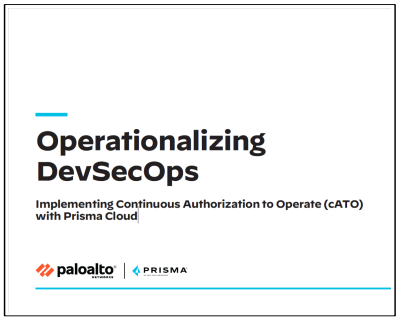


Operationalizing DevSecOps

Implementing Continuous Authorization to Operate (cATO) with Prisma Cloud

Thank you for downloading this Palo Alto Networks' e-book! Carahsoft is the master government aggregator and distributor for Palo Alto Networks' Cybersecurity solutions available via GSA, The Quilt, NASPO, and other contract vehicles.

To learn how to take the next step toward acquiring Palo Alto Networks' solutions, please check out the following resources and information:

For additional resources:
carah.io/PANWResources

For upcoming events:
carah.io/PANWEvents

For additional Palo Alto Networks solutions:
carah.io/PANWSolutions

For additional Cybersecurity solutions:
carah.io/CyberSecuritySolutions

To set up a meeting:
PaloAltoNetworks@carahsoft.com
(855)-6NEXTGN

To purchase, check out the contract vehicles available for procurement:
carah.io/PANWContracts

For more information, contact Carahsoft or our reseller partners:
PaloAltoNetworks@carahsoft.com | (855)-6NEXTGN

Operationalizing DevSecOps

Implementing Continuous Authorization to Operate (cATO) with Prisma Cloud

paloalto NETWORKS | PRISMA BY PALO ALTO NETWORKS

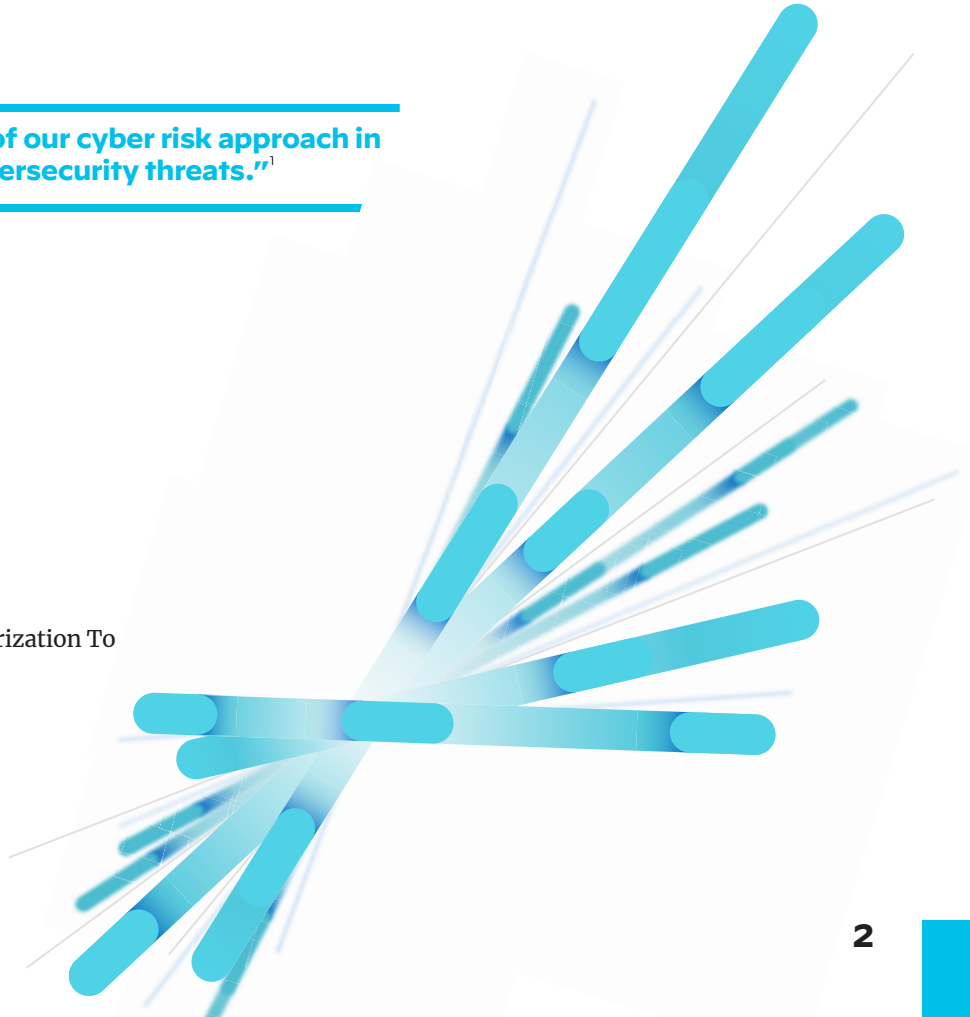
Continuous Authority to Operate (cATO)

"cATO represents a challenging but necessary enhancement of our cyber risk approach in order to accelerate innovation while outpacing expanding cybersecurity threats."[1]

In order to achieve cATO, the Authorizing Official (AO) must be able to demonstrate three main competencies:

1. On-going visibility of key cybersecurity activities inside of the system boundary with a robust continuous monitoring of RMF controls;
2. Ability to conduct active cyber defense in order to respond to cyber threats in real time; and
3. Adoption and use of an approved DevSecOps reference design.

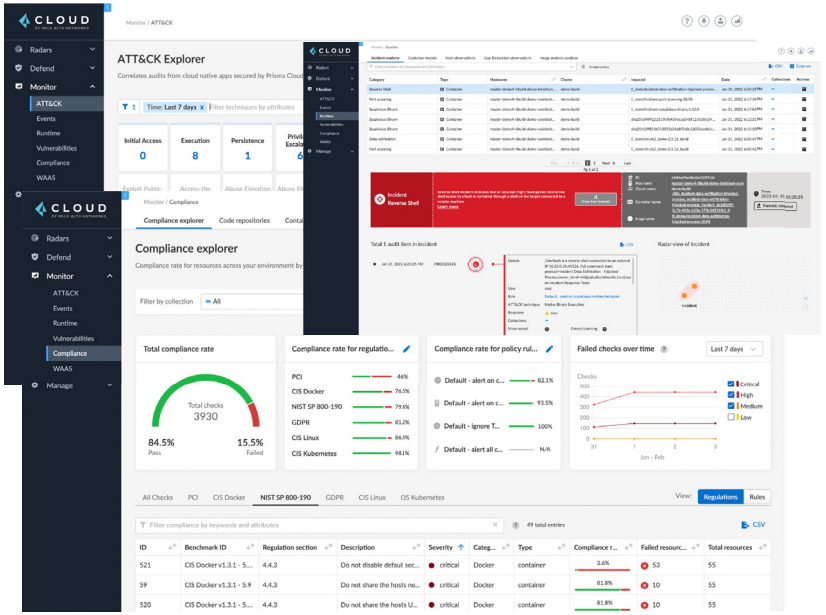
To learn more, please see Department of Defense Memo on Continuous Authorization To Operate (cATO) published February 3, 2022.



cATO Competencies – CONMON

"On-going visibility of key cybersecurity activities inside of the system boundary with a robust continuous monitoring of RMF controls"[1]

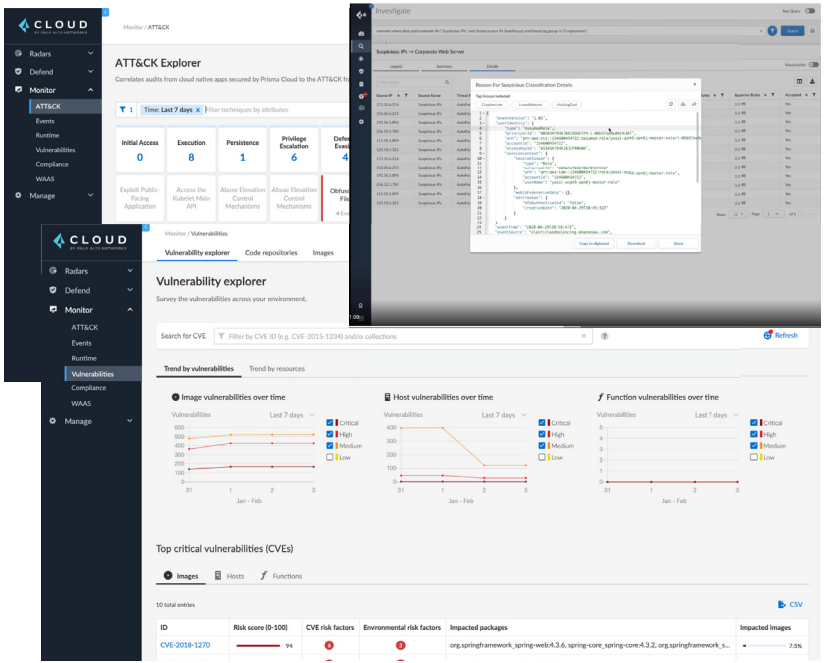
- **Continuous monitoring** for "drift" from the ATO identified controls, identifying non-compliance with controls as well as runtime anomalies.
- Events mapped to the ATT&CK framework within our **ATT&CK Explorer** for easier analysis by security engineers.
- Machine Learning and heuristics are used to analyze events, in order to detect incidents such as cryptomining, malware & kubernetes attacks.
- Incidents can be analyzed in the **Incident Explorer**
- *Live Forensic* information is provided to help troubleshoot and address the attack.



cATO Competencies – Active Cyber Defense

"Ability to conduct active cyber defense in order to respond to cyber threats in real time"[1]

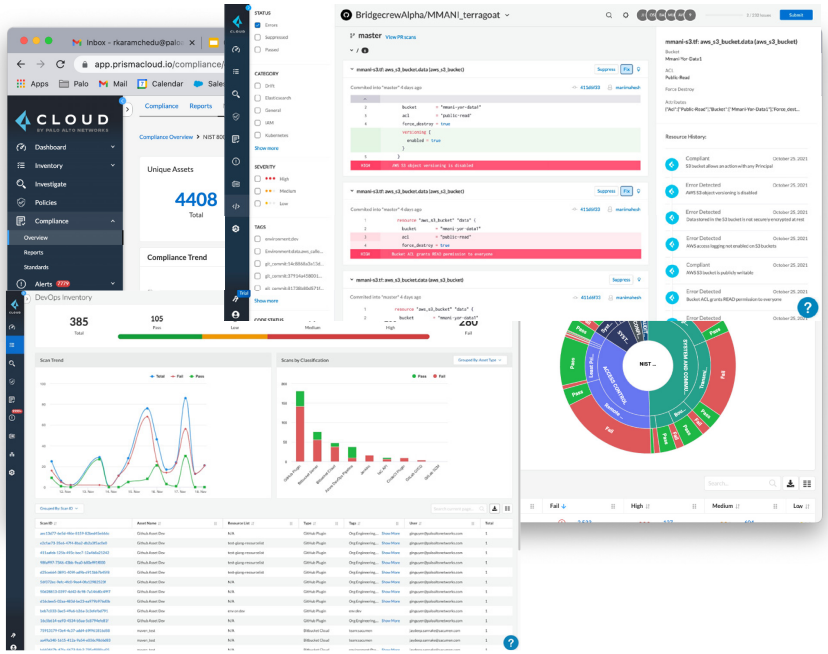
- The Prisma Cloud **Intelligence Stream (IS)** provides real-time feed of vulnerability data and threat intelligence (for both offline and online environments)
- Prisma Cloud **Advanced Threat Protection (ATP)** allows the runtime defense system to detect suspicious activities
- **App-specific network intelligence** detects runtime anomalies
- **ATT&CK Explorer** presents real-time view of TTPs employed by adversaries.
- **Vulnerability Explorer** provides context and prioritization of your biggest risks.
- **Machine Learning** and heuristics are used to analyze events and detect incidents such as cryptomining, malware & kubernetes attacks.
- **WAAS and Virtual Patching** allow for quicker reaction to new threats and enable protection.



cATO Competencies – Secure Software Supply Chain

"Adoption and use of an approved DevSecOps reference design"[1]

- **Prisma Cloud IaC Security** embeds security in popular integrated development environments (IDE), version control systems (VCS) and continuous integration/continuous delivery (CI/CD) tools.
- Prisma Cloud Compute provides **Container Vulnerability Assessment (CVA)** to protect against common container misconfigurations and insecure software packaging.
- **Image analysis sandbox** lets you dynamically analyze the runtime behaviour of images before running them in your development and production environments.
- Prisma Cloud Identity and Access Management (IAM) ensure secure identity and access management to your supply chain and source code.



[1] Department of Defense Memo on Continuous Authorization To Operate (cATO)