DEMISTO
A PALO ALTO NETWORKS® COMPANY

paloalto NETWORKS®

Automated Network Visibility and Incident Response

Benefits

- Automate data retrieval, enrichment, and enforcement actions from Panorama within Demisto through playbook-driven processes.
- Unify Panorama's network security management with other actions across your security product stack.
- Improve analyst efficiency by centralizing collaboration, investigation, and documentation.
- Shorten decision-making cycle by automating key tasks with analyst review.

Compatibility

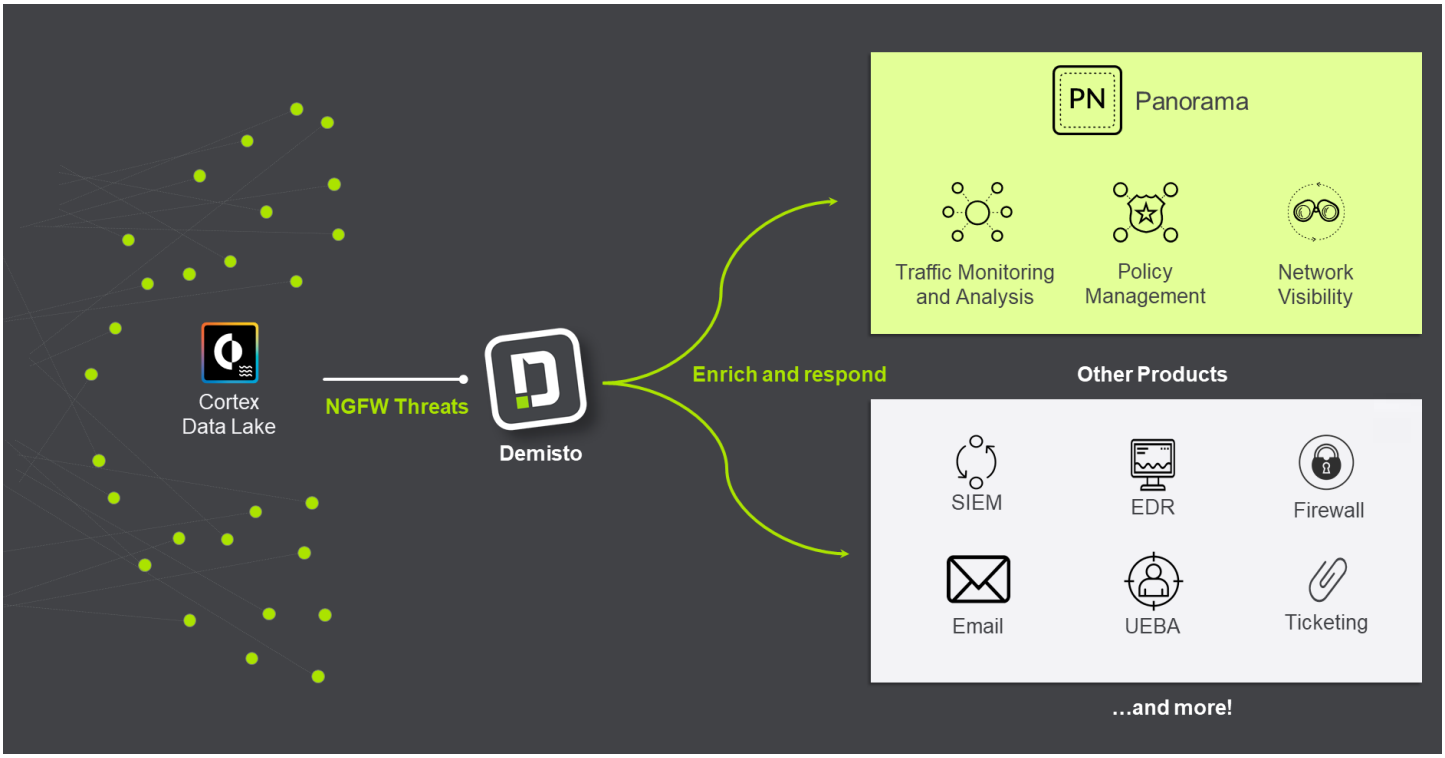
- Products: Demisto Enterprise, Palo Alto Networks® Panorama™

New and sophisticated cybersecurity threats are continually emerging to target enterprises, utilizing multiple attack vectors and evolving entry points. In this environment, displaying accuracy and agility during incident analysis and response become critical. Unfortunately, teams are overloaded with myriad security rules and mountains of data from multiple sources. Analysts need a tool stack that primes the organization for centralized visibility over network traffic and scalable, standardized response to threats that spans across security products.

Users can now leverage Demisto's security orchestration and automation with the network security management capabilities of Palo Alto Networks® Panorama™ for rich insight into network-wide traffic and automated threat response.

Integration Features

- Automate firewall rule creation, access, and deletion in Demisto playbooks using actions from Panorama.
- List rules, packet capture data, address groups, service groups, and more from Panorama within Demisto, either as automated playbook tasks or in real-time.
- Register IP addresses to tags and unregister IP addresses from tags within Demisto.
- Leverage hundreds of Demisto product integrations to further enrich WildFire data and coordinate response across security functions.
- Run 1000s of commands (including for Panorama) interactively via a ChatOps interface while collaborating with other analysts and Demisto's chatbot.

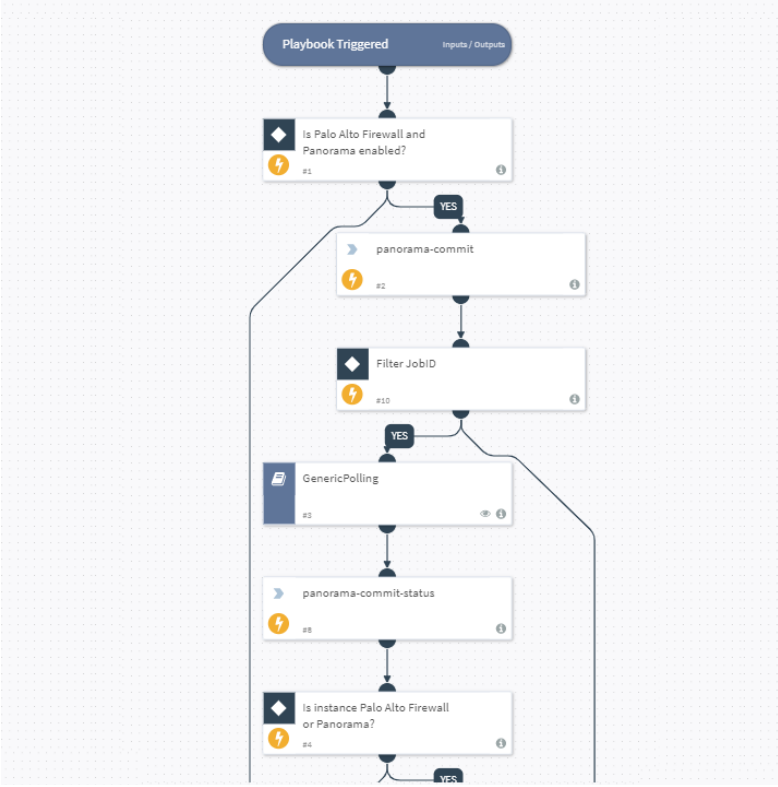


USE CASE #1 AUTOMATED THREAT PROTECTION AND RESPONSE

Challenge: When responding to alerts, time is of the essence. This time constraint is often at odds with the vast array of security products and data sources that analysts have to navigate, making context extraction and incident response a tall order. Many of these product-specific tasks, while essential to incident response, are repetitive and time-consuming, miring analysts in fatigue and preventing them from actual problem-solving.

Solution: SOCs can integrate the usage of Demisto Enterprise with Panorama for both alert ingestion and playbook-driven response. Demisto can ingest NGFW alerts through its integration with Cortex Data Lake. Once ingested, these alerts trigger playbooks that orchestrate and automate a variety of critical but repeatable actions during incident response. For instance, Demisto playbooks can retrieve details of dynamic lists and address groups, create and edit custom block policy rules, and get packet capture data from Panorama, among other things.

If any of these actions are missed by playbooks, they can also be run in real-time from an incident's War Room. This ensures that results are stored in a central location for further study and individual product consoles don't need to be accessed for every task.

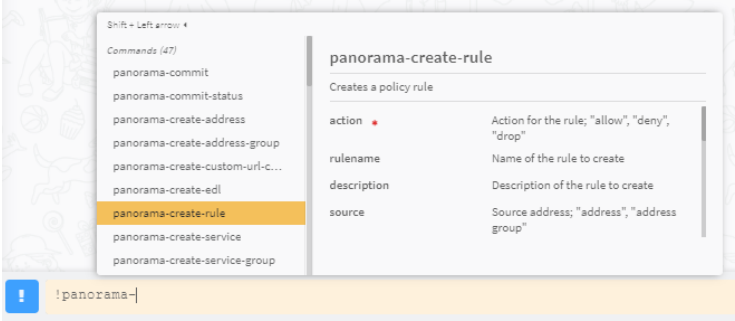


Benefit: Demisto acts as a bridge between Panorama and other security products that a SOC may use to both quicken incident resolution and orchestrate any allied tasks that fall outside the direct purview of incident response. This ensures standardized response and updates, reduced effort and time through automation, and archived documentation for future learning.

USE CASE #2 PROACTIVE AND SCHEDULED NETWORK SECURITY MANAGEMNT

Challenge: As organizations scale, coordinating day-to-day security operations in addition to incident response across heterogenous environments becomes tough. Managers face challenges in unifying security policy actions across disparate networks and tying in these actions with incident response and other security measures.

Solution: Demisto playbooks using Panorama can be scheduled as 'Jobs' to run at pre-determined intervals for network security management. For example, a playbook might run once every day, check malicious indicators against existing NGFW rules, and update rules as and when it spots a malicious indicator that slipped through the cracks. Conversely, the playbook can also remove safe indicators that were incorrectly placed in blacklists.



These playbooks can also be tied in or 'nested' within response playbooks, ensuring that both proactive and reactive grounds are covered with respect to cyberdefense.

Benefit: By partially/fully automating a vital part of security operations like network security management, security teams ensure that their environments are less vulnerable and more prepared as and when breaches occur. These scheduled 'Jobs' also free up analyst time for more strategic problem-solving, measurement, and execution of long-term security improvements.

About Palo Alto Networks® Panorama™

Security deployments can be complex, overloading IT teams with myriad security rules and mountains of data from multiple sources. Panorama™ network security management empowers you with easy-to-implement, consolidated policy creation, and centralized management features. You can provision firewalls centrally and use industry-leading functionality to create effective security rules as well as gain insight into network traffic and threats.

About Demisto

Demisto, a Palo Alto Networks company, is a comprehensive Security Orchestration, Automation, and Response (SOAR) platform that combines playbook orchestration, incident management, and interactive investigation to serve security teams across the incident lifecycle. With Demisto, security teams can standardize processes, automate repeatable tasks and manage incidents across their security product stack to improve response time and analyst productivity. For more information, visit www.demisto.com.