (3).1 (ii)
- NIST SP 800-53 Revision 4::AC-2 (3)
- NIST SP 800-53 Revision 5::AC-2 (3) (d)

CCI-000044

Enforce the organization-defined limit of consecutive invalid logon attempts by a user during the organization-defined time period.

- NIST SP 800-53::AC-7 a
- NIST SP 800-53A::AC-7.1 (ii)
- NIST SP 800-53 Revision 4::AC-7 a
- NIST SP 800-53 Revision 5::AC-7 a

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-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-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)

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-000795

The organization manages information system identifiers by disabling the identifier after an organization-defined time period of inactivity.

- NIST SP 800-53::IA-4 e
- NIST SP 800-53A::IA-4.1 (iii)
- NIST SP 800-53 Revision 4::IA-4 e

CCI-000200

The information system prohibits password reuse for the organization-defined number of generations.

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

CCI-000195

The information system, for password-based authentication, when new passwords are created, enforces that at least an organization-defined number of characters are changed.

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

CCI-000198

The information system enforces minimum password lifetime restrictions.

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

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-002238

Automatically lock the account or node for either an organization-defined time period, until the locked account or node is released by an administrator, or delays the next logon prompt according to the organization-defined delay algorithm when the maximum number of unsuccessful logon attempts is exceeded.

- NIST SP 800-53 Revision 4::AC-7 b
- NIST SP 800-53 Revision 5::AC-7 b

CCI-002142

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

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

CCI-002145

Enforce organization-defined circumstances and/or usage conditions for organization-defined system accounts.

- NIST SP 800-53 Revision 4::AC-2 (11)
- NIST SP 800-53 Revision 5::AC-2 (11)

1.3 DRAG-OT-000200 (Manual)

Profile Applicability:

- SEVERITY: CAT II

Description:

The Dragos Platform must display the Standard Mandatory DOD Notice and Consent Banner before granting local or remote access to the system.

```
GROUP ID: V-270916
RULE ID: SV-270916r1057996
```

Rationale:

Display of a standardized and approved use notification before granting access to the operating system 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 applicable DOD policy. Use the following verbiage for operating systems that can accommodate 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."
```

Use the following verbiage for operating systems that have severe limitations on the number of characters that can be displayed in the banner:

```
"I've read & consent to terms in IS user agreem't."
```

Satisfies: SRG-APP-000068, SRG-APP-000069

Audit:

Verify the Dragos Platform displays the Standard Mandatory DOD Notice and Consent Banner before granting access to the system when login in via SSH.

If the banner does not exist or is not formatted in accordance with applicable DOD policy, this is a finding.

Remediation:

Configure the Dragos Platform to display the Standard Mandatory DOD Notice and Consent Banner before granting access to the system:

1. Log in to the SiteStore or Sensor via SSH.
2. Input "config banner pre_login" into the CLI.
3. Input the banner text shown below, pressing "Enter" after each line. Press config appl CTRL-D to save the text or CTRL-C to quit without saving.
4. Apply the banner by executing the following:
5. `config apply`

The banner must be formatted in accordance with applicable DOD policy. Use the following verbiage for operating systems that can accommodate 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."
```

Use the following verbiage for operating systems that have severe limitations on the number of characters that can be displayed in the banner:

```
"I've read & consent to terms in IS user agreem't."
```

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

1.4 DRAG-OT-000220 (Manual)

Profile Applicability:

- SEVERITY: CAT II

Description:

The publicly accessible Dragos Platform application must display the Standard Mandatory DOD Notice and Consent Banner before granting access to Dragos Platform.

```
GROUP ID: V-270917
RULE ID: SV-270917r1058026
```

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."
```

Use the following verbiage for operating systems that have severe limitations on the number of characters that can be displayed in the banner:

```
"I've read & consent to terms in IS user agreem't."
```

Audit:

Verify that the Standard Mandatory DOD Notice and Consent Banner appears before being granted access to Dragos Platform UI.

If the Standard Mandatory DOD Notice is not presented, this is a finding.

Remediation:

1. Download the following script and put it in the /root directory on the sitestore where the DOD Banner is to be applied (see below).
2. Run the script with the following syntax: `python3 DOD_Banner_Config_Utility.py`, and go to the sitestore login page to verify the banner is present.
3. Schedule the cron with the following syntax to ensure the change survives reboots:

```
5 * * * * python3 /root/DOD_Banner_Config_Utility.py --persist-banner

DOD_Banner_Config_Utility.py

Utility: import os, json, sys, time
# Created by bdudley@dragos.com to assist with Dragos STIG implementation
# specifically related to DoD Banner for web UI before login
os.chdir("/root")
# version compatibility check
if 'Platform Version: 2.4.' not in os.popen("dragoscmd version").read():
    print("This version of the Dragos platform is incompatible with this
script.")
    exit()
DOD_BANNER_JS = "alert('You are accessing a U.S. Government (USG) Information
System (IS) that is provided for USG-authorized use only.\\nBy using this IS
(which includes any device attached to this IS), you consent to the following
conditions:\\n-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.\\n-At any time,
the USG may inspect and seize data stored on this IS.\\n-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.\\n-This IS includes security measures (e.g., authentication and access
controls) to protect USG interests--not for your personal benefit or
privacy.\\n-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.');"
fstream = open('banner.js', 'w')
fstream.write(DOD_BANNER_JS)
fstream.close()
# get the platform-ui container id
platformui = os.popen("kubectl get pods | grep platform-ui | grep -v platform-
ui-logger | awk '{print $1}'").read().strip()
BANNER_DIR = '/usr/share/nginx/html/source/'
HTML_DIR = '/usr/share/nginx/html/'
```

```
if "--restore-defaults" in sys.argv:
    print("Restoring to default, no banner.")
    os.system("kubectl -n dragos-sitestore cp ./index.html.bak
"+platformui+":"+HTML_DIR+"index.html")
    print("Done, reload the page to test changes.")
    exit()
# this will check periodically to make sure the banner changes persisted, and
re-apply them if not
if "--persist-banner" in sys.argv:
    # check the current settings
    current_html = os.popen("curl -k https://localhost").read()
    if "./source/banner.js" in current_html:
        print("Banner is currently set, taking no action.")
        exit()
    else:
        fstream = open("banner.log", "a")
        fstream.write("["+time.ctime().replace("  ", "")+"] banner was not set,
setting banner now.\n")
        fstream.close()
    # put the banner js file in the appropriate directory
    os.system("kubectl -n dragos-sitestore cp ./banner.js
"+platformui+":"+BANNER_DIR+"banner.js")
    # update the current version of index.html in the pod
    os.system("kubectl -n dragos-sitestore cp ./index.html.patched
"+platformui+":"+HTML_DIR+"index.html")
    exit()
# is the sitestore up and running?
if "System is ready." not in os.popen("dragoscmd system k3s status").read():
    print("System is not ready, wait until all pods are started before
configuring banner.")
    exit()
# is there a backup of the old index.html file
if os.path.exists('index.html.bak') == False:
    print("Creating an index.html backup...")
    os.system("kubectl -n dragos-sitestore cp
"+platformui+":"+HTML_DIR+"index.html ./index.html.bak")
    print("Done.")
# put the banner js file in the appropriate directory
os.system("kubectl -n dragos-sitestore cp ./banner.js
"+platformui+":"+BANNER_DIR+"banner.js")
# perform appropriate patching on the index.html backup
fstream = open("index.html.bak", "r")
html = fstream.read()
fstream.close()
original = '<script nonce="**CSP_NONCE**" type="module" crossorigin'
replacement = '<script src="./source/banner.js"
nonce="**CSP_NONCE**"></script><script nonce="**CSP_NONCE**" type="module"
crossorigin'
fstream = open("index.html.patched", "w")
fstream.write(html.replace(original, replacement))
fstream.close()
# update the current version of index.html in the pod
os.system("kubectl -n dragos-sitestore cp ./index.html.patched
"+platformui+":"+HTML_DIR+"index.html")
print("Banner configuration changes complete, reload the login page (or logout)
to see the popup.  If the formatting for the popup needs to be adjusted, make
the changes in the banner block above and re-run this script.")
print("\nUse the below format to create a cron that makes the banner persist
through reboots:\n\n*/5 * * * * python3 /root/DOD_Banner_Config_Utility.py --
persist-banner\n\n")
```

Additional Information:

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

1.5 DRAG-OT-000240 (Manual)

Profile Applicability:

- SEVERITY: CAT II

Description:

The Dragos Platform must only allow local administrative and service user accounts.

```
GROUP ID: V-270919
RULE ID: SV-270919r1107124
```

Rationale:

Only two default accounts facilitate the initial setup and configuration of the Platform. These accounts provide immediate access to the system, allowing administrators to quickly get the system up and running without needing to create new user accounts during the initial installation phase.

During maintenance, updates, or support operations, default accounts allow vendor support teams to access the system without needing to manage a variety of customer-specific accounts. This can streamline support activities and reduce downtime.

Default accounts passwords need to be protected so they cannot be exploited by attackers to gain unauthorized access to the system.

Satisfies: SRG-APP-000080, SRG-APP-000234

Audit:

Verify local user accounts.

While logged in to the Dragos Platform with a user account with administrative privileges, navigate to Admin >> User Management >> Users.

If any local user except the UI Administrator and DragOS CLI Service Account exists, this is a finding.

Remediation:

Remove users except the UI Administrator and DragOS CLI Service Account.

While logged in to the Dragos Platform with a user account with administrative privileges, navigate to Admin >> User Management >> Users.

Click the kebab menu next to the user and select "Delete User".

Click "DELETE" in the verification window.

Additional Information:

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-001682

Automatically remove or disable emergency accounts after an organization-defined time period for each type of account.

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

1.6 DRAG-OT-000370 (Manual)

Profile Applicability:

- SEVERITY: CAT II

Description:

The Dragos Platform must have notification and audit services installed.

```
GROUP ID: V-270932
RULE ID: SV-270932r1058029
```

Rationale:

Installing the Knowledge Pack(s) is essential for the Dragos Platform to provide comprehensive security monitoring, compliance, and operational visibility within industrial environments. It enhances the Platform's capabilities in detecting and responding to threats, ensuring regulatory compliance, and maintaining the overall security. It is critical for the appropriate personnel to be aware if a system is at risk of failing to process audit logs as required.

The pack provides enhanced visibility into the operations of the Dragos Platform. This includes monitoring user activities, changes to system configurations, and other critical events. Improved visibility helps in identifying potential security issues and operational anomalies before they escalate into significant problems.

Audit:

Ensure all notification and audit services are functional.

Log in to the SiteStore CLI and execute the following command:

```
system k3s status
```

If the message does not return "system is ready", this is a finding.

(**Note** that for approximately 15–20 minutes after system startup or reboot, system will not be ready. Additionally, until the sensor is paired with a SiteStore, one pod on the sensor will not be ready).

Remediation:

If a notification does not appear, install `KP-CW-24-001`. This knowledge pack will add this and other notifications relevant to the STIG to the Dragos Platform.

To add Knowledge Pack:

While logged in to the Dragos Platform with a user account with administrative privileges, navigate to Admin >> SiteStore Management >> Knowledge Packs.

Locate all `STIG-KP_Plus` Knowledge Pack(s).

Click "Deploy" button next to the Knowledge Pack(s).

Fill in the form and click "DEPLOY".

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

1.7 DRAG-OT-000490 (Manual)

Profile Applicability:

- SEVERITY: CAT II

Description:

The Dragos Platform must be configured to send backup audit records.

```
GROUP ID: V-270944
RULE ID: SV-270944r1107127
```

Rationale:

Configuring the Dragos Platform to send out backup audit records is a critical best practice for ensuring the security, integrity, and availability of audit data. It supports disaster recovery, regulatory compliance, forensic investigations, and overall operational resilience, thereby strengthening the organization's cybersecurity posture.

Storing backup audit records in a separate location ensures that even if the primary system is compromised or experiences a failure, the audit records remain intact and secure. This separation enhances the overall integrity and security of the audit data.

In the event of a catastrophic event such as a cyberattack, hardware failure, or natural disaster, having backup audit records stored offsite allows for recovery of critical audit data. This capability is essential for restoring operations and conducting post-incident analyses.

In the aftermath of a security incident, forensic investigators rely on audit records to reconstruct events and understand the nature and impact of the incident. Backup audit records provide a reliable source of information for these investigations, even if the primary records are tampered with or deleted.

Regularly backing up audit records ensures operational continuity by safeguarding critical data. In case of an unexpected event, the Dragos Platform can quickly access the backup records to continue monitoring and analyzing security events without significant disruption.

Regular backups of audit records help ensure accountability by providing a reliable and tamper-evident log of activities. This accountability is essential for maintaining trust and transparency within the organization and with external stakeholders.

Satisfies: SRG-APP-000125, SRG-APP-000515, SRG-APP-000358

Audit:

Verify third-party server is used to offload audit records.

1. Check for a configured Syslog Server. In the UI, navigate to Admin >> Integrations.

Click "LAUNCH" in the Syslog section.

If a Syslog Server is not listed or Status is not connected, this is a finding.

If the protocol of the Syslog Server is not TLS or mTLS, this is a finding.

2. Check for an export rule. In the UI, navigate to Notification >> RULES Tab.

   Verify a rule exists and has the following:

```
Action = "Send Syslog (<your syslog server>)"
Criteria = "IF Notification Type equals System"
```

If this rule does not exist with the correct Action and Criteria, this is a finding.

Remediation:

Create Syslog server and Rule.

1. Create a Syslog server on a third-party device. The steps may vary depending on the chosen Syslog server software.
2. Create a syslog server output in the Dragos UI.

   Navigate to Admin >> Integrations.

   Click "LAUNCH" in the Syslog section.

   Click "ADD NEW SERVER".

   Enter third-party server information, select TLS or mTLS in the protocol dropdown, and click "NEXT". Note: This step may require TLS certificate generation.

   Input Message Template.

   Click "SAVE".

3. Create a rule.

   Navigate to Notification >> RULES Tab.

   Click "NEW RULE".

   Fill in Name and Processing Order.

   Select For Rule Criteria:

```
If ANY of the following - "Notification Type" "Equals" "System"
Action = Send Syslog (third-party server)
```

   Click "SAVE".

Additional Information:

CCI-001348

Store audit records on an organization-defined frequency in a repository that is part of a physically different system or system component than the system or component being audited.

- NIST SP 800-53::AU-9 (2)
- NIST SP 800-53A::AU-9 (2).1 (iii)
- NIST SP 800-53 Revision 4::AU-9 (2)
- NIST SP 800-53 Revision 5::AU-9 (2)

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)

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)

1.8 DRAG-OT-000500 (Manual)

Profile Applicability:

- SEVERITY: CAT II

Description:

The Dragos Platform must have disk encryption enabled on a virtual machines (VMs).

```
GROUP ID: V-270945
RULE ID: SV-270945r1107130
```

Rationale:

Enabling disk encryption on VMs running the Dragos Platform is a critical security measure to protect sensitive data, ensure compliance with regulations, and provide a robust defense against various threats, including unauthorized access, data breaches, and insider threats.

Disk encryption ensures that the data stored on the VM's disk is unreadable to unauthorized users. This is crucial for protecting sensitive information, such as security logs, configurations, and other operational data, from being accessed if the disk is physically stolen or if unauthorized access is obtained.

In the event of a security breach, encrypted disks prevent attackers from easily accessing the data stored on the VMs. This is particularly important for mitigating the risks associated with data breaches, including the potential exposure of sensitive operational technology (OT) and industrial control system (ICS) data.

VMs can be snapshotted or cloned, creating exact copies of the VM, including its data. Disk encryption ensures that even if a snapshot or clone is made, the data remains protected and cannot be accessed without the appropriate decryption keys.

Disk encryption protects data at rest, which is data stored on the disk when the system is not in use. This is a critical aspect of data security, as it ensures that the data remains protected even if the VM is powered off or in a dormant state.

For organizations using both on-premises and cloud environments, disk encryption provides a consistent approach to data security. This helps maintain uniform security policies and practices across different infrastructure setups.

In multi-tenant environments, where multiple virtual machines run on the same physical hardware, disk encryption ensures that data on one VM cannot be accessed by other tenants or compromised VMs on the same host.

Audit:

If Dragos is running on an appliance, this check is Not Applicable.

If the hypervisor is using full disk encryption, this check is Not Applicable.

Check for disk encryption in a VM.

Log into the VM and access the VM using remote access method, such as SSH.

Use Built-in Tools or Commands:

Linux:

1. Open a terminal window.
2. Use the following command to check if any encrypted partitions exist:
3. `lsblk -o NAME,FSTYPE,LABEL,UUID,SIZE,MOUNTPOINT,TYPE`
4. Check for partitions with the filesystem type `crypto_LUKS` or similar.
5. Use the following command to list encrypted volumes:
6. `cryptsetup luksDump /dev/sdX`

   (Replace `/dev/sdX` with the appropriate device name)

If volumes are not encrypted, this is a finding.

Remediation:

If Dragos is running on an appliance, this check is Not Applicable.

If the hypervisor is using full disk encryption, this check is Not Applicable.

LUKS (Linux Unified Key Setup):

During the installation process, most Linux distributions provide an option to encrypt the disk. Select this option to set up encryption.

To encrypt an existing installation, use tools such as `cryptsetup` to set up encryption manually. Here is a general guide:

Execute the following (Replace `/dev/sdX` with the appropriate device name):

```
sudo cryptsetup luksFormat /dev/sdX
sudo cryptsetup open /dev/sdX encrypted_disk
sudo mkfs.ext4 /dev/mapper/encrypted_disk
sudo mount /dev/mapper/encrypted_disk /mnt
```

Additional Information:

CCI-001350

Implement cryptographic mechanisms to protect the integrity of audit information.

- NIST SP 800-53::AU-9 (3)
- NIST SP 800-53A::AU-9 (3).1
- NIST SP 800-53 Revision 4::AU-9 (3)
- NIST SP 800-53 Revision 5::AU-9 (3)

1.9 DRAG-OT-000520 (Manual)

Profile Applicability:

- SEVERITY: CAT I

Description:

Dragos Platforms must limit privileges and not allow the ability to run shell.

```
GROUP ID: V-270947
RULE ID: SV-270947r1058031
```

Rationale:

If Dragos Platform were to allow any user to make changes to software libraries, then those changes might be implemented without undergoing the appropriate testing and approvals that are part of a robust change management process.

This requirement applies to applications with software libraries that are accessible and configurable, as in the case of interpreted languages. Software libraries also include privileged programs which execute with escalated privileges. Only qualified and authorized individuals must be allowed to obtain access to information system components for purposes of initiating changes, including upgrades and modifications.

Satisfies: SRG-APP-000133, SRG-APP-000206, SRG-APP-000246, SRG-APP-000340, SRG-APP-000342, SRG-APP-000384

Audit:

Verify shell environment:

Log in to the Dragos Platform CLI.

Execute the following command:

```
run shell
```

If the option "run shell" executes successfully and places the terminal session into a shell environment, this is a finding.

Note: A shell environment will be noticeable because the terminal line will be in the format `user@dragos:~$` compared to `dragoscmd`, which would be *`<dragos>`*. If shell is properly uninstalled, the return will be `Error: No such command 'shell'.`

Remediation:

Uninstall shell environment:

Log in to the Dragos Platform CLI.

Execute the following command:

```
run ushell
```

Once this is done, users cannot initiate communications outside low threshold (nonuser configurable) ICMP packets. Nonsigned installation packages cannot be added to the Dragos Platform. This command removes the shell from the Platform; it cannot be reinstalled without installing Dragos Platform from baseline images.

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)

CCI-001166

Identify organization-defined unacceptable mobile code.

- NIST SP 800-53::SC-18 (1)
- NIST SP 800-53A::SC-18 (1).1 (i)
- NIST SP 800-53 Revision 4::SC-18 (1)
- NIST SP 800-53 Revision 5::SC-18 (1)

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)

CCI-002235

Prevent non-privileged users from executing privileged functions.

- NIST SP 800-53 Revision 4::AC-6 (10)
- NIST SP 800-53 Revision 5::AC-6 (10)

CCI-002233

Prevent the organization-defined software from executing at higher privilege levels than users executing the software.

- NIST SP 800-53 Revision 4::AC-6 (8)
- NIST SP 800-53 Revision 5::AC-6 (8)

CCI-001764

Prevent program execution in accordance with organization-defined policies, rules of behavior, and/or access agreements regarding software program usage and restrictions; rules authorizing the terms and conditions of software program usage.

- NIST SP 800-53 Revision 4::CM-7 (2)
- NIST SP 800-53 Revision 5::CM-7 (2)

1.10 DRAG-OT-000610 (Manual)

Profile Applicability:

- SEVERITY: CAT II

Description:

Dragos must allow only the individuals appointed by the information system security manager (ISSM) to have full admin rights to the system.

```
GROUP ID: V-270952
RULE ID: SV-270952r1057499
```

Rationale:

Without restricting which roles and individuals can select which events are audited, unauthorized personnel may be able to prevent the auditing of critical events.

Misconfigured audits may degrade the system's performance by overwhelming the audit log. Misconfigured audits may also make it more difficult to establish, correlate, and investigate the events relating to an incident or identify those responsible for one.

Audit:

Obtain the LDAP group name mapped to the admin role.

Request from the LDAP administrator the group membership of this LDAP group, and compare to the list of individuals appointed by the ISSM.

If users that are not defined by the ISSM as requiring admin rights are present in the admin role membership, this is a finding.

Remediation:

Provide the list of individuals assigned by the ISSM to be members of the admin role to the Dragos administrator.

Provide the list of individuals assigned by the ISSM to be members of the admin role to the LDAP administrator to add to the LDAP group mapped to the admin role.

Create user accounts and assign the admin role for users provided in the lists.

Additional Information:

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)

1.11 DRAG-OT-000650 (Manual)

Profile Applicability:

- SEVERITY: CAT II

Description:

The Dragos Platform must configure local password policies.

```
GROUP ID: V-270955
RULE ID: SV-270955r1058011
```

Rationale:

The shorter the password, the lower the number of possible combinations that need to be tested before the password is compromised.

Password complexity, or strength, is a measure of the effectiveness of a password in resisting attempts at guessing and brute-force attacks. Password length is one factor of several that helps to determine strength and how long it takes to crack a password. Use of more characters in a password helps to exponentially increase the time and/or resources required to compromise the password.

Satisfies: SRG-APP-000164, SRG-APP-000166, SRG-APP-000167, SRG-APP-000168, SRG-APP-000169, SRG-APP-000174

Audit:

Check password configurations. In the UI, navigate to Admin >> SiteStore Management >> Authentication Providers.

Click "EDIT" in the Local Authentication section.

Verify the following settings:

1. Password Expiration is set to `2 months` or less.
2. Password Reuse Limit is set to `5` or less.
3. Minimum Length is set to `15` or greater.
4. Uppercase and lowercase letters is checked.
5. Special characters is checked.
6. Numeric characters is checked.

If any settings are not configured correctly, this is a finding.

Remediation:

Change password configurations.

In the UI, navigate to Admin >> SiteStore Management >> Authentication Providers.

Click "EDIT" in the Local Authentication section.

Change the fields to the following settings:

- Password Expiration = `2 months` or less
- Password Reuse Limit = `5` or less
- Minimum Length = `15` or greater
- Uppercase and lowercase letters = Checked
- Special characters = Checked
- Numeric characters = Checked

Click "SAVE".

Additional Information:

CCI-000205

The information system enforces minimum password length.

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

CCI-000192

The information system enforces password complexity by the minimum number of upper case characters used.

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

CCI-000193

The information system enforces password complexity by the minimum number of lower case characters used.

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

CCI-000194

The information system enforces password complexity by the minimum number of numeric characters used.

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

CCI-001619

The information system enforces password complexity by the minimum number of special characters used.

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

CCI-000199

The information system enforces maximum password lifetime restrictions.

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

1.12 DRAG-OT-001010 (Manual)

Profile Applicability:

- SEVERITY: CAT II

Description:

Dragos must use FIPS-validated encryption and hashing algorithms to protect the confidentiality and integrity of application configuration files and user-generated data stored or aggregated on the device.

```
GROUP ID: V-270978
RULE ID: SV-270978r1057577
```

Rationale:

Confidentiality and integrity protections are intended to address the confidentiality and integrity of system information at rest (e.g., network device rule sets) when it is located on a storage device within the network device or as a component of the network device. This protection is required to prevent unauthorized alteration, corruption, or disclosure of information when not stored directly on the network device.

This requirement addresses protection of user-generated data as well as operating system-specific configuration data. Organizations may choose to employ different mechanisms to achieve confidentiality and integrity protections, as appropriate, in accordance with the security category and/or classification of the information.

Audit:

If using Dragos hardware, this check is Not Applicable.

In a virtual environment, check for FIPS-validated encryption:

- Check the documentation of the virtual environment being used (e.g., virtual machine software or cloud service provider documentation) to find out if it uses FIPS compliance or FIPS-validated encryption support.
- Check for configuration settings related to encryption algorithms and cryptographic modules in the virtual environment. Some platforms allow users to enable FIPS mode.
- Perform testing to ensure that only FIPS-approved cryptographic algorithms are being used within the virtual environment. This would involve testing encryption and decryption processes to confirm compliance with FIPS standards.

If the virtual environment is not using FIPS-validated encryption or is not using FIPS compliance, this is a finding.

Remediation:

If using Dragos hardware, this check is Not Applicable.

Configuring FIPS compliance in a virtual environment involves enabling settings or options that enforce the use of only FIPS-approved cryptographic algorithms and modules. The exact steps may vary depending on the virtualization platform being used (e.g., VMware, Hyper-V, VirtualBox) or the cloud service provider being used (e.g., AWS, Azure). Here is a general guide on how to configure FIPS compliance in a virtual environment:

Review Documentation:

- Start by reviewing the documentation provided by the virtualization platform or cloud service provider. Check for information on FIPS compliance and how to enable it within the environment.

Enable FIPS Mode:

- Many virtualization platforms offer an option to enable FIPS mode. Depending on the platform, this option may be found in the settings or configuration menu.

Update Software:

- Ensure the virtualization software and any guest operating systems are up to date. Some updates may include patches or changes related to FIPS compliance.

Configure Security Policies:

- Check if there are specific security policies or configurations related to FIPS compliance that need to be set within the virtual environment. This could include policies related to encryption, authentication, or other security-related settings.

Test Configuration:

- After enabling FIPS mode and configuring any necessary settings, perform testing to ensure that only FIPS-approved cryptographic algorithms are being used within the virtual environment. Test various cryptographic operations to verify compliance.

Additional Information:

CCI-001199

Protects the confidentiality and/or integrity of organization-defined information at rest.

- NIST SP 800-53::SC-28
- NIST SP 800-53A::SC-28.1
- NIST SP 800-53 Revision 4::SC-28
- NIST SP 800-53 Revision 5::SC-28

1.13 DRAG-OT-001190 (Manual)

Profile Applicability:

- SEVERITY: CAT II

Description:

The Dragos Platform must notify system administrators and information system security officer (ISSO) of local account activity.

```
GROUP ID: V-270993
RULE ID: SV-270993r1058013
```

Rationale:

Once an attacker establishes access to an application, the attacker often attempts to create a persistent method of re-establishing access. One way to accomplish this is for the attacker to simply create a new account. Sending notification of account creation events to the system administrator and ISSO is one method for mitigating this risk.

Satisfies: SRG-APP-000291, SRG-APP-000292, SRG-APP-000293, SRG-APP-000294

Audit:

While logged in to the Dragos Platform with a user account with administrative privileges, navigate to Admin >> User Management >> Users.

Create a new user account (does not require roles or authentication).

(Within 15 minutes)

1. Click the "Notifications" button.
    - Verify a notification appears within Dragos Platform notifications page.
    - If a notification does not occur, this is a finding.
2. Observe that the same notification appears in the aggregate server/syslog recipient.

    (**Note:** Depending on the software application used, steps to view syslog third-party alerts may vary.)

    - If an alert is not being sent to third-party syslog, this is a finding.
3. Check Rules:
    - Navigate to Notification >> RULES Tab.
    - Verify a rule exists and has the following:

```
Action = "Send Syslog (third-party server)"
Criteria = "Detected By Equals Authentication to the Dragos Platform"
          "Detected By Equals User Account Activity"
```

- If a rule does not exist with the correct Action and Criteria, this is a finding.

4. Remove the test user just created.

Remediation:

1. If a notification does not appear, install KP-CW-24-001. This knowledge pack will add this and other notifications relevant to the STIG to the Dragos Platform.
   - Adding Knowledge Pack:

     While logged in to the Dragos Platform with administrative privileges, navigate to Admin >> SiteStore Management >> Knowledge Packs.

     - Locate all `STIG-KP_Plus` Knowledge Pack(s).
     - Click "Deploy" button next to the Knowledge Pack(s).
     - Fill in the form and click "DEPLOY".
2. If a notification appears but is not received by the aggregate/syslog server, ensure there is a rule to trigger a syslog export in the "Notifications" applet of the Dragos Platform. If not, create one.
   - To create a rule, navigate to Notification >> RULES Tab.
   - Create two Attributes.
     - Click "NEW RULE".
     - Fill in Name and Processing Order.
       - Click "ADD ATTRIBUTE" in the "If ANY of the following" block

```
Type = "Detected By"
Select Operation = "Equals"
Select Value = "Authentication to the Dragos Platform"
```

       - Click "ADD ATTRIBUTE" in the "If ANY of the following" block

```
Type = "Detected By"
Select Operation = "Equals"
Select Value = "User Account Activity"
```

       - In the "THEN perform the following actions block:
         - Click "ADD ACTION"

```
Action = Send Syslog (third-party server)
```

     - Click "SAVE".

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)

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)

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)

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)

1.14 DRAG-OT-001430 (Manual)

Profile Applicability:

- SEVERITY: CAT II

Description:

Dragos Platform must allocate audit record storage retention length.

```
GROUP ID: V-271008
RULE ID: SV-271008r1057667
```

Rationale:

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

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

Audit:

In the UI, navigate to Admin >> SiteStore Management >> Advanced Settings.

Review the System Security Plan (SSP).

Verify Deleted Retention Days and Source Data Retention Days is set accordance with organization-defined audit record storage requirements. If not, this is a finding.

Remediation:

In the UI, navigate to Admin >> SiteStore Management >> Advanced Settings.

Set "Deleted Retention Days" and "Source Data Retention Days" (length in days) in accordance with organization-defined audit record storage requirements.

Click "Save & Apply".

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

1.15 DRAG-OT-001630 (Manual)

Profile Applicability:

- SEVERITY: CAT II

Description:

The Syslog client must use TCP connections.

```
GROUP ID: V-271027
RULE ID: SV-271027r1057724
```

Rationale:

Removal of unneeded or nonsecure functions, ports, protocols, and services mitigate the risk of unauthorized connection of devices, unauthorized transfer of information, or other exploitation of these resources.

The organization must perform a periodic scan/review of Dragos (as required by CCI-000384) and disable functions, ports, protocols, and services deemed to be unneeded or nonsecure.

Audit:

Use the `netstat` command to display active UDP connections:

```
netstat -n -p UDP
```

If the syslog client is using a UDP connection, this is a finding.

Remediation:

Changing UDP ports to TCP ports and using TCP instead involves modifying the configuration of the application or service that uses UDP for communication.

Modify the syslog client configuration to specify TCP instead of UDP. This may involve changing port numbers or selecting TCP as the communication protocol.

After making the necessary changes, restart the application or service to apply the new configuration settings. This ensures that the syslog client starts using TCP ports instead of UDP ports.

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)

1.16 DRAG-OT-001750 (Manual)

Profile Applicability:

- SEVERITY: CAT II

Description:

Dragos Platform must accept the DOD CAC or other PKI credential for identity management and personal authentication.

```
GROUP ID: V-271034
RULE ID: SV-271034r1057745
```

Rationale:

The use of Personal Identity Verification (PIV) credentials facilitates standardization and reduces the risk of unauthorized access.

PIV credentials are those credentials issued by federal agencies that 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 agency-wide use of PIV credentials.

Satisfies: SRG-APP-000402, SRG-APP-000403, SRG-APP-000391, SRG-APP-000392, SRG-APP-000402, SRG-APP-000403, SRG-APP-000177, SRG-APP-000176, SRG-APP-000175, SRG-APP-000401

Audit:

Verify that Dragos is configured to use the DOD CAC or other PKI credential to log in to the application.

Log in to the application.

If DOD CAC or other PKI is not configured, this is a finding.

Remediation:

Configure an SSO proxy service using LDAP to provide PKI credentials.

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)

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)

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)

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)

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)

CCI-000186

For public key-based authentication, enforce authorized access to the corresponding private key.

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

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)

CCI-001991

The information system, for PKI-based authentication, implements a local cache of revocation data to support path discovery and validation in case of inability to access revocation information via the network.

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

1.17 DRAG-OT-001910 (Manual)

Profile Applicability:

- SEVERITY: CAT II

Description:

The Dragos Platform must only allow the use of DOD PKI established certificate authorities for verification of the establishment of protected sessions.

```
GROUP ID: V-271049
RULE ID: SV-271049r1057790
```

Rationale:

Untrusted Certificate Authorities (CA) can issue certificates, but they may be issued by organizations or individuals that seek to compromise DOD systems or by organizations with insufficient security controls. If the CA used for verifying the certificate is not a DOD-approved CA, trust of this CA has not been established.

The DOD will only accept PKI certificates obtained from a DOD-approved internal or external certificate authority. Reliance on CAs for the establishment of secure sessions includes, for example, the use of TLS certificates.

This requirement focuses on communications protection for Dragos Platform session rather than for the network packet.

This requirement applies to applications that use communications sessions. This includes, but is not limited to, web-based applications and Service-Oriented Architectures (SOA).

Satisfies: SRG-APP-000427, SRG-APP-000605

Audit:

Open a web browser and navigate to the Dragos Platform UI.

Locate the security or certificate status indicator at the address bar.

Open the certificate information. If the certificate is signed by anyone other than DOD, PKI, or CA, this is a finding.

Remediation:

Change Certificate via GUI.

In the UI, navigate to Admin >> SiteStore Management >> Advanced Settings.

Click "Change Certificate".

Fill in the correct fields and either upload or insert the certificate.

Click "Save & Apply".

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)

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)

1.18 DRAG-OT-002120 (Manual)

Profile Applicability:

- SEVERITY: CAT II

Description:

The Dragos Platform must alert the information system security officer (ISSO), information system security manager (ISSM), and other individuals designated by the local organization when events are detected that indicate a compromise or potential for compromise.

```
GROUP ID: V-271070
RULE ID: SV-271070r1107133
```

Rationale:

When a security event occurs, Dragos Platform 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 mechanisms, or prevention mechanisms.

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.

Audit:

1. Check Server Configuration.
    - If using Syslog Server:
    - Verify third-party server is used to receive communication-related notifications.
    - Check for a configured Syslog Server.
    - In the UI, navigate to Admin >> Integrations.
    - Click "LAUNCH" in the Syslog section.

    If no server is configured or the status is not "Connected", this is a finding.

    If no recipient is configured, this is a finding.

2. Check Rules:
    - Navigate to Notification >> RULES Tab.
    - Verify a rule exists and has the following:

```
Action = "Send ()"
Criteria = "Notification Type Equals System"
```

```
"Notification Type Equals System Failure"
```

3. If a rule does not exist with the correct Action and Criteria, this is a finding.

Remediation:

1. Configure Servers.
    - If using Syslog Server:
        - Create a Syslog server on a third-party device.
        - The steps may vary depending on the chosen Syslog server software. Refer to 2.3.x Dragos Platform Syslog Integration Guide in the Customer Portal for additional help.
    - Create a syslog server output in the Dragos UI.
        - Navigate to Admin >> Integrations.
        - Click "LAUNCH" in the Syslog section.
        - Click "ADD NEW SERVER".
        - Enter third-party server information and click "NEXT".
        - Input Message Template.
        - Click "SAVE".
2. Creating System Rules:
    - Navigate to Notification >> RULES Tab.
        - Click "NEW RULE".
        - Fill in Name and Processing Order.
    - Create two Attributes.
        - Click "ADD ATTRIBUTE" in the "If ANY of the following" block:

```
Type = "Notification Type"
Select Operation = "Equals"
Select Value = "System"
```

        - Click "ADD ATTRIBUTE" in the "If ANY of the following" block:

```
Type = "Notification Type"
Select Operation = "Equals"
Select Value = "System failure"
```

    - In the "THEN perform the following actions block:
        - Click "ADD ACTION".

```
Action = "Send ()"
```

    - Click "SAVE".

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)

1.19 DRAG-OT-002480 (Manual)

Profile Applicability:

- SEVERITY: CAT II

Description:

Before establishing a network connection with a Network Time Protocol (NTP) server, Dragos Platform must authenticate using a bidirectional, cryptographically based authentication method that uses a FIPS-validated Advanced Encryption Standard (AES) cipher block algorithm to authenticate with the NTP server.

```
GROUP ID: V-271105
RULE ID: SV-271105r1057958
```

Rationale:

Without device-to-device authentication, communications with malicious devices may be established. Bidirectional authentication provides stronger safeguards to validate the identity of other devices for connections that are of greater risk.

Currently, DOD requires the use of AES for bidirectional authentication since it is the only FIPS-validated AES cipher block algorithm. The NTP uses MD5 authentication keys. The MD5 algorithm is not approved for use in either the FIPS or NIST recommendation; thus, a CAT 1 finding is allocated in CCI-000803. However, the use of MD5 is preferred to no authentication at all and can be used to mitigate this requirement to a CAT II finding.

The trusted-key statement permits authenticating NTP servers. The product must be configured to support separate keys for each NTP server. Severs should have PKI device certificate involved for use in the device authentication process.

Server authentication is performed by the client using the server's public key certificate, which the server presents during the handshake. The exact nature of the cryptographic operation for server authentication is dependent on the negotiated cipher suite and extensions. In most cases (e.g., RSA for key transport, DH, and ECDH), authentication is performed explicitly through verification of digital signatures present in certificates and implicitly by the use of the server public key by the client during the establishment of the master secret. A successful "Finished" message implies that both parties calculated the same master secret and thus, the server must have known the private key corresponding to the public key used for key establishment.

Audit:

Verify NTP Server.

Log in to the Dragos Platform CLI.

Execute the following command:

```
config show
```

If an NTP server is configured, the following will be in the output. If the following is not in the output, this is a finding. (**Note:** "servers" will be the configured server.)

```
 "system": {
    "ntp": {
      "enabled": true,
      "servers": [
        "pool.ntp.org"
      ]
    }
  }
```

Remediation:

Configure NTP Server.

Log in to the Dragos Platform CLI.

Execute the following command:

```
config ntp server add ["SERVER_NAME"]
```

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)

Appendix: Summary Table

CIS Benchmark Recommendation		Set Correctly	
		Yes	No
1	**STIG RULES**		
1.1	DRAG-OT-000020 (Manual)	☐	☐
1.2	DRAG-OT-000090 (Manual)	☐	☐
1.3	DRAG-OT-000200 (Manual)	☐	☐
1.4	DRAG-OT-000220 (Manual)	☐	☐
1.5	DRAG-OT-000240 (Manual)	☐	☐
1.6	DRAG-OT-000370 (Manual)	☐	☐
1.7	DRAG-OT-000490 (Manual)	☐	☐
1.8	DRAG-OT-000500 (Manual)	☐	☐
1.9	DRAG-OT-000520 (Manual)	☐	☐
1.10	DRAG-OT-000610 (Manual)	☐	☐
1.11	DRAG-OT-000650 (Manual)	☐	☐
1.12	DRAG-OT-001010 (Manual)	☐	☐
1.13	DRAG-OT-001190 (Manual)	☐	☐
1.14	DRAG-OT-001430 (Manual)	☐	☐
1.15	DRAG-OT-001630 (Manual)	☐	☐
1.16	DRAG-OT-001750 (Manual)	☐	☐
1.17	DRAG-OT-001910 (Manual)	☐	☐
1.18	DRAG-OT-002120 (Manual)	☐	☐
1.19	DRAG-OT-002480 (Manual)	☐	☐

Appendix: Change History

Date	Version	Changes for this version
Sep 12, 2025	1.0.0	Initial CIS Release