PALO ALTO NETWORKS (PAN)
PRISMA CLOUD COMPUTE
SECURITY TECHNICAL IMPLEMENTATION GUIDE
(STIG) OVERVIEW

Version 1, Release 2

02 September 2022

Developed by Palo Alto Networks and DISA for the DoD

Trademark Information

Names, products, and services referenced within this document may be the trade names, trademarks, or service marks of their respective owners. References to commercial vendors and their products or services are provided strictly as a convenience to our users, and do not constitute or imply endorsement by the Defense Information Systems Agency (DISA) of any nonfederal entity, event, product, service, or enterprise.

TABLE OF CONTENTS

Page

LIST OF TABLES

Page

LIST OF FIGURES

Page

1. INTRODUCTION

1.1 Executive Summary

The Prisma Cloud Compute Security Technical Implementation Guide (STIG) provides guidance for the configuration and use of Prisma Cloud Compute. This guidance incorporates technical recommendations for the deployment of the solution within a self-hosted environment.

Prisma Cloud Compute protects cloud native assets (e.g., running containers, serverless functions, noncontainer hosts, etc.) anywhere these assets operate, from the public cloud to isolated environments. It provides comprehensive visibility across all infrastructures, with continuous, automated monitoring that provides insights into new and existing assets, anomalous behaviors, and potential threats.

1.2 Authority

Department of Defense Instruction (DoDI) 8500.01 requires that “all IT [information technology] that receives, processes, stores, displays, or transmits DoD information will be […] configured […] consistent with applicable DoD cybersecurity policies, standards, and architectures.” The instruction tasks that DISA “develops and maintains control correlation identifiers (CCIs), security requirements guides (SRGs), security technical implementation guides (STIGs), and mobile code risk categories and usage guides that implement and are consistent with DoD cybersecurity policies, standards, architectures, security controls, and validation procedures, with the support of the NSA/CSS [National Security Agency/Central Security Service], using input from stakeholders, and using automation whenever possible.” This document is provided under the authority of DoDI 8500.01.

Although the use of the principles and guidelines in these SRGs/STIGs provides an environment that contributes to the security requirements of DoD systems, applicable NIST SP 800-53 cybersecurity controls must be applied to all systems and architectures based on the Committee on National Security Systems (CNSS) Instruction (CNSSI) 1253.

1.3 Vulnerability Severity Category Code Definitions

Severity Category Codes (referred to as CAT) are a measure of vulnerabilities used to assess a facility or system security posture. Each security policy specified in this document is assigned a Severity Category Code of CAT I, II, or III.

Table 1-1: Vulnerability Severity Category Code Definitions

Category	DISA Category Code Guidelines
CAT I	Any vulnerability, the exploitation of which will **directly and immediately** result in loss of Confidentiality, Availability, or Integrity.
CAT II	Any vulnerability, the exploitation of which **has a potential** to result in loss of Confidentiality, Availability, or Integrity.
CAT III	Any vulnerability, the existence of which **degrades measures** to protect against loss of Confidentiality, Availability, or Integrity.

1.4 STIG Distribution

Parties within the DoD and federal government's computing environments can obtain the applicable STIG from the DoD Cyber Exchange website at https://cyber.mil/. This site contains the latest copies of STIGs, SRGs, and other related security information. Those without a Common Access Card (CAC) that has DoD Certificates can obtain the STIG from https://public.cyber.mil/.

1.5 SRG Compliance Reporting

All technical NIST SP 800-53 requirements were considered while developing this STIG. Requirements that are applicable and configurable will be included in the final STIG. A report marked Controlled Unclassified Information (CUI) will be available for items that did not meet requirements. This report will be available to component authorizing official (AO) personnel for risk assessment purposes by request via email to: disa.stig_spt@mail.mil.

1.6 Document Revisions

Comments or proposed revisions to this document should be sent via email to the following address: disa.stig_spt@mail.mil. DISA will coordinate all change requests with the relevant DoD organizations before inclusion in this document. Approved changes will be made in accordance with the DISA maintenance release schedule.

1.7 Other Considerations

DISA accepts no liability for the consequences of applying specific configuration settings made on the basis of the SRGs/STIGs. It must be noted that the configuration settings specified should be evaluated in a local, representative test environment before implementation in a production environment, especially within large user populations. The extensive variety of environments makes it impossible to test these configuration settings for all potential software configurations.

For some production environments, failure to test before implementation may lead to a loss of required functionality. Evaluating the risks and benefits to a system's particular circumstances and requirements is the system owner's responsibility. The evaluated risks resulting from not applying specified configuration settings must be approved by the responsible AO. Furthermore, DISA implies no warranty that the application of all specified configurations will make a system 100 percent secure.

Security guidance is provided for the DoD. While other agencies and organizations are free to use it, care must be given to ensure that all applicable security guidance is applied at both the device hardening level and the architectural level due to the fact that some settings may not be configurable in environments outside the DoD architecture.

1.8 Product Approval Disclaimer

The existence of a STIG does not equate to DoD approval for the procurement or use of a product.

STIGs provide configurable operational security guidance for products being used by the DoD. STIGs, along with vendor confidential documentation, also provide a basis for assessing compliance with cybersecurity controls/control enhancements, which supports system assessment and authorization (A&A) under the DoD Risk Management Framework (RMF). Department of Defense AOs may request available vendor confidential documentation for a product that has a STIG for product evaluation and RMF purposes from disa.stig_spt@mail.mil. This documentation is not published for general access to protect the vendor's proprietary information.

AOs have the purview to determine product use/approval in accordance with DoD policy and through RMF risk acceptance. Inputs into acquisition or pre-acquisition product selection include such processes as:

- National Information Assurance Partnership (NIAP) evaluation for National Security Systems (NSS) (https://www.niap-ccevs.org/) IAW CNSSP #11
- National Institute of Standards and Technology (NIST) Cryptographic Module Validation Program (CMVP) (https://csrc.nist.gov/groups/STM/cmvp/) IAW Federal/DoD mandated standards
- DoD Unified Capabilities (UC) Approved Products List (APL) (https://www.disa.mil/network-services/ucco) IAW DoDI 8100.04

2. ASSESSMENT CONSIDERATIONS

2.1 Security Assessment Information

As technology has become a fundamental component of organizations, security concerns have been a driving force behind more standardized and structured IT practices. Best practices have emerged in response to a growing field of sophisticated threats. Protection that encompasses the entire lifecycle of an application, from the build phase through deployment and execution in production environments, is a non-negotiable requirement of any organization.

3. CONCEPTS AND TERMINOLOGY CONVENTIONS

3.1 Full Life Cycle Security Management

Prisma Cloud Compute meets the requirement for a full life cycle tool, covering both containerized environments and standard host-centric deployments where applications are directly managed at the bare metal host or virtual machine level.

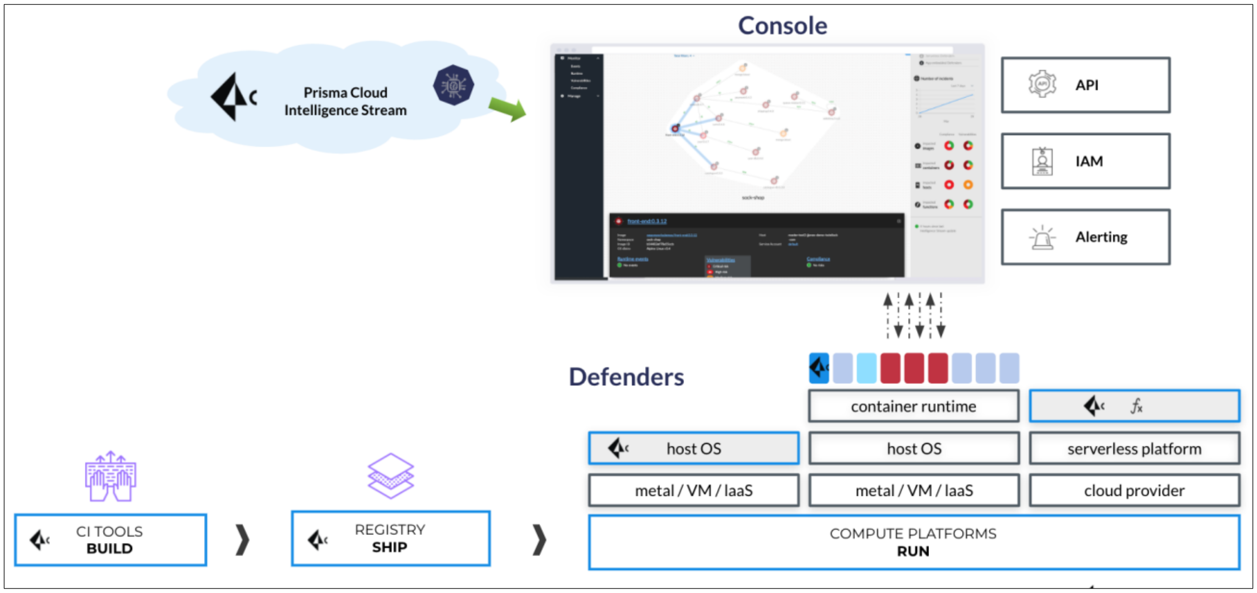
The security protections delivered by Prisma Cloud Compute include vulnerability detection, configurable checks for compliance adherence, runtime anomaly detection with a focus on contemporary attack types and techniques, and other tools and features.

3.2 Two Primary Components of Prisma Cloud Compute

Console: This management point for Prisma Cloud Compute is packaged as a Linux container that executes an application server and database. The Console is the central control for an instance of Prisma Cloud Compute.

Defenders: These protection agents run on all protected hosts. They are deployed as Linux containers or as Linux or Windows processes depending on the details of the target host. Defenders enforce the policies defined on the Console and send events back to the Console's manager process.

Figure 3-1: Prisma Cloud Compute Architecture



When deployed, Defenders connect to the Console via TCP to port 8084 on the Console using an x.500-based mutual TLS WebSocket session (WSS). This persistent WSS enables bidirectional communications. Upon initial connection, Defenders retrieve the full set of policies and configuration parameters from the Console and begin enforcement. Enforcement events are sent to the Console over the WSS connection for recording and alerting.

3.3 API

Prisma Cloud Compute's REST API allows for the programmatic automation of workflows and integration with external systems. This API is a function of the Console container. The HTML-based user interface and direct API interaction occurs over HTTPS on port 8083 of the Console container. TCP port 8083 is the default, configurable port, and third-party x.509 certificates/keys can be used to secure the TLS communications. The REST API's endpoints are documented in every release's distribution openapi.json file.

3.4 Intelligence Stream

Up-to-date vulnerability information is delivered via the Intelligence Stream, which comprises dozens of security feeds from open-source language projects, Linux distributions, other vendors such as Microsoft, etc. This feed is frequently updated and is available over the internet for regular, authenticated synchronization by deployed Consoles. Multiple methods are available for updating the Intelligence Stream in air-gapped environments, including downloading and uploading using a command line tool, a central Console that can serve Intelligence Stream updates, or an HTTP/HTTPS distribution point.

3.5 Authentication and Authorization

This STIG recommends implementation of the Security Assertion Markup Language (SAML) for authentication and authorization to the Console. Many organizations use SAML to authenticate users for web services. Prisma Cloud Compute supports the SAML 2.0 federation protocol to access the Prisma Cloud Console. When SAML authentication is enabled, users can log in to the Console with their federated credentials (e.g., DoD CAC).

All users should be managed by SAML, and only the "break glass" default administrator should be tied to a local "auth user" for emergency backup purposes. Credentials for this user must be protected.

This STIG was baselined using SAML as the third-party identity provider.

3.6 Trusted Images

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 environment. This STIG includes the configuration of the U.S. Air Force's Platform One Iron Bank) and Registry1 as the trusted images' registries. Organizations implementing this STIG can adjust the Trusted Images configuration according to their organization's defined trusted image sources.

3.7 Kubernetes/Docker

Prisma Cloud Compute’s Console and Defenders run as Linux containers within the organization’s containerization platform. Prisma Cloud Compute supports the Open Container Initiative (OCI) standard container formats and runtimes and supports the deployment via Kubernetes.

The Console is created using a Kubernetes deployment, ensuring a single copy of Console is always up and available. Defenders are deployed as a Kubernetes DaemonSet, guaranteeing an instance of Defender runs on each worker node in the cluster.

This STIG includes compliance checks that monitor both Kubernetes and Docker configurations, but Prisma Cloud Compute does not implement configuration changes to the environment. Therefore, the organization should implement the specific STIG or technology Security Requirements Guide (SRG) for its virtualization and orchestration technology.

4. GENERAL SECURITY REQUIREMENTS

4.1 Hosted Operating Systems

Prisma Cloud Compute relies on underlying OCI-compliant systems to provide a platform for operation. It is important that all pieces of the software stack be analyzed and security controls applied according to best practices and industry standards. Depending on the organization's selected OIC-compliant technology, the appropriate STIG or SRG must be applied to the underlying technology.

4.2 Logging

Prisma Cloud Compute Console and Defenders support the ability to send audit events to the virtualization node's syslog and/or standard out. This STIG instructs the organization to implement this capability. The organization is responsible for the collection and monitoring of the syslog audit data from the virtualization nodes within the environment. The Prisma Cloud Compute Alert feature can be configured to further define the notification method of selected events based on the appropriate stakeholder.

4.3 Identity Provider (IdP)

This STIG was baselined using SAML as the third-party identity provider. STIG and SRG user account controls are to be implemented by the SAML identity provider. Use the specific vendor STIG or technology SRG to secure the IdP.