CIS Center for Internet Security®

CIS Benchmarks™

# CIS Palo Alto Networks Prisma Cloud Compute STIG Benchmark

v1.0.0 - 08-22-2025

# 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

# Overview

## Target Technology Details

Palo Alto Networks Prisma Cloud Compute Secure Technical Implementation Guide (STIG)

Version: 2 Release: 2 Benchmark

Date: 30 Jan 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 Palo Alto Networks Prisma Cloud Compute 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 Palo Alto Networks Prisma Cloud Compute.

# Recommendations

## 1 STIG RULES

Palo Alto Networks Prisma Cloud Compute

Palo Alto Networks Prisma Cloud Compute Secure Technical Implementation Guide (STIG)

Version: 2 Release: 2 Benchmark

Date: 30 Jan 2025

CLASSIFICATION unclassified

## *1.1 CNTR-PC-000020 (Manual)*

**Profile Applicability:**

- SEVERITY: CAT I

**Description:**

Prisma Cloud Compute Console must use TLS 1.2 for user interface and API access. Communication TCP ports must adhere to the Ports, Protocols, and Services Management Category Assurance Levels (PSSM CAL).

```
GROUP ID: V-253522
RULE ID: SV-253522r960759
```

**Rationale:**

Communication to Prisma Cloud Compute Console's User Interface (UI) and API is protected by TLS v1.2+ (HTTPS). By default, only HTTPS communication to the Console's UI and API endpoints is enabled.

Prisma Cloud Compute TCP port usage is configurable.

Default configuration: TCP 8081 Console user interface and API (HTTP) - disabled by default. TCP 8083 Console user interface and API TLS v1.2 (HTTPS) TCP 8084 Console-to-Defender communication via mutual TLS v1.2 WebSocket session.

Satisfies: SRG-APP-000014-CTR-000040, SRG-APP-000142-CTR-000325, SRG-APP-000185-CTR-000490, SRG-APP-000645-CTR-001410

**Audit:**

For Kubernetes deployment:

Query the ports used by the twistlock-console service:

```
$ kubectl describe svc twistlock-console -n twistlock
```

If the TargetPort management-port-http exists and has a port assignment, this is a finding.

Port: management-port-http 8081/TCP

TargetPort: 8081/TCP

For Docker deployment:

Determine the name of the Console container:

```
docker ps|grep console
```

For example, the Console container is: ad8b41a2fec9 twistlock/private:console_22_01_840

Inspect the container's PortBindings:

```
docker inspect ad8b41a2fec9|grep PortBindings -A 20
```

If port 8081 is listed, this is a finding.

**Remediation:**

For Kubernetes deployment:

Edit the deployment.apps/twistlock-console.

Find the - name: MANAGEMENT_PORT_HTTP setting

Remove the value assignment (e.g., 8081):

- name: MANAGEMENT_PORT_HTTP

value: "8081"

Save and exit the editing session. The Console will restart automatically.

For Docker deployment:

Modify the twistlock.cfg located in the extracted release tar directory.

Remove the value assignment for the MANAGEMENT_PORT_HTTP= variable.

Redeploy the Console using the twistlock.sh script located in the extracted release tar directory.

```
$ sudo ./twisltock.sh -sy onebox
```

**Additional Information:**

CCI-000068 Implement cryptographic mechanisms to protect the confidentiality 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-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

CCI-000877 Employ strong authentication in the establishment of nonlocal maintenance and diagnostic sessions.

- NIST SP 800-53::MA-4 c
- NIST SP 800-53A::MA-4.1 (iv)
- NIST SP 800-53 Revision 4::MA-4 c
- NIST SP 800-53 Revision 5::MA-4 c

## *1.2 CNTR-PC-000030 (Manual)*

**Profile Applicability:**

- SEVERITY: CAT II

**Description:**

Access to Prisma Cloud Compute must be managed based on user need and least privileged using external identity providers for authentication and grouping to role-based assignments when possible.

```
GROUP ID: V-253523
RULE ID: SV-253523r1043176
```

**Rationale:**

Integration with an organization's existing identity management policies technologies reduces the threat of account compromise and misuse.

Centralized authentication services provide additional functionality to fulfill security requirements:

- Multifactor authentication.
- Disabling users after a period of time.
- Encrypted storage and transmission of secure information.
- Secure authentication protocols such as LDAP over TLS or LDAPS using FIPS 140-2 approved encryption modules.
- PKI-based authentication.

Satisfies: SRG-APP-000023-CTR-000055, SRG-APP-000024-CTR-000060, SRG-APP-000025-CTR-000065, SRG-APP-000033-CTR-000095, SRG-APP-000065-CTR-000115, SRG-APP-000068-CTR-000120, SRG-APP-000069-CTR-000125, SRG-APP-000149-CTR-000355, SRG-APP-000150-CTR-000360, SRG-APP-000151-CTR-000365, SRG-APP-000152-CTR-000370, SRG-APP-000163-CTR-000395, SRG-APP-000165-CTR-000405, SRG-APP-000170-CTR-000430, SRG-APP-000173-CTR-000445, SRG-APP-000174-CTR-000450, SRG-APP-000291-CTR-000675, SRG-APP-000292-CTR-000680, SRG-APP-000293-CTR-000685, SRG-APP-000294-CTR-000690, SRG-APP-000317-CTR-000735, SRG-APP-000318-CTR-000740, SRG-APP-000345-CTR-000785, SRG-APP-000397-CTR-000955

**Audit:**

Confirm the Prisma Cloud Console has been configured from SAML-based authentication.

Navigate to Prisma Cloud Compute Console's Manage >> Authentication >> Identity Providers tab.

Verify SAML settings are "Enabled" and an identity provider has been configured.

If SAML settings are not enabled and an identity provider has not been configured, this is a finding.

**Remediation:**

Configure Prisma Cloud Console for SAML-based authentication in which the SAML IdP enforces multifactor authentication (e.g., x509/smartcard authentication).

Navigate to Prisma Cloud Compute Console's Manage >> Authentication >> Identity Providers:

- Click "Add provider".
- For Protocol, select "SAML".
- For Identity provider, select provider.
- Configure the settings and click "Save".
- SAML settings = Enabled
-
- Configure an SAML identity provider that enforces privileged account multifactor authentication for the Prisma Cloud Compute service provider.

**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-000016 Automatically remove or disable temporary and emergency accounts after an organization-defined time-period for each type of account.

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

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-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-004066 For password-based authentication, enforce organization-defined composition and complexity rules.

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

CCI-004061 For password-based authentication, verify when users create or update passwords, that the passwords are not found on the list of commonly-used, expected, or compromised passwords in IA-5 (1) (a).

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

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-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-003627 Disable accounts when the accounts have expired.

- NIST SP 800-53 Revision 5::AC-2 (3) (a)

CCI-004045 Require users to be individually authenticated before granting access to the shared accounts or resources.

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

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)

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-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-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)

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-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)

CCI-002142 The information system terminates shared/group account credentials when members leave the group.

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

## *1.3 CNTR-PC-000120 (Manual)*

**Profile Applicability:**

- SEVERITY: CAT II

**Description:**

Users requiring access to Prisma Cloud Compute's Credential Store must be assigned and accessed by the appropriate role holders.

```
GROUP ID: V-253524
RULE ID: SV-253524r960792
```

**Rationale:**

The container platform keystore is used to store credentials that are used to build a trust between the container platform and an external source. This trust relationship is authorized by the organization. If a malicious user were to have access to the container platform keystore, two negative scenarios could develop:

1. Keys not approved could be introduced.
2. Approved keys could be deleted, leading to the introduction of container images from sources the organization never approved.

To thwart this threat, it is important to protect the container platform keystore and give access to only individuals and roles approved by the organization.

Satisfies: SRG-APP-000033-CTR-000100, SRG-APP-000118-CTR-000240, SRG-APP-000121-CTR-000255, SRG-APP-000133-CTR-000300, SRG-APP-000211-CTR-000530, SRG-APP-000233-CTR-000585, SRG-APP-000340-CTR-000770, SRG-APP-000380-CTR-000900

**Audit:**

Navigate to Prisma Cloud Compute Console's >> Manage >> Authentication >> Users tab.

Inspect the users' role assignments:

- Review role assigned to users. If role and/or the Collection assignment is incorrect, this is a finding.
- If a user is not assigned a role, this is a finding.
- Review users assigned the administrator role. If a user has the administrator role and does not require access, this is a finding.

Navigate to Prisma Cloud Compute Console's >> Manage >> Authentication >> Groups tab.
(Only the Administrator, Operator Prisma Cloud Compute roles have the ability to create/modify policy that could affect runtime behaviors.)
Inspect the groups' role assignments:

- If any users or groups are assigned the Auditor or higher role and do not require access to audit information, this is a finding.
- If a group is not assigned a role, this is a finding.
- If role and/or Collection assignment is incorrect, this is a finding.
- Review groups assigned the Administrator or Operator role. If a group has the Administrator or Operator role and does not require access to Prisma Cloud Compute's Credential Store, this is a finding.

**Remediation:**

Navigate to Prisma Cloud Compute Console's >> Manage >> Authentication >> Users tab.

- Set the users' role assignments to the ones who have the authority to review the audit data.
- Assign roles to all users and groups.
- Assign administrator and operator roles only to the users requiring the rights to modify the Prisma Cloud Compute's Credential Store.
- Remove the Administrator or Operator role for users who do not require access.

Navigate to Prisma Cloud Compute Console's >> Manage >> Authentication >> Groups tab.

- Set the groups' role assignments to the ones who have the authority to review audit data.
- Assign roles to all users and groups.
- Set the groups' Administrator and Operator role assignments to only to the groups requiring the rights to modify the Prisma Cloud Compute's Credential Store.

Adjust user, group, and Collection assignments to align with organizational policies.

**Additional Information:**

CCI-000162 Protect audit information 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-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-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

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-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-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-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)

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)

## *1.4 CNTR-PC-000130 (Manual)*

**Profile Applicability:**

- SEVERITY: CAT II

**Description:**

Prisma Cloud Compute Collections must be used to partition views and enforce organizational-defined need-to-know access.

```
GROUP ID: V-253525
RULE ID: SV-253525r960801
```

**Rationale:**

Prisma Cloud Compute Collections are used to scope rules to target specific resources in an environment, partition views, and enforce which views specific users and groups can access. Collections can control access to data on a need-to-know basis.

**Audit:**

Navigate to Prisma Cloud Compute Console's >> Manage >> Collections and Tags >> Collections tab.

Review the Collections according to organizational policy.

If no organizational-specific Collections are defined, this is a finding.

**Remediation:**

Navigate to Prisma Cloud Compute Console's >> Manage >> Collections and Tags >> Collections tab.

Create a collection:

- Click "Add Collection".
- Enter a name and description and then specify a filter to target specific resources.
- Click "Save".

**Additional Information:**

CCI-001368 Enforce approved authorizations for controlling the flow of information within the system 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

## *1.5 CNTR-PC-000140 (Manual)*

**Profile Applicability:**

- SEVERITY: CAT I

**Description:**

Prisma Cloud Compute Cloud Native Network Firewall (CNNF) automatically monitors layer 4 (TCP) intercontainer communications. Enforcement policies must be created.

```
GROUP ID: V-253526
RULE ID: SV-253526r960804
```

**Rationale:**

Network segmentation and compartmentalization are important parts of a comprehensive defense-in-depth strategy. CNNF works as an east-west firewall for containers. It limits damage by preventing attackers from moving laterally through the environment when they have already compromised the perimeter.

Satisfies: SRG-APP-000039-CTR-000110, SRG-APP-000384-CTR-000915

**Audit:**

Navigate to Prisma Cloud Compute Console's >> Radars >> Settings.

If Container network monitoring is disabled, this is a finding.

If Host network monitoring is disabled, this is a finding.

**Remediation:**

Navigate to Prisma Cloud Compute Console's >> Radars >> Settings.

Set Container network monitoring to "enabled".

Set Host network monitoring to "enabled".

**Additional Information:**

CCI-000381 Configure the system to provide only organization-defined mission essential capabilities.

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

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

## *1.6 CNTR-PC-000240 (Manual)*

**Profile Applicability:**

- SEVERITY: CAT II

**Description:**

Prisma Cloud Compute Defender must be deployed to containerization nodes that are to be monitored.

```
GROUP ID: V-253527
RULE ID: SV-253527r960897
```

**Rationale:**

Container platforms distribute workloads across several nodes. The ability to uniquely identify an event within an environment is critical. Prisma Cloud Compute Container Runtime audits record the time, container, corresponding image, and node where the event occurred.

Satisfies: SRG-APP-000097-CTR-000180, SRG-APP-000100-CTR-000200

**Audit:**

Navigate to Prisma Cloud Compute Console's >> Manage >> Defenders >> Manage tab.

Verify Prisma Cloud Compute Defenders have been deployed to all container runtime nodes to be monitored.

Review the list of deployed Defenders. If a Defender is missing, this is a finding.

**Remediation:**

Navigate to Prisma Cloud Compute Console's >> Manage >> Defenders >> Manage tab.

Deploy Defender to containerization node:

- Select the method of Defender deployment.
- Configure the Defender policy.

**Additional Information:**

CCI-000132 Ensure that audit records containing information that establishes where the event occurred.

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

CCI-001487 Ensure that audit records containing information that establishes the identity of any individuals, subjects, or objects/entities associated with the event.

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

## *1.7 CNTR-PC-000260 (Manual)*

**Profile Applicability:**

- SEVERITY: CAT II

**Description:**

Prisma Cloud Compute must be configured for forensic data collection.

```
GROUP ID: V-253528
RULE ID: SV-253528r960903
```

**Rationale:**

Prisma Cloud Compute correlates raw audit data to actionable security intelligence, enabling a more rapid and effective response to incidents. This reduces the manual, time-consuming task of correlating data.

Prisma Cloud Forensics is a lightweight distributed data recorder that runs alongside all containers in the environment. Prisma Cloud continuously collects detailed runtime information to help incident response teams understand what happened before, during, and after a breach.

Forensic data consists of additional supplemental runtime events that complement the data (audits) already captured by Prisma Cloud's runtime sensors. It provides additional context when trying to identify the root cause of an incident.

Satisfies: SRG-APP-000099-CTR-000190, SRG-APP-000409-CTR-000990

**Audit:**

Navigate to Prisma Cloud Compute Console's >> Manage >> System >> Forensics tab.

If "Forensics data collection" is disabled, this is a finding.

**Remediation:**

Navigate to Prisma Cloud Compute Console's >> Manage >> System >> Forensics tab.

Set "Forensics data collection" to "enabled".

**Additional Information:**

CCI-000134 Ensure that audit records containing information that establishes the outcome of the event.

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

CCI-002884 Log organization-defined audit events for nonlocal maintenance and diagnostic sessions.

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

## *1.8 CNTR-PC-000290 (Manual)*

**Profile Applicability:**

- SEVERITY: CAT I

**Description:**

The configuration integrity of the container platform must be ensured and runtime policies must be configured.

```
GROUP ID: V-253529
RULE ID: SV-253529r960909
```

**Rationale:**

Prisma Cloud Compute's runtime defense is the set of features that provides both predictive and threat-based active protection for running containers.

Consistent application of Prisma Cloud Compute runtime policies ensures the continual application of policies and the associated effects. Prisma Cloud Compute's configurations must be monitored for configuration drift and addressed according to organizational policy.

Satisfies: SRG-APP-000101-CTR-000205, SRG-APP-000384-CTR-000915, SRG-APP-000447-CTR-001100, SRG-APP-000450-CTR-001105, SRG-APP-000507-CTR-001295, SRG-APP-000508-CTR-001300

**Audit:**

Verify runtime policies are enabled.

Navigate to Prisma Cloud Compute Console's Defend >> Runtime.

Select "Container policy".

- If a rule does not exist, this is a finding.
- If "Enable automatic runtime learning" is set to "off", this is a finding.
- Click the three dots in the "Actions" column for the rule.
- If the policy is disabled, this is a finding.
- Click the Container runtime policy.
- If the policy is not scoped to "All", this is a finding.

Select the "App-Embedded policy" tab.

- If a rule does not exist, this is a finding.
- Click the three dots in the "Actions" column for rule "Default - alert on suspicious runtime behavior".
- If the policy is disabled, this is a finding.
- Click the "Default - alert on suspicious runtime behavior" policy row.
- If the "Default - alert on suspicious runtime behavior" policy is not scoped to "All", this is a finding.

Select the "Host policy" tab.

- If a rule does not exist, this is a finding.
- Click the three dots in the "Actions" column for the rule.
- If the policy is disabled, this is a finding.
- Click the Host runtime policy.
- If the policy is not scoped to "All", this is a finding.

**Remediation:**

Enable runtime policies.

Navigate to Prisma Cloud Compute Console's Defend >> Runtime.

Click the tab to be edited.

To add policy (for Host or App-Embedded policy):

- Click "Add rule".
- Enter rule name.
- Scope = All
- Accept the defaults and click "Save".

To enable policy:

- Click the rule's three-dot menu.
- Set to "Enable".

To change scope, click the rule row:

- Change the policy scope to "All".
- Click "Save".

To add container policy:

- Select the "Container policy" tab.
- Set "Enable automatic runtime learning" to "On".

To create a new runtime rule:

- Click "Add rule".
- Configure the following settings:
- Enter rule name
- Scope = All

Select the "Anti-malware" tab.
Set the following:

- Prisma Cloud advanced threat protection = on
- Kubernetes attacks = on
- Suspicious queries to cloud provider APIs = on

Select the "Process" tab.
Set the following:
Process monitoring = enabled
Select the "Network" tab.

Set the following:
IP connectivity = enabled
Select the "File system" tab.
Set the following:

- File system monitoring = enabled
- Accept the defaults and click "Save".

Select the "App-Embedded policy" tab.

- Click the rule's three-dot menu. Set to "Enable".
- Click the rule name row.
- Change the scope to "All".
- Click "Save".

Create a new runtime rule:

- Click "add rule."
- Enter rule name.
- Scope = All
- Accept the defaults and click "Save".

Select the "Host policy" tab.

- Click the rule's three-dot menu. Set to "Enable".
- Click the rule name row.
- Change the scope to "All".
- Click "Save".
- Click "Add rule".
- Enter rule name.
- Scope = All
- Select the "Activities" tab.
- Set the following:
- Host activity monitoring ="Enabled"
- Docker commands = "On"
- New sessions spawned by sshd = "On"
- Commands run with sudo or su = "On"
- Log activity from background apps = "On"
- Track SSH events = "On"
- Accept the defaults and click "Save".

**Additional Information:**

CCI-000135 Generate audit records containing the organization-defined additional information that is to be included in the audit records.

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

CCI-000172 Generate audit records for the event types defined in AU-2 c that include the audit record content defined in AU-3.

- NIST SP 800-53::AU-12 c
- NIST SP 800-53A::AU-12.1 (iv)
- NIST SP 800-53 Revision 4::AU-12 c
- NIST SP 800-53 Revision 5::AU-12 c

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)

CCI-002754 Verify that the system behaves in a predictable and documented manner that reflects organizational and system objectives when invalid inputs are received.

- NIST SP 800-53 Revision 4::SI-10 (3)
- NIST SP 800-53 Revision 5::SI-10 (3)

CCI-002824 Implement organization-defined controls to protect the system memory from unauthorized code execution.

- NIST SP 800-53 Revision 4::SI-16
- NIST SP 800-53 Revision 5::SI-16

## *1.9 CNTR-PC-000310 (Manual)*

**Profile Applicability:**

- SEVERITY: CAT II

**Description:**

Prisma Cloud Compute must be configured to send events to the hosts' syslog.

```
GROUP ID: V-253530
RULE ID: SV-253530r960918
```

**Rationale:**

Event log collection is critical in ensuring the security of a containerized environment due to the ephemeral nature of the workloads. In an environment that is continually in flux, audit logs must be properly collected and secured. Prisma Cloud Compute can be configured to send audit events to the host node's syslog in RFC5424-compliant format.

Satisfies: SRG-APP-000111-CTR-000220, SRG-APP-000181-CTR-000485, SRG-APP-000358-CTR-000805, SRG-APP-000474-CTR-001180, SRG-APP-000516-CTR-000790

**Audit:**

Navigate to Prisma Cloud Compute Console's >> Manage >> Alerts >> Logging tab.

If the Syslog setting is "disabled", this is a finding.

Select the "Manage" tab.

If no Alert Providers are configured, this is a finding.

**Remediation:**

Navigate to Prisma Cloud Compute Console's >> Manage >> Alerts >> Logging tab.

Set Syslog to "enabled".

Select the "Manage" tab.

Click "Add profile".

Complete the form based on the organization. At a minimum, the following Alert triggers must be selected:

- Host vulnerabilities.
- Image vulnerabilities.

Click "Save".

**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)

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

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-001876 Provide an audit reduction capability that supports on-demand reporting requirements.

- NIST SP 800-53 Revision 4::AU-7 a
- NIST SP 800-53 Revision 5::AU-7 a

CCI-002702 Shut the system down, restart the system, and/or initiate organization-defined alternative action(s) when anomalies in the operation of the organization-defined security functions are discovered.

- NIST SP 800-53 Revision 4::SI-6 d
- NIST SP 800-53 Revision 5::SI-6 d

## *1.10 CNTR-PC-000450 (Manual)*

**Profile Applicability:**

- SEVERITY: CAT I

**Description:**

The configuration integrity of the container platform must be ensured and compliance policies must be configured.

```
GROUP ID: V-253532
RULE ID: SV-253532r960960
```

**Rationale:**

Consistent application of Prisma Cloud Compute compliance policies ensures the continual application of policies and the associated effects. Prisma Cloud Compute's configurations must be monitored for configuration drift and addressed according to organizational policy.

Satisfies: SRG-APP-000133-CTR-000305, SRG-APP-000384-CTR-000915, SRG-APP-000435-CTR-001070, SRG-APP-000472-CTR-001170

**Audit:**

Verify compliance policies are enabled.

Navigate to Prisma Cloud Compute Console's Defend >> Compliance.

Select the "Code repositories" tab.

Select the "Repositories" and "CI" tab.

- If "Default – alert all components" does not exist, this is a finding.
- Click the three dots in the "Actions" column for rule "Default - alert all components".
- If the policy is disabled, this is a finding.
- Click the "Default – alert all components" policy row.
- If the "Default - alert on critical and high" policy is not scoped to "All", this is a finding.

Select the "Containers and images" tab.
For the "Deployed" and "CI" tab:

- If the "Default - alert on critical and high" does not exist, this is a finding.
- Click the three dots in the "Actions" column for rule "Default - alert on critical and high".
- If the policy is disabled, this is a finding.
- Click the "Default - alert on critical and high" policy row.
- If the "Default - alert on critical and high" policy is not scoped to "All", this is a finding.

Select the "Hosts" tab.
For the "Running hosts" and "VM images" tab:

- If the "Default - alert on critical and high" does not exist, this is a finding.
- Click the three dots in the "Actions" column for rule "Default - alert on critical and high".
- If the policy is disabled, this is a finding.
- Click the "Default - alert on critical and high" policy row.
- If the "Default - alert on critical and high" policy is not scoped to "All", this is a finding.

Select the "Functions" tab.
For the "Functions" and "CI" tab:

- If the "Default – alert all components" does not exist, this is a finding.
- Click the three dots in the "Actions" column for rule "Default -alert all components".
- If the policy is disabled, this is a finding.
- Click the "Default - alert all components" policy row.
- If the "Default - alert on critical and high" policy is not scoped to "All", this is a finding.

**Remediation:**

Enable compliance policies.

Navigate to Prisma Cloud Compute Console's Defend >> Compliance and click tab to be edited.

To add rule:

- Click "Add rule."
- Enter rule name.
- Scope = All
- Accept the defaults and click "Save".

Click the rule's three-dot menu. Set to "Enable".
Click the rule row.

- Change the policy scope to "All".
- Click "Save".

**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-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)

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

CCI-002696 Verify correct operation of organization-defined security functions.

- NIST SP 800-53 Revision 4::SI-6 a
- NIST SP 800-53 Revision 5::SI-6 a

## *1.11 CNTR-PC-000430 (Manual)*

**Profile Applicability:**

- SEVERITY: CAT I

**Description:**

Prisma Cloud Compute host compliance baseline policies must be set.

```
GROUP ID: V-253531
RULE ID: SV-253531r960960
```

**Rationale:**

Consistent application of Prisma Cloud Compute compliance policies ensures the continual application of policies and the associated effects.

Satisfies: SRG-APP-000133-CTR-000295, SRG-APP-000133-CTR-000310, SRG-APP-000141-CTR-000315, SRG-APP-000384-CTR-000915

**Audit:**

Navigate to Prisma Cloud Compute Console's >> Defend >> Compliance >> Hosts tab >> Running hosts tab.

If a "Default - alert on critical and high" rule does not exist, this is a finding.

Check all the rules to verify the following Actions are not set to "Ignore". (Click "Rule name".)

ID = 8112 - Verify the --anonymous-auth argument is set to false (kube-apiserver) - master node.

ID = 8212 - Verify the --anonymous-auth argument is set to false (kubelet) - worker node.

ID = 8311 - Verify the --anonymous-auth argument is set to false (federation-apiserver).

ID = 81427 - Verify the Kubernetes PKI directory and file ownership are set to root:root.

ID = 81428 - Verify the Kubernetes PKI certificate file permissions are set to 644 or more restrictive.

ID = 8214 - Verify the --client-ca-file argument is set as appropriate (kubelet).

ID = 8227 - Verify the certificate authorities file permissions are set to 644 or more restrictive (kubelet).

ID = 8115 - Verify the --kubelet-https argument is set to true (kube-apiserver).

ID = 8116 - Verify the --insecure-bind-address argument is not set (kube-apiserver).

ID = 8117 - Verify the --insecure-port argument is set to 0 (kube-apiserver) can determine if the Kubernetes API is configured to only listen on the TLS-enabled port (TCP 6443).

ID = 8118 - Verify the --secure-port argument is not set to 0 (kube-apiserver).

ID = 81122 - Verify the --kubelet-certificate-authority argument is set as appropriate (kube-apiserver).

ID = 81123 - Verify the --kubelet-client-certificate and --kubelet-client-key arguments are set as appropriate (kube-apiserver).

ID = 81129 - Verify the --tls-cert-file and --tls-private-key-file arguments are set as appropriate (kube-apiserver).

ID = 82112 - Verify the --tls-cert-file and --tls-private-key-file arguments are set as appropriate (kubelet).

ID = 81141 - Verify the --authorization-mode argument includes RBAC (kube-apiserver).

If any of these checks are set to "Ignore", to all host nodes within the intended monitored environment, this is a finding.

**Remediation:**

Navigate to Prisma Cloud Compute Console's >> Defend >> Compliance >> Hosts tab >> Running hosts tab.

Add Rule:

- Click "Add rule".
- Name = "Default - alert on critical and high"
- Scope = "All"
- Change Action to the values shown below (Change Action).
- Accept the other defaults and click "Save".

Change Action:

- Click "Rule name".
- <Filter on Rule ID>

ID = 8112 - Description (--anonymous-auth argument is set to false (kube-apiserver) - master node)

- Change Action to "Alert" or "Block" (based on organizational needs).
- Click "Save".

ID = 8212 - Description (--anonymous-auth argument is set to false (kubelet) - worker node)

- Change Action to "Alert" or "Block" (based on organizational needs).
- Click "Save".

ID = 8311 - Description (--anonymous-auth argument is set to false (federation-apiserver)).

- Change Action to "Alert" or "Block" (based on organizational needs).
- Click "Save".

ID = 81427 - Description (Kubernetes PKI directory and file ownership is set to root:root).

- Change Action to "Alert" or "Block" (based on organizational needs).
- Click "Save".

ID = 81428 - Description (Kubernetes PKI certificate file permissions are set to 644 or more restrictive).

- Change Action to "Alert" or "Block" (based on organizational needs).
- Click "Save".

ID = 8214 - Description (--client-ca-file argument is set as appropriate (kubelet)).

- Change Action to "Alert" or "Block" (based on organizational needs).
- Click "Save".

ID = 8227 - Description (certificate authorities file permissions are set to 644 or more restrictive (kubelet)).

- Change Action to "Alert" or "Block" (based on organizational needs).
- Click "Save".

ID = 8115 - Description (--kubelet-https argument is set to true (kube-apiserver))

- Change Action to "Alert" or "Block" (based on organizational needs).
- Click "Save".

ID = 8116 - Description (--insecure-bind-address argument is not set (kube-apiserver)).

- Change Action to "Alert" or "Block" (based on organizational needs).
- Click "Save".

ID = 8117 - Description (--insecure-port argument is set to 0 (kube-apiserver) can determine if the Kubernetes API is configured to only listen on the TLS enabled port (TCP 6443)).

- Change Action to "Alert" or "Block" (based on organizational needs).
- Click "Save".

ID = 8118 - Description (--secure-port argument is not set to 0 (kube-apiserver)).

- Change Action to "Alert" or "Block" (based on organizational needs).
- Click "Save".

ID = 81122 - Description (--kubelet-certificate-authority argument is set as appropriate (kube-apiserver)).

- Change Action to "Alert" or "Block" (based on organizational needs).
- Click "Save".

ID = 81123 - Description (--kubelet-client-certificate and --kubelet-client-key arguments are set as appropriate (kube-apiserver)).
ID = 81129 - Description (--tls-cert-file and --tls-private-key-file arguments are set as appropriate (kube-apiserver)).

- Change Action to "Alert" or "Block" (based on organizational needs).
- Click "Save".

ID = 82112 - Description (--tls-cert-file and --tls-private-key-file arguments are set as appropriate (kubelet)).

- Change Action to "Alert" or "Block" (based on organizational needs).
- Click "Save".

ID = 81141 - Description (--authorization-mode argument includes RBAC (kube-apiserver)).

- Change Action to "Alert" or "Block" (based on organizational needs).
- Click "Save".

**Additional Information:**

CCI-000381 Configure the system to provide only organization-defined mission essential capabilities.

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

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-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)

## *1.12 CNTR-PC-000480 (Manual)*

**Profile Applicability:**

- SEVERITY: CAT II

**Description:**

Images stored within the container registry must contain only images to be run as containers within the container platform.

```
GROUP ID: V-253533
RULE ID: SV-253533r960963
```

**Rationale:**

The Prisma Cloud Compute Trusted Images feature allows the declaration, by policy, of which registries, repositories, and images to trust and how to respond when untrusted images are started in the organization's environment.

Satisfies: SRG-APP-000141-CTR-000320, SRG-APP-000386-CTR-000920

**Audit:**

Navigate to Prisma Cloud Compute Console's >> Defend >> Compliance Trusted Images tab.

Select the "Trust groups" tab.

If there is no Group, this is a finding.

Select the "Policy" tab.

If the Trusted Images Rules is set to "off", this is a finding.

If a rule does not exist, this is a finding.

Click the three dots in the "Actions" column for rule.

If the policy is disabled, this is a finding.

Click the policy row.

If the policy is not scoped to "All", this is a finding.

**Remediation:**

Navigate to Prisma Cloud Compute Console's >> Defend >> Compliance >> Trusted Images tab.

Select the "Trust groups" tab.

Create a trusted group:

- Click "Add Group".
- Name: "IronBank"
- Specify a registry or repository: https://ironbank.dso.mil
- Click "Add to group".
- Specify a registry or repository: https://registry1.dso.mil/
- (There are two group images total.)
- Click "Save".

Select the "Policy" tab.
Set the Trusted Images Rules to "on".
If a rule does not exist:

- Click "Add rule".
- Rule name = "IronBank"
- Scope = "All"

Allowed:

- Click "Select groups".
- Select "IronBank".
- Click "Apply".
- Keep all defaults and click "Save".

Enable policy:

- Click the "Default - alert all components" policy three-dot menu.
- Set to "Enable".

Policy row scope:

- Click the policy rows.
- Change the policy scope to all images and containers within the intended monitored environment.
- Click "Save".

**Additional Information:**

CCI-000381 Configure the system to provide only organization-defined mission essential capabilities.

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

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)

## *1.13 CNTR-PC-000500 (Manual)*

**Profile Applicability:**

- SEVERITY: CAT II

**Description:**

Prisma Cloud Compute must use TCP ports above 1024.

```
GROUP ID: V-253534
RULE ID: SV-253534r1043177
```

**Rationale:**

Privileged ports are ports below 1024 that require system privileges for their use. If containers are able to use these ports, the container must be run as a privileged user. The container platform must stop containers that try to map to these ports directly. Allowing nonprivileged ports to be mapped to the container-privileged port is the allowable method when a certain port is needed. Prisma Cloud Compute default TCP ports are 8083 (Console UI and API) and 8084 (Console-to-Defender communication). To use TCP ports below 1024, the Console would have to be configured to use privileged ports.

**Audit:**

For Kubernetes deployment:

Query the ports used by the twistlock-console service:

```
$ kubectl describe svc twistlock-console -n twistlock
```

If any port number is below 1024, this is a finding.

For Docker deployment:

Determine the name of the Console container:

```
docker ps|grep console
```

For example, the Console container is: `ad8b41a2fec9 ad8b41a2fec9 twistlock/private:console_22_01_840`

Inspect the container's PortBindings:

```
docker inspect ad8b41a2fec9|grep PortBindings -A 20
```

If the port is below 1024, this is a finding.

**Remediation:**

For Kubernetes deployment:

Edit the deployment.apps/twistlock-console.

Find the - name: TargetPorts below 1024.

Change to port number above 1024.

Save and exit the editing session. The Console will restart automatically.

For Docker deployment:

Modify the twistlock.cfg located in the extracted release tar directory.

Change any port assignment below 1024 to above 1024:

```
MANAGEMENT_PORT_HTTP=

MANAGEMENT_PORT_HTTPS=8083

COMMUNICATION_PORT=8084
```

Redeploy the Console using the twistlock.sh script in the extracted release tar directory:

```
$ sudo ./twisltock.sh -sy onebox
```

**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

## *1.14 CNTR-PC-000510 (Manual)*

**Profile Applicability:**

- SEVERITY: CAT II

**Description:**

All Prisma Cloud Compute users must have a unique, individual account.

```
GROUP ID: V-253535
RULE ID: SV-253535r1051115
```

**Rationale:**

Prisma Cloud Compute does not have a default account. During installation, the installer creates an administrator. This account can be removed once other accounts have been added. To ensure accountability and prevent unauthenticated access, users must be identified and authenticated to prevent potential misuse and compromise of the system.

**Audit:**

Confirm there is only one "break glass" local administrative account.

Navigate to Prisma Cloud Compute Console's Manage >> Authentication >> Users tab.

Only the administrative break glass account is allowed to have Authentication Method = Local.

For all other accounts, Authentication Method = SAML.

If any local account, except the administrative break glass account, has Authentication Method set to other than "SAML", this is a finding.

**Remediation:**

Navigate to Prisma Cloud Compute Console's >> Manage >> Authentication >> Users tab.

Ensure only the break glass administrator account is a "local" account.

Delete all other local accounts and use the SAML identity provider for all authentication and authorization to the Prisma Cloud Compute Console.

**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

## *1.15 CNTR-PC-000530 (Manual)*

**Profile Applicability:**

- SEVERITY: CAT II

**Description:**

Prisma Cloud Compute Console must run as nonroot user (uid 2674).

```
GROUP ID: V-253536
RULE ID: SV-253536r1051115
```

**Rationale:**

Containers not requiring root-level permissions must run as a unique user account. To ensure accountability and prevent unauthenticated access to containers, the user the container is using to execute must be uniquely identified and authenticated to prevent potential misuse and compromise of the system.

**Audit:**

Locate the node in which the Prisma Cloud Compute Console container is running.

Determine the process owner for "app/server".

Execute:

```
ps -aux | grep "/app/server
```

If the process is owned by root, this is a finding.

**Remediation:**

In the root directory of the extracted release tar file, modify the twistlock.cfg file's line:

```
RUN_CONSOLE_AS_ROOT=false
```

For Kubernetes deployment, perform these additional steps:

When generating the twistlock_console.yaml deployment file, supply the --run-as-user flag.

```
Linux/twistcli console export kubernetes --service-type ClusterIP --
run-as-user 2674
```

Modify the resulting twistlock_console.yaml file to include fsGroup: 2674 within the Deployment pod specification's securityContext:

```
securityContext: fsGroup: 2674
```

Add runAsGroup: 2674 to the container specification's securityContext:

```
securityContext: runAsUser: 2674
```

```
runAsGroup: 2674
```

**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

## *1.16 CNTR-PC-000590 (Manual)*

**Profile Applicability:**

- SEVERITY: CAT II

**Description:**

Prisma Cloud Compute must be configured with unique user accounts.

```
GROUP ID: V-253537
RULE ID: SV-253537r1015785
```

**Rationale:**

Sharing accounts, such as group accounts, reduces the accountability and integrity of Prisma Cloud Compute.

**Audit:**

Navigate to Prisma Cloud Compute Console's >> Manage >> Authentication >> Users tab.

Review the accounts for uniqueness. If there are shared local accounts, this is a finding.

**Remediation:**

Navigate to Prisma Cloud Compute Console's Manage >> Authentication >> Users tab.

Delete shared accounts and create a unique account for every Prisma Cloud Compute user.

Delete shared accounts:

- Click the three-dot menu.
- Click "Delete" and confirm "Delete User".

Create a local user account where the local user account is unique:

- Click "+Add user".
- Complete the form and click "Save".

**Additional Information:**

CCI-004045 Require users to be individually authenticated before granting access to the shared accounts or resources.

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

CCI-000770 The organization requires individuals to be authenticated with an individual authenticator when a group authenticator is employed.

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

## *1.17 CNTR-PC-000640 (Manual)*

**Profile Applicability:**

- SEVERITY: CAT II

**Description:**

Prisma Cloud Compute local accounts must enforce strong password requirements.

```
GROUP ID: V-253538
RULE ID: SV-253538r1015786
```

**Rationale:**

Use of a complex password helps to increase the time and resources required to compromise the password. Password complexity, or strength, is a measure of the effectiveness of a password in resisting attempts at guessing and brute-force attacks.

Password complexity is one factor of several that determine how long it takes to crack a password. The more complex the password is, the greater the number of possible combinations that must be tested before the password is compromised.

Satisfies: SRG-APP-000164-CTR-000400, SRG-APP-000166-CTR-000410, SRG-APP-000167-CTR-000415, SRG-APP-000168-CTR-000420, SRG-APP-000169-CTR-000425, SRG-APP-000389-CTR-000925, SRG-APP-000391-CTR-000935, SRG-APP-000400-CTR-000960

**Audit:**

Navigate to Prisma Cloud Compute Console's >> Manage >> Authentication >> Logon tab.

- If "Token validity period" is greater than 15, this is a finding.
- If "Enable context sensitive help and single sign on to the Prisma Cloud Support site" is set to "on", this is a finding.
- If "Disable basic authentication for the API" is set to "off", this is a finding.
- If "Require strong passwords for local accounts" is set to "off", this is a finding.
- If "Require strict certificate validation in Defender installation links" is set to "on", this is a finding.

**Remediation:**

Navigate to Prisma Cloud Compute Console's >> Manage >> Authentication >>

Logon tab.

- Set "Token validity period" to 15 or less.
- Set "Enable context sensitive help and single sign on to the Prisma Cloud Support site" to "off".
- Set "Disable basic authentication for the API" to "on".
- Set "Require strong passwords for local accounts" to "on".
- Set "Require strict certificate validation in Defender installation links" to "off".
- Click "Save" and "Restart".

**Additional Information:**

CCI-004066 For password-based authentication, enforce organization-defined composition and complexity rules.

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

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-002007 Prohibit the use of cached authenticators after an organization-defined time period.

- NIST SP 800-53 Revision 4::IA-5 (13)
- NIST SP 800-53 Revision 5::IA-5 (13)

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-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-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-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

## *1.18 CNTR-PC-000750 (Manual)*

**Profile Applicability:**

- SEVERITY: CAT II

**Description:**

Prisma Cloud Compute must be configured to require local user accounts to use x.509 multifactor authentication.

```
GROUP ID: V-253539
RULE ID: SV-253539r1015787
```

**Rationale:**

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: (i) something a user knows (e.g., password/PIN); (ii) something a user has (e.g., cryptographic identification device, token); or (iii) something a user is (e.g., biometric).

User access to Prisma Cloud Compute must use multifactor (x.509 based) authentication.

Satisfies: SRG-APP-000177-CTR-000465, SRG-APP-000391-CTR-000935, SRG-APP-000401-CTR-000965, SRG-APP-000402-CTR-000970, SRG-APP-000605-CTR-001380

**Audit:**

Navigate to Prisma Cloud Compute Console's >> Manage >> Authentication >> System Certificate tab.

If not performing direct smart card authentication to the console, this is not a finding.

If performing direct smart card authentication to the console:

Revocation block: If "Enable certificate revocation checking" is set to "Off", this is a finding.

Show Advanced certificate configuration:

- In the "Certificate-based authentication to Console" block, verify the issuing CA(s) of the end users' certificates are within the Console CA certificate(s) field.
- If there is no users' certificates, this is a finding.

Click the "Users" tab.
Review accounts with Authentication method "Local".
If the local user account's name does not match the user's x.509 certificate's subjectName or the subject alternative name's PrincipalName value, this is a finding.

**Remediation:**

Navigate to Prisma Cloud Compute Console's >> Manage >> Authentication >> System Certificate tab.

Revocation block: Set "Enable certificate revocation checking" to "On" and click "Save".

In the "Certificate-based authentication to Console" block, import the smart card's issuing CA's chain of trust to the Console CA certificate(s) field. Click "Save".

Click the "Users" tab. (Accounts cannot be edited. They must be removed and recreated correctly.)

Delete account:

- Click the three-dot menu.
- Click "Delete" and confirm "Delete User".

Create a local user account where the local user account name matches the user's x.509 certificate's subjectName or subject alternative name's PrincipalName value:

- Click "+Add user".
- Authentication Source = Local
- Username = subject alternative name's PrincipalName value
- Password = random password that is not given to the user
- Assign Role.
- Click "Save".

**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)

CCI-001857 Defines the personnel, roles, and/or locations to receive alerts when organization-defined audit failure events occur.

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

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-004068 For public key-based authentication, implement a local cache of revocation data to support path discovery and validation.

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

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-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)

## *1.19 CNTR-PC-000850 (Manual)*

**Profile Applicability:**

- SEVERITY: CAT II

**Description:**

Prisma Cloud Compute must prevent unauthorized and unintended information transfer.

```
GROUP ID: V-253540
RULE ID: SV-253540r961149
```

**Rationale:**

Prisma Cloud Compute Compliance policies must be enabled to ensure running containers do not access privileged resources.

Satisfies: SRG-APP-000243-CTR-000595, SRG-APP-000243-CTR-000600, SRG-APP-000246-CTR-000605, SRG-APP-000342-CTR-000775

**Audit:**

Navigate to Prisma Cloud Compute Console's Defend >> Compliance >> Containers and images tab >> Deployed tab.

For each rule name, click the rule and confirm the following checks:

(Filter on ID)

ID = 54: Do not use privileged container

ID = 5525: Restrict container from acquiring additional privileges are not configured

ID = 59: Do not share the host's network namespace

ID = 515: Do not share the host's process namespace

ID = 516: Do not share the host's IPC namespace

ID = 517: Do not directly expose host devices to containers

ID = 520: Do not share the host's UTS namespace

ID = 530: Do not share the host's user namespaces

ID = 55: Do not mount sensitive host system directories on containers

ID = 57: Do not map privileged ports within containers

ID = 5510: Limit memory usage for container

ID = 5511: Set container CPU priority appropriately

ID = 599: Container is running as root

ID = 41 Image should be created with a non-root user

If the action for each rule is set to "Ignore", this is a finding.

**Remediation:**

Navigate to Prisma Cloud Compute Console's Defend >> Compliance >> Containers and images tab >> Deployed tab.

Change action:

(Click the rule name)

<Filter on Rule ID>

ID = 54 - Description (Do not use privileged container)

Change Action to "Alert" or "Block" (based on organizational needs).

Click "Save".

ID = 5525 - Description (Restrict container from acquiring additional privileges are not configured)

Change Action to "Alert" or "Block" (based on organizational needs).

Click "Save".

ID = 59 - Description (Do not share the host's network namespace)

Change Action to "Alert" or "Block" (based on organizational needs).

Click "Save".

ID = 515 - Description (Do not share the host's process namespace)

Change Action to "Alert" or "Block" (based on organizational needs).

Click "Save".

ID = 516 - Description (Do not share the host's IPC namespace)

Change Action to "Alert" or "Block" (based on organizational needs).

Click "Save".

ID = 517 - Description (Do not directly expose host devices to containers)

Change Action to "Alert" or "Block" (based on organizational needs).

Click "Save".

ID = 520 - Description (Do not share the host's UTS namespace)

Change Action to "Alert" or "Block" (based on organizational needs).

Click "Save".

ID = 530 - Description (Do not share the host's user namespaces)

Change Action to "Alert" or "Block" (based on organizational needs).

Click "Save".

ID = 55 - Description (Do not mount sensitive host system directories on containers)

Change Action to "Alert" or "Block" (based on organizational needs).

Click "Save".

ID = 57 - Description (Do not map privileged ports within containers)

Change Action to "Alert" or "Block" (based on organizational needs).

Click "Save".

ID = 5510 - Description (Limit memory usage for container)

Change Action to "Alert" or "Block" (based on organizational needs).

Click "Save".

ID = 5511 - Description (Set container CPU priority appropriately)

Change Action to "Alert" or "Block" (based on organizational needs).

Click "Save".

ID = 599 - Description (Container is running as root)

Change Action to "Alert" or "Block" (based on organizational needs).

Click "Save".

ID = 41 - Description (Image should be created with a non-root user)

Change Action to "Alert" or "Block" (based on organizational needs).

Click "Save".

**Additional Information:**

CCI-001090 Prevent unauthorized and unintended information transfer via shared system resources.

- NIST SP 800-53::SC-4
- NIST SP 800-53A::SC-4.1
- NIST SP 800-53 Revision 4::SC-4
- NIST SP 800-53 Revision 5::SC-4

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-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)

## *1.20 CNTR-PC-000880 (Manual)*

**Profile Applicability:**

- SEVERITY: CAT II

**Description:**

Prisma Cloud Compute must not write sensitive data to event logs.

```
GROUP ID: V-253541
RULE ID: SV-253541r961167
```

**Rationale:**

The determination of what is sensitive data varies from organization to organization. The organization must ensure the recipients for the event log information have a need to know and the log is sanitized based on the audience.

**Audit:**

Navigate to Prisma Cloud Compute Console's >> Manage >> System >> General tab.

Inspect the Log Scrubbing section. If "Automatically scrub secrets from runtime events" is "off", this is a finding.

**Remediation:**

Navigate to Prisma Cloud Compute Console's >> Manage >> System >> General tab.

In the Log Scrubbing section, set "Automatically scrub secrets from runtime events" to "on" and click "Save".

**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

## *1.21 CNTR-PC-001030 (Manual)*

**Profile Applicability:**

- SEVERITY: CAT II

**Description:**

The node that runs Prisma Cloud Compute containers must have sufficient disk space to allocate audit record storage capacity in accordance with organization-defined audit record storage requirements.

```
GROUP ID: V-253542
RULE ID: SV-253542r961392
```

**Rationale:**

To ensure sufficient storage capacity in which to write the audit logs, Prisma Cloud compute must be able to allocate audit record storage capacity.

**Audit:**

When deploying Prisma Cloud Compute within a Kubernetes cluster, the Console's persistent value is by default 100GB.

The logs are stored within this persistent volume. Within the Kubernetes cluster, issue the command "kubectl get pv".

If the twistlock/twistlock-console claim's capacity is not 100GB or greater, this is a finding.

**Remediation:**

When deploying the Prisma Cloud Console, specify the size of the persistent volume with the "—persistent-volume-storage" parameter.

**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

## *1.22 CNTR-PC-001170 (Manual)*

**Profile Applicability:**

- SEVERITY: CAT I

**Description:**

The configuration integrity of the container platform must be ensured and vulnerabilities policies must be configured.

```
GROUP ID: V-253543
RULE ID: SV-253543r961473
```

**Rationale:**

Prisma Cloud Compute's vulnerabilities defense is the set of features that provides both predictive and threat-based active protection for running containers.

Consistent application of Prisma Cloud Compute vulnerabilities policies ensures the continual application of policies and the associated effects. Prisma Cloud Compute's configurations must be monitored for configuration drift and addressed according to organizational policy.

Satisfies: SRG-APP-000384-CTR-000915, SRG-APP-000384-CTR-000915, SRG-APP-000456-CTR-001125, SRG-APP-000516-CTR-001335

**Audit:**

To verify that vulnerabilities policies are enabled, navigate to Prisma Cloud Compute Console's Defend >> Vulnerabilities.

Select the "Code repositories" tab.

For the "Repositories" and "CI" tab:

- If "Default - alert all components" does not exist, this is a finding.
- Click the three dots in the "Actions" column for rule "Default - alert all components".
- If the policy is disabled, this is a finding.
- Click the "Default - alert all components" policy row.
- If "Default - alert all components" is not scoped to "All", this is a finding.

Select the "Images" tab.
For the "CI" and "Deployed" tab:

- If "Default - alert all components" does not exist, this is a finding.
- Click the three dots in the "Actions" column for rule "Default - alert all components".
- If the policy is disabled, this is a finding.

- Click the "Default - alert all components" policy row.
- If "Default - alert all components" is not scoped to "All", this is a finding.

Select the "Hosts" tab.
For the "Running hosts" and "VM images" tab:

- If the "Default - alert all components" does not exist, this is a finding.
- Click the three dots in the "Actions" column for rule "Default - alert all components".
- If the policy is disabled, this is a finding.
- Click the "Default - alert all components" policy row.
- If "Default - alert all components" is not scoped to "All", this is a finding.

Select the "Functions" tab.
For the "Functions" and "CI" tab:

- If the "Default - alert all components" does not exist, this is a finding.
- Click the three dots in the "Actions" column for rule "Default - alert all components".
- If the policy is disabled, this is a finding.
- Click the "Default - alert all components" policy row.
- If "Default - alert all components" is not scoped to "All", this is a finding.

**Remediation:**

To enable vulnerabilities policies, navigate to Prisma Cloud Compute Console's Defend >> Vulnerabilities. Click tab to be edited.

To add rule:

- Click "Add rule".
- Enter rule name.
- Scope = All
- Accept the defaults and click "Save".

Click the rule three-dot menu. Set to "Enable".
Click the rule row:

- Change the policy scope to "All".
- Click "Save".

**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

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)

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

## *1.23 CNTR-PC-001220 (Manual)*

**Profile Applicability:**

- SEVERITY: CAT I

**Description:**

Prisma Cloud Compute must be configured to scan images that have not been instantiated as containers.

```
GROUP ID: V-253544
RULE ID: SV-253544r961473
```

**Rationale:**

Prisma Cloud Compute ships with "only scan images with running containers" set to "on". To meet the requirements, "only scan images with running containers" must be set to "off" to disable or remove components that are not required.

**Audit:**

Navigate to Prisma Cloud Compute Console's >> Manage >> System >> Scan tab.

Verify that for Running images, For Running images, "Only scan images with running containers" is set to "Off".

If "Only scan images with running containers" is set to "On", this is a finding.

**Remediation:**

Navigate to Prisma Cloud Compute Console's >> Manage >> System >> Scan tab.

For Running images:

- Set "Only scan images with running containers" = "Off".
- Click "Save".

**Additional Information:**

CCI-000381 Configure the system to provide only organization-defined mission essential capabilities.

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

## *1.24 CNTR-PC-001250 (Manual)*

**Profile Applicability:**

- SEVERITY: CAT II

**Description:**

Prisma Cloud Compute Defender must reestablish communication to the Console via mutual TLS v1.2 WebSocket session.

```
GROUP ID: V-253545
RULE ID: SV-253545r986174
```

**Rationale:**

When the secure WebSocket session between the Prisma Cloud Compute Console and Defenders is disconnected, the Defender will continually attempt to reestablish the session. Without reauthentication, unidentified or unknown devices may be introduced; thereby facilitating malicious activity.

The Console must be configured to remove a Defender that has not established a connection in a specified period of days.

**Audit:**

Navigate to Prisma Cloud Compute Console's >> Manage >> Defenders.

Select the "Manage" tab. Select the "Defenders" tab.

Click "Advanced Settings".

If "Automatically remove disconnected Defenders after (days)" is not configured to the organization's policies, this is a finding.

**Remediation:**

Navigate to Prisma Cloud Compute's Manage >> Defenders.

Select the "Manage" tab. Select the "Defenders" tab.

Click "Advanced Settings".

Set the "Automatically remove disconnected Defenders after (days)" value to the organization's defined period.

**Additional Information:**

CCI-002036 Defines the circumstances or situations under which users will be required to reauthenticate.

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

## *1.25 CNTR-PC-001350 (Manual)*

**Profile Applicability:**

- SEVERITY: CAT II

**Description:**

Prisma Cloud Compute Defender containers must run as root.

```
GROUP ID: V-253546
RULE ID: SV-253546r1050656
```

**Rationale:**

In certain situations, the nature of the vulnerability scanning may be more intrusive, or the container platform component that is the subject of the scanning may contain highly sensitive information. To protect the sensitive nature of such scanning, Prisma Cloud Compute Defenders perform the vulnerability scanning function. The Defender container must run as root and not privileged.

**Audit:**

Verify that when deploying the Defender via daemonSet, "Run Defenders as privileged" is set to "On".

Verify the Defender containers were deployed using the daemonSet.yaml in which the securityContext is privileged (privileged = "on").

If "Run Defenders as privileged" is not set to "On" or the Defender containers were not deployed using the daemonSet.yaml in which the securityContext - privileged = "on", this is a finding.

**Remediation:**

Redeploy the Defender with appropriate rights by setting "Run Defenders as privileged" to "On".

Delete the old twistlock-defender-ds daemonSet and redeploy daemonSet with the new yaml in which the securityContext - privileged = "on".

**Additional Information:**

CCI-001067 Implement privileged access authorization to organization-identified system components for organization-defined vulnerability scanning activities.

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

## *1.26 CNTR-PC-001380 (Manual)*

**Profile Applicability:**

- SEVERITY: CAT II

**Description:**

Prisma Cloud Compute must run within a defined/separate namespace (e.g., Twistlock).

```
GROUP ID: V-253547
RULE ID: SV-253547r961608
```

**Rationale:**

Namespaces are a key boundary for network policies, orchestrator access control restrictions, and other important security controls. Prisma Cloud Compute containers running within a separate and exclusive namespace will inherit the namespace's security features. Separating workloads into namespaces can help contain attacks and limit the impact of mistakes or destructive actions by authorized users.

**Audit:**

Inspect the Kubernetes namespace in which Prisma Cloud Compute is deployed:

```
$ kubectl get pods -n twistlock
NAME READY STATUS RESTARTS AGE
twistlock-console-855744b66b-xs9cm 1/1 Running 0 4d6h
twistlock-defender-ds-99zj7 1/1 Running 0 58d
twistlock-defender-ds-drsh8 1/1 Running 0 58d
```

Inspect the list of pods.

If a non-Prisma Cloud Compute (does not start with "twistlock") pod is running in the same namespace, this is a finding.

**Remediation:**

Deploy the Prisma Cloud Compute Console and Defender containers within a distinct namespace.

**Additional Information:**

CCI-002530 Maintain a separate execution domain for each executing system process.

- NIST SP 800-53 Revision 4::SC-39
- NIST SP 800-53 Revision 5::SC-39

## *1.27 CNTR-PC-001390 (Manual)*

**Profile Applicability:**

- SEVERITY: CAT I

**Description:**

Prisma Cloud Compute must protect the confidentiality and integrity of transmitted information.

```
GROUP ID: V-253548
RULE ID: SV-253548r961632
```

**Rationale:**

Without protection of the transmitted information, confidentiality and integrity may be compromised since unprotected communications can be intercepted and either read or altered.

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:**

Navigate to Prisma Cloud Compute Console's >> Manage >> System >> General tab.

Inspect the Telemetry section.

If "Share telemetry on product usage with Palo Alto Networks" is "On", this is a finding.

If "Allow admins and operators to upload logs to Customer Support directly from Console UI" is "On", this is a finding.

**Remediation:**

Navigate to Prisma Cloud Compute Console's >> Manage >> System >> General tab.

In the Telemetry section:

Set "Share telemetry on product usage with Palo Alto Networks" to "Off".

Set "Allow admins and operators to upload logs to Customer Support directly from Console UI" to "Off".

Click "Save".

**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

## *1.28 CNTR-PC-001440 (Manual)*

**Profile Applicability:**

- SEVERITY: CAT II

**Description:**

Prisma Cloud Compute must be running the latest release.

```
GROUP ID: V-253549
RULE ID: SV-253549r961677
```

**Rationale:**

Prisma Cloud Compute releases are distributed as Docker images. Each release updates or removes components as needed based on the vulnerabilities associated with the component or the functional need of the component.

**Audit:**

Navigate to the Prisma Cloud Compute Console.

In the top right corner, click the bell icon. A banner with the version will display.

If there is a newer version, this is a finding.

**Remediation:**

Upgrade the Prisma Cloud Compute Console and Defenders according to published procedures.

https://docs.twistlock.com/docs/compute_edition/upgrade/upgrade_process_self_hosted.html

**Additional Information:**

CCI-002617 Remove previous versions of organization-defined software components after updated versions have been installed.

- NIST SP 800-53 Revision 4::SI-2 (6)
- NIST SP 800-53 Revision 5::SI-2 (6)

## *1.29 CNTR-PC-001470 (Manual)*

**Profile Applicability:**

- SEVERITY: CAT II

**Description:**

Prisma Cloud Compute's Intelligence Stream must be kept up to date.

```
GROUP ID: V-253550
RULE ID: SV-253550r961683
```

**Rationale:**

The Prisma Cloud Compute Console pulls the latest vulnerability and threat information from the Intelligence Stream (intelligence.twistlock.com). The Prisma Cloud Intelligence Stream provides timely vulnerability data collected and processed from a variety of certified upstream sources.

**Audit:**

Navigate to Prisma Cloud Compute Console's >> Manage >> System >> Intelligence tab.

If the "Last streams update" date is older than 36 hours, this is a finding.

**Remediation:**

Prisma Cloud Compute Console's ability to communicate with the Intelligence Stream endpoint (https://intelligence.twistlock.com) dictates the method of vulnerability updates.

If the Console is able to communicate with the internet, ensure that intelligence.twistlock.com is resolvable, routable, and can establish a TLS session on TCP port 443.

If the Console is in an isolated environment and is unable to communicate with the internet, configure the Console to receive Intelligence Stream updates using one of the following methods:

- Manual import.
- Central console.
- HTTP/S distribution point.

https://docs.paloaltonetworks.com/prisma/prisma-cloud/22-01/prisma-cloud-compute-edition-admin/tools/update_intel_stream_offline.html

**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

## *1.30 CNTR-PC-001490 (Manual)*

**Profile Applicability:**

- SEVERITY: CAT II

**Description:**

Configuration of Prisma Cloud Compute must be continuously verified.

```
GROUP ID: V-253551
RULE ID: SV-253551r961734
```

**Rationale:**

Prisma Cloud Compute's configuration of Defender deployment must be monitored to ensure monitoring and protection of the environment is in accordance with organizational policy.

**Audit:**

Navigate to Prisma Cloud Compute Console's >> Manage >> Defenders.

Select the "Manage" tab. Select the "Defenders" tab.

Determine the deployment status of the Defenders.

If a Defender is not deployed to intended workload(s) to be protected, this is a finding.

**Remediation:**

Navigate to Prisma Cloud Compute Console's >> Manage >> Defenders.

Select the "Manage" tab. Select the "Defenders" tab.

Deploy Defender to containerization node. Select the method of Defender deployment.

https://docs.paloaltonetworks.com/prisma/prisma-cloud/22-01/prisma-cloud-compute-edition-admin/install/defender_types.html

**Additional Information:**

CCI-002699 Perform verification of the correct operation of organization-defined security functions: when the system is in an organization-defined transitional state; upon command by a user with appropriate privileges; and/or on an organization-defined frequency.

- NIST SP 800-53 Revision 4::SI-6 b
- NIST SP 800-53 Revision 5::SI-6 b

## *1.31 CNTR-PC-001770 (Manual)*

**Profile Applicability:**

- SEVERITY: CAT II

**Description:**

Prisma Cloud Compute release tar distributions must have an associated SHA-256 digest.

```
GROUP ID: V-253552
RULE ID: SV-253552r961896
```

**Rationale:**

Each Prisma Cloud Compute release's tar file has an associated SHA-256 digest hash value to ensure the components have not been modified.

**Audit:**

Offline Intelligence Stream:

If using Iron Bank distribution of Prisma Cloud Compute Console and Defenders, verify the Console and Defender imageID SHA256 values match the Palo Alto Networks published release values.

For the Console and Defender images, perform the following command:

```
$ docker inspect twistlock/private:console_22_01_839 | grep '"Image":'
        "Image":
"sha256:dcd881fe9c796ed08867c242389737c4f2e8ab463377a90deddc0add4c3e8524",
```

If the imageID values do not match the published release SHA256 for the version of the image release, this is a finding.

Note: Image tag will be the release number, e.g., console_22_01_839. Published release image sha values are published here: https://docs.paloaltonetworks.com/prisma/prisma-cloud/prisma-cloud-compute-edition-public-sector/isolated_upgrades/releases.html

**Remediation:**

Deploy the latest version from https://support.paloaltonetworks.com.

**Additional Information:**

CCI-000803 Implement mechanisms for authentication to a cryptographic module that meet the requirements of applicable laws, Executive Orders, directives, policies, regulations, standards, and guidance for such authentication.

- NIST SP 800-53::IA-7
- NIST SP 800-53A::IA-7.1
- NIST SP 800-53 Revision 4::IA-7
- NIST SP 800-53 Revision 5::IA-7

# Appendix: Summary Table

| CIS Benchmark Recommendation | | Set Correctly | |
|---|---|---|---|
| | | Yes | No |
| **1** | **STIG RULES** | | |
| 1.1 | CNTR-PC-000020 (Manual) | ☐ | ☐ |
| 1.2 | CNTR-PC-000030 (Manual) | ☐ | ☐ |
| 1.3 | CNTR-PC-000120 (Manual) | ☐ | ☐ |
| 1.4 | CNTR-PC-000130 (Manual) | ☐ | ☐ |
| 1.5 | CNTR-PC-000140 (Manual) | ☐ | ☐ |
| 1.6 | CNTR-PC-000240 (Manual) | ☐ | ☐ |
| 1.7 | CNTR-PC-000260 (Manual) | ☐ | ☐ |
| 1.8 | CNTR-PC-000290 (Manual) | ☐ | ☐ |
| 1.9 | CNTR-PC-000310 (Manual) | ☐ | ☐ |
| 1.10 | CNTR-PC-000450 (Manual) | ☐ | ☐ |
| 1.11 | CNTR-PC-000430 (Manual) | ☐ | ☐ |
| 1.12 | CNTR-PC-000480 (Manual) | ☐ | ☐ |
| 1.13 | CNTR-PC-000500 (Manual) | ☐ | ☐ |
| 1.14 | CNTR-PC-000510 (Manual) | ☐ | ☐ |
| 1.15 | CNTR-PC-000530 (Manual) | ☐ | ☐ |
| 1.16 | CNTR-PC-000590 (Manual) | ☐ | ☐ |
| 1.17 | CNTR-PC-000640 (Manual) | ☐ | ☐ |
| 1.18 | CNTR-PC-000750 (Manual) | ☐ | ☐ |
| 1.19 | CNTR-PC-000850 (Manual) | ☐ | ☐ |

| CIS Benchmark Recommendation | | Set Correctly | |
|---|---|---|---|
| | | Yes | No |
| 1.20 | CNTR-PC-000880 (Manual) | ☐ | ☐ |
| 1.21 | CNTR-PC-001030 (Manual) | ☐ | ☐ |
| 1.22 | CNTR-PC-001170 (Manual) | ☐ | ☐ |
| 1.23 | CNTR-PC-001220 (Manual) | ☐ | ☐ |
| 1.24 | CNTR-PC-001250 (Manual) | ☐ | ☐ |
| 1.25 | CNTR-PC-001350 (Manual) | ☐ | ☐ |
| 1.26 | CNTR-PC-001380 (Manual) | ☐ | ☐ |
| 1.27 | CNTR-PC-001390 (Manual) | ☐ | ☐ |
| 1.28 | CNTR-PC-001440 (Manual) | ☐ | ☐ |
| 1.29 | CNTR-PC-001470 (Manual) | ☐ | ☐ |
| 1.30 | CNTR-PC-001490 (Manual) | ☐ | ☐ |
| 1.31 | CNTR-PC-001770 (Manual) | ☐ | ☐ |

# Appendix: Change History

| Date | Version | Changes for this version |
| --- | --- | --- |
| Aug 22, 2025 | 1.0.0 | Initial CIS Release |