DEMISTO
A PALO ALTO NETWORKS® COMPANY

paloalto NETWORKS®

Automated Malware Analysis and Response

Benefits

- Execute WildFire's cutting-edge, cloud-delivered malware analysis within Demisto in real-time.
- Orchestrate WildFire malware analysis with other security processes through task-based playbooks.
- Reduce time to resolution by using one platform to collaborate, investigate, and document.
- Shorten decision-making cycle by automating key tasks with analyst review.

Compatibility

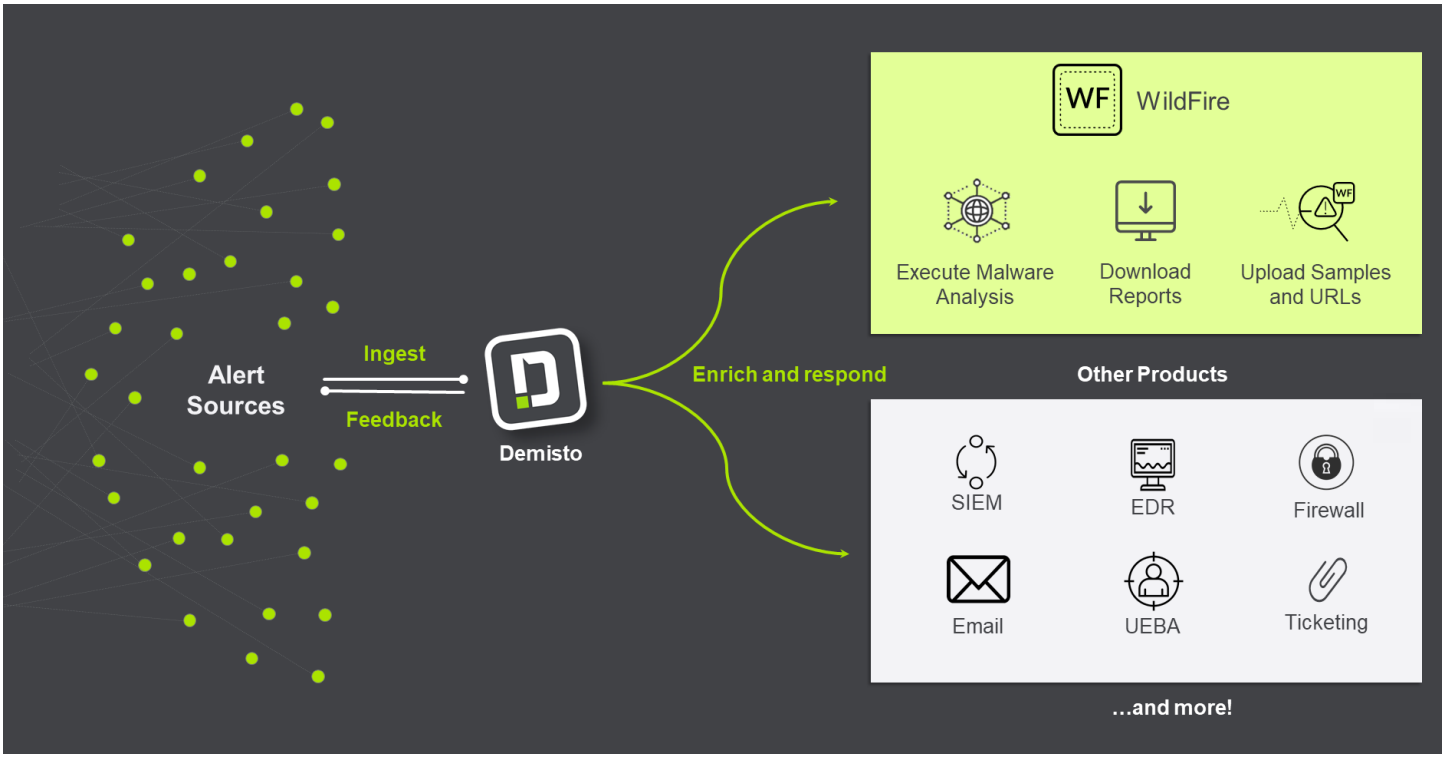
- Products: Demisto Enterprise, Palo Alto Networks® WildFire™
- Platform: Platform independent

In today's security landscape, threat actors use multiple entry vectors and attack techniques to target organizations. With so many moving parts, security teams struggle to reconcile data between isolated malware analysis tools and other security products. They lose valuable time shuttling between screens and executing repeatable tasks while the attack continues to manifest. Analysts need a platform that unifies data from malware analysis products and other sources on one console, resulting in rich incident context and accelerated response without tab-switching and manual rework.

Joint users can combine WildFire's cloud-delivered malware analysis capabilities with Demisto's security orchestration and automation features to standardize their response processes, increase analyst productivity, and reduce remediation times.

Integration Features

- Retrieve samples, results for file hashes, and verdicts from WildFire within Demisto through automated playbook-driven tasks.
- Submit samples to WildFire for analysis and download reports from within Demisto.
- Upload URLs of remote files or webpages to WildFire for analysis from within Demisto.
- Leverage hundreds of Demisto product integrations to further enrich WildFire data and coordinate response across security functions.
- Run thousands of commands (including for WildFire) interactively via a ChatOps interface while collaborating with other analysts and Demisto's chatbot.

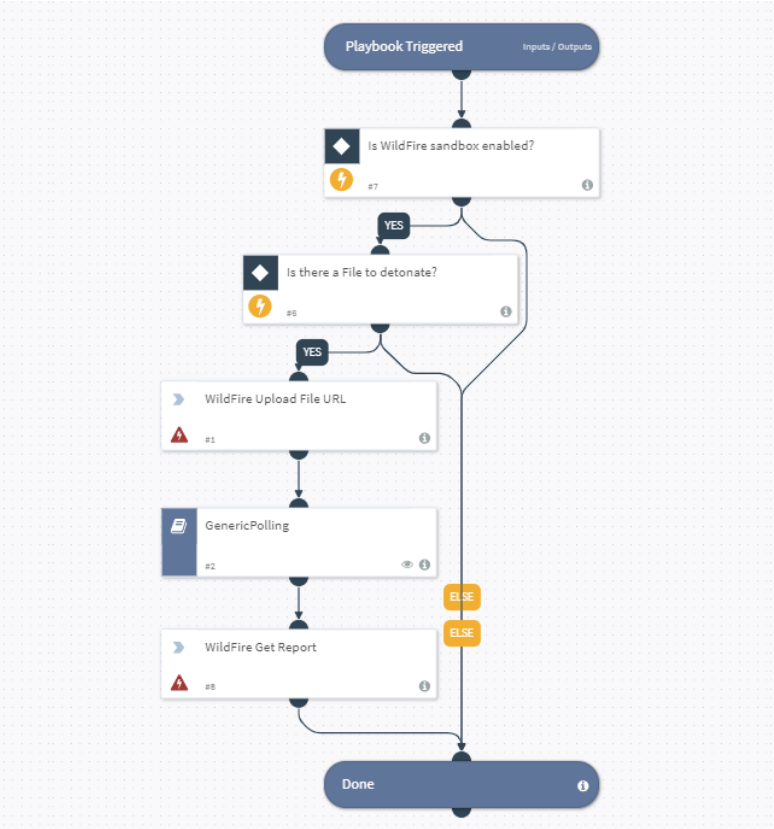


USE CASE #1 AUTOMATED MALWARE ANALYSIS AND RESPONSE

Challenge: As alert numbers grow, analysts find it tough to keep up with the repetitive, high-quantity tasks that encompass malware triage and analysis for further study. This can eventually lead to increased error rate, incomplete investigations, and alerts slipping through the cracks.

Solution: SOCs can have standardized playbooks that run automatically and query WildFire for malware analysis. These playbooks can perform checks to initiate triage, run detonation actions, and return the reports to the analysts for subsequent investigation. By aligning malware analysis with other concurrent security functions, these playbooks ensure that security teams have central visibility over incident response processes.

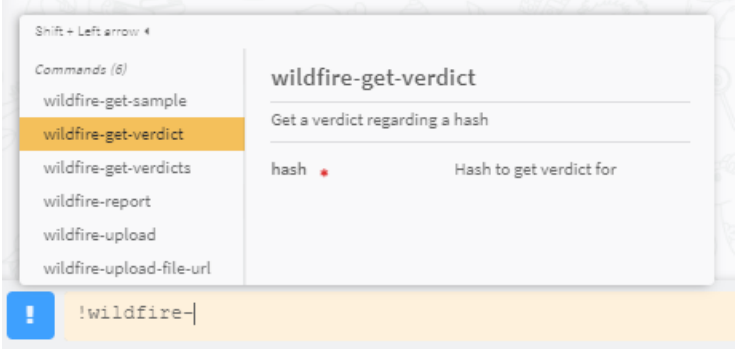
Benefit: Analysts will save time and eliminiate redundant effort by automating triage and detonation tasks, saving their energies for more nuanced and sophisticated investigation actions. This will also ensure standardized response, reduced error rate, and no alerts slipping through the cracks.



USE CASE #2 INTERACTIVE INVESTIGATIONS FOR DEEPER MALWARE STUDY

Challenge: The attacks of today are different from the attacks of yesterday, so just playbook orchestration may not be enough for response. 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 analysts in a screen-switching cycle during investigation and a documentation-chasing cycle after investigations end.

Solution: After playbook execution, analysts can conduct joint investigations in the Demisto War Room and run WildFire-specific commands in real-time. For example, if the playbook for a particular incident extracted a hash, analysts can run the **wildfire-get-verdict** command to get the WildFire verdict for that hash.



Security teams can also run commands from hundreds of other products in the War Room, ensuring a unified platform for collaboration, investigation, and documentation of actions.

Benefit: All participating analysts will have full task-level visibility of the process followed and be able to run and document commands from the same window, thus preventing the need for collating information from multiple sources for documentation.

About Palo Alto Networks® WildFire™

Palo Alto Networks WildFire® malware prevention service is the industry's most advanced analysis and prevention engine for highly evasive zero-day exploits and malware. The service employs a unique multi-technique approach, combining dynamic and static analysis, innovative machine learning techniques, and a groundbreaking bare metal analysis environment to detect and prevent even the most evasive 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.