PALO ALTO NETWORKS AND DEMISTO FOR AUTOMATED INCIDENT RESPONSE

Benefits

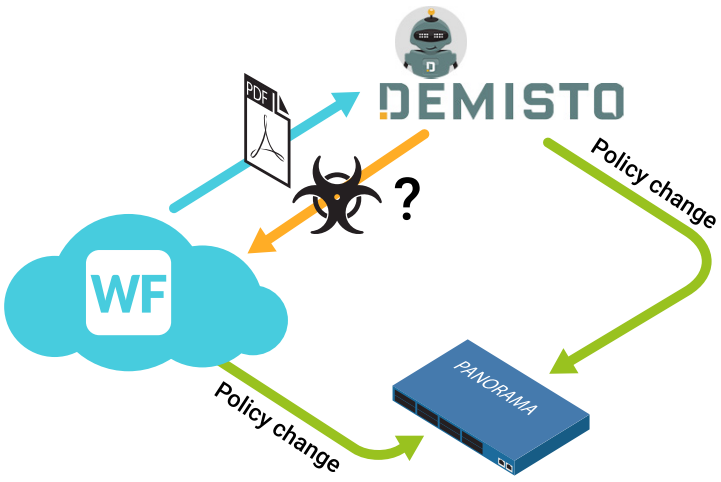
- Demisto and Palo Alto Networks for Automated Incident Response.
- Automated incident response and playbook-driven triage of security alerts.
- Enrichment of investigation data and malware analysis in complex investigations.
- ChatOps-based automation and collaboration to foster learning, sharing and faster incident resolution.

New forms of sophisticated cybersecurity threats continually emerge to target enterprises in new ways, utilizing multiple attack vectors. When investigating a security event or breach, Demisto customers can now enrich their investigation data with Palo Alto Networks® WildFireTM threat intelligence and malware analysis results.

Demisto customers can also optimize and automate their response procedures by configuring new security rules in Palo Alto Networks Next-Generation Security Platform.

Palo Alto Networks and Demisto integration provides:

- Automatic data enrichment and analysis with Demisto's playbooks and Palo Alto Networks WildFire.
- Remediation via Demisto's playbooks and automation scripts adjusting Palo Alto Networks PanoramaTM policy.
- On-demand malware analysis during incident investigation provided by DBot, first security chatbot, using Palo Alto Networks WildFire.
- Collaborative interface to investigate with rich data provided by WildFire .
- IOCs discovered during investigations in Demisto update WildFire.



USE CASE #1

Automated and instant response to an ongoing attack

Challenge:

When an organization is under attack, time is of the essence. Every minute that passes until response is made may mean greater damage. In most organizations this is a manual process in which an analyst may ask the IT helpdesk to disconnect a network segment, an endpoint, etc. The process may take unnecessary time and is error prone.

Solution:

When an attack is investigated in Demisto, a security analyst can trigger immediate, predefined response procedures. Also an auto- mated playbook can trigger response via the Palo Alto Networks Panorama API, allowing the Demisto analyst to run a script that, for example, isolates a network segment or disconnects a host from the network.

Additional Benefit:

All actions are recorded in the virtual war room so that the response and remediation procedures can be reported on, and revisited after the investigation is closed

USE CASE #2

Automated enrichment of investigation data

Challenge:

During investigations analysts need to check artifacts and find out whether or not they are malicious. Faced with many artifacts, this can be a tedious process that is both time-consuming and repetitive

Solution:

Demisto offloads the tedious work by integrating with Palo Alto Networks WildFire, allowing analysts to not only perform malware analysis by issuing commands to DBot but also to perform many of the checks automatically – setting the war room up to check submit files, emails, and other artifacts that pop up during an investigation for analysis in WildFire.

Additional Benefit:

Once identified as malware, WildFire automatically generates protections and delivers them back to the security products, thereby closing the loop of finding malware, analyzing it, and protecting the network.

About Demisto

Demisto helps Security Operations Centers scale their human resources, improve incident response times, and capture evidence while working to solve problems collaboratively. Demisto Enterprise is the first comprehensive, Bot-powered Security ChatOps Platform to combine intelligent automation with collaboration. Demisto's intelligent automation is powered by DBot which works with teams to automate playbooks, correlate artifacts, enable information sharing and auto document the entire incident lifecycle. Demisto is backed by Accel and has offices in Silicon Valley and Tel Aviv. For more information visit www.demisto.com or email info@demisto.com.

About Palo Alto

Palo Alto Networks is the next-generation security company, leading a new era in cybersecurity by safely enabling applica- tions and preventing cyber breaches for tens of thousands of organizations worldwide. Built with an innovative approach and highly differentiated cyberthreat prevention capabilities, our game-changing security platform delivers security far superior to

legacy or point products, safely enables daily business operations, and protects an organization's most valuable assets. Find out more at www.paloaltonetworks.com.

DEMISTO

10056 Orange Avenue
Cupertino, CA 95014, USA

54 Achad Ha'am St.
Tel Aviv, Israel

Website: www.demisto.com
Email: info@demisto.com
Twitter: @demistoinc