DEMISTO
A PALO ALTO NETWORKS® COMPANY

paloalto NETWORKS®

Palo Alto Networks and Demisto for Automated Data Visibility, Enrichment, and Response

Benefits

- Leverage Palo Alto Networks Cortex Data Lake for ingestion of rich network, cloud, and endpoint data.
- Ingest aggregated alerts from Cortex XDR for playbook-driven enrichment and response.
- Orchestrate network security, malware analysis, and threat intelligence actions through playbooks.
- Lessen dead time by using one platform for collaboration, investigation, and documentation.
- Shorten decision-making cycle by automating key tasks with analyst review.

Compatibility

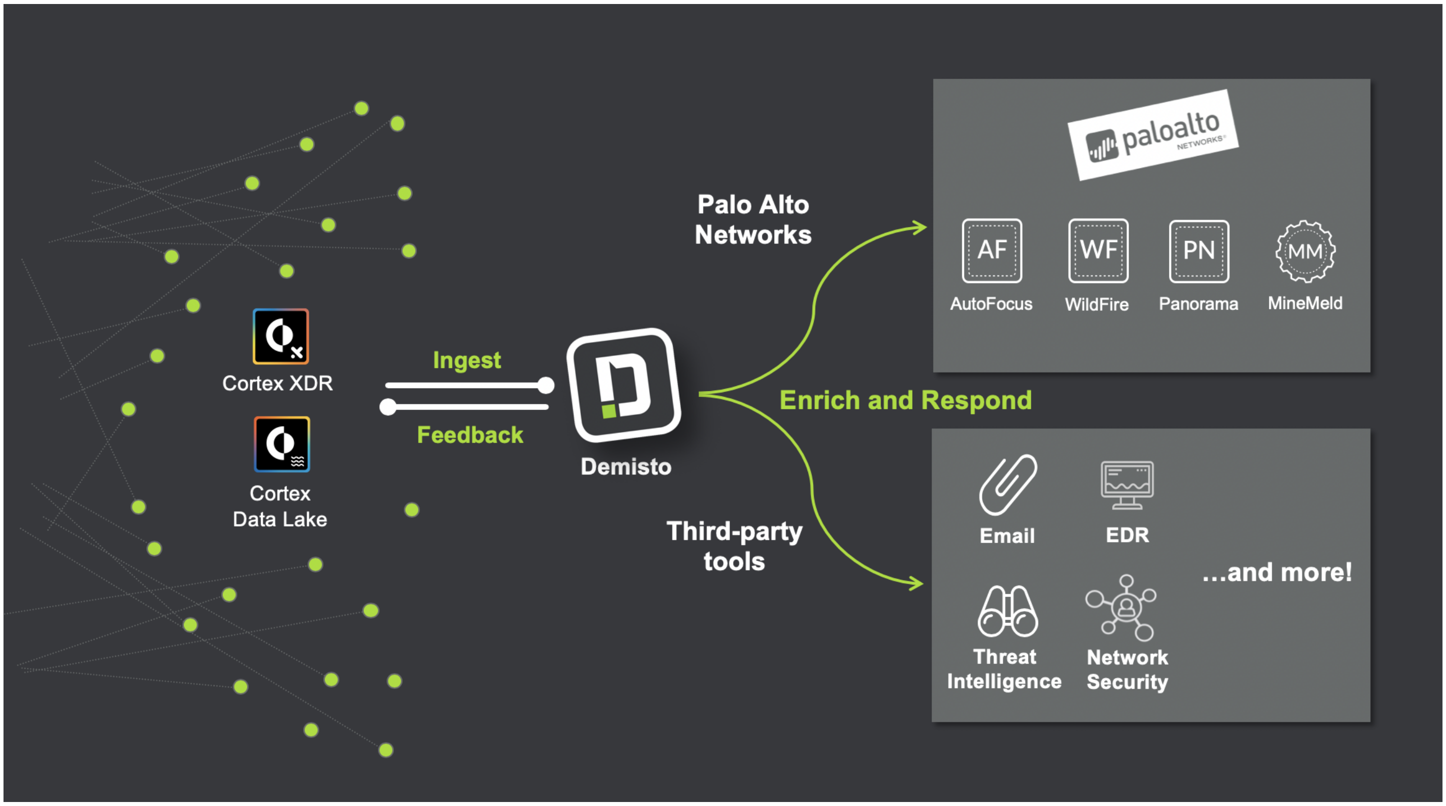
- Palo Alto Networks Cortex Data Lake, Cortex XDR, WildFire, Panorama, AutoFocus and MineMeld.
- Platform: Platform independent.

In this environment of sophisticated cybersecurity threats, understanding network and cloud traffic and being agile in analysis and response become vital. Analysts need a platform that enables complete visibility over both cloud and network data and primes the SOC for scalable, standardized enrichment and remediation actions.

Users can now leverage Demisto's security orchestration and automation capabilities with Palo Alto Networks products to rapidly act on rich, relevant security data and accelerate incident response.

Palo Alto Networks and Demisto integration features

- Create Demisto incidents and trigger playbooks in response to alerts from Cortex XDR for enrichment, triage, and resolution.
- Pull logs from Cortex Data Lake into Demisto via custom queries, enhancing incident context within Demisto.
- Automate malware sample analysis in Demisto playbooks using WildFire.
- Automate firewall policy modifications and actions in Demisto playbooks using Panorama.
- Automate threat intelligence actions in Demisto playbooks using AutoFocus.
- Automate and enrich incident indicators with MineMeld threat intelligence.
- Run 1000s of commands (including for Palo Alto Networks products) interactively via a ChatOps interface while collaborating with other analysts and Demisto's chatbot.



USE CASE #1 AUTOMATED INCIDENT INGESTION, ENRICHMENT, AND RESPONSE

Challenge: Organizations today deal with an expanded threat surface. Security attacks can leave footprints across network, endpoint, or cloud environments, but teams struggle to continuously monitor these environments, correlate data across sources to get the bigger picture, and then drive that data to response in a scalable manner.

Solution: Cortex collects rich, detailed data across network, endpoint, and cloud environments before applying behavioral analytics and AI to stitch the data together and display alerts in a sequenced manner. Demisto can ingest alerts from Cortex XDR as incidents and trigger playbooks that coordinate across users' security product stack for further enrichment and response. These playbooks can be automated, manual, or a mixture of both, depending on user requirements.

Benefit: Leveraging threat detection capabilities along with Demisto's security orchestration and automation helps teams unify response processes across their product stack. Demisto playbooks triggered off Cortex XDR data help minimize screen switching, manual reconciliation of data, and repetitive work for security teams.

USE CASE #2 REAL-TIME INVESTIGATION FOR COMPLEX THREATS

Challenge: Standardized processes are not enough for responding to every security alert. Apart from running automated actions, attack investigations usually require additional real-time tasks such as pivoting from one suspicious indicator to another to gather critical evidence, drawing relations between incidents, and finalizing resolution. Running these commands traps teams in a screen-switching cycle during investigation and a documentation-chasing cycle after investigations end.

Solution: SOCs can integrate usage of Demisto Enterprise with a host of Palo Alto Networks products – AutoFocus, Minemeld, Panorama, and WildFire – to orchestrate and automate a variety of actions during incident response. For instance, Demisto playbooks can automate file detonation using WildFire, perform indicator reputation lookup using AutoFocus, enrich with Minemeld indicator data and create firewall blocklists using Panorama.

These actions can also be run in real-time from an incident's War Room, ensuring that results are stored in a central location for further study and individual product consoles don't need to be accessed for every repeatable task.

Benefit: Demisto acts as a bridge between Palo Alto Networks products 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.

About Demisto

Demisto, a Palo Alto Networks company, is the only Security Orchestration, Automation, and Response (SOAR) platform that combines security 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.

About Palo Alto Networks

Palo Alto Networks is a global cybersecurity leader, known for always challenging the security status quo. Our mission is to protect our way of life in the digital age by preventing successful cyberattacks. This has given us the privilege of safely enabling tens of thousands of organizations and their customers. Our pioneering Security Operating Platform emboldens their digital transformation with continuous innovation that seizes the latest breakthroughs in security, automation, and analytics. By delivering a true platform and empowering a growing ecosystem of change-makers like us, we provide highly effective and innovative cybersecurity across clouds, networks, and mobile devices. Find out more at www.paloaltonetworks.com.