Cisco AMP Threat Grid | DEMISTO

CISCO THREAT GRID AND DEMISTO FOR AUTOMATED MALWARE PROTECTION

Benefits

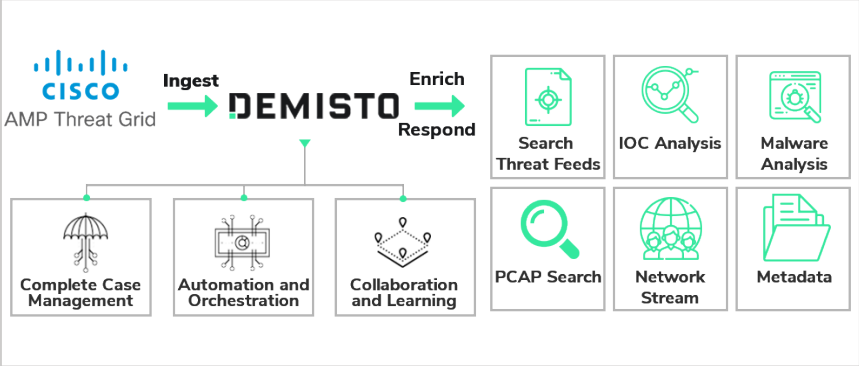
- Ingest threat feed data, orchestrate enrichment across other security products, and accelerate incident response.
- Orchestrate malware protection and threat intelligence actions through automated playbooks.
- Reduce time to resolution by using one platform to collaborate, investigate, and document.
- Shorten decision-making cycle by automating key tasks with analyst review.

Compatibility

- Products: Demisto Enterprise, Cisco Threat Grid
- 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 from isolated malware analysis and threat intelligence tools, among others. 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 IOC threat intelligence, malware analysis, and other sources on one console, resulting in rich incident context and accelerated response without tab-switching and manual rework.

Users can combine Cisco Threat Grid's malware analysis and threat intelligence capabilities with Demisto's security orchestration and automation features to standardize their response processes, increase analyst productivity, and reduce time to detection and remediation.



Integration Features

- Ingest threat feed data from Threat Grid into Demisto and run tailored automated playbooks to add context to alerts as well as respond to alerts.
- Orchestrate Threat Grid sandboxing actions along with other security products in one window through Demisto playbooks.
- Leverage hundreds of Demisto product integrations to further enrich Threat Grid alerts and coordinate response across security functions.
- Run thousands of commands (including for Threat Grid) interactively via a ChatOps interface while collaborating with other analysts and Demisto's chatbot.

USE CASE #1

STREAMLINED THREAT INTELLIGENCE INGESTION ACROSS CONSOLES

Challenge: If a security analyst uses different platforms for threat intelligence and security orchestration and automation respectively, it can be tough to track the lifecycle of an alert due to flitting between screens, fragmented information, and lack of single-window documentation.

Solution: If SOCs use Cisco Threat Grid for threat intelligence and Demisto Enterprise for security orchestration and automation respectively, they can trigger actions for specific alert types in Threat Grid to create an incident in Demisto.

Benefit: Demisto playbooks and investigation toolkits can gather additional information needed for triage and resolution of Threat Grid alerts. Analysts get a comprehensive view of the incident's lifecycle, can access documentation from a single source, and forego the need to switch between screens.

USE CASE #2

AUTOMATE SANDBOX DETONATION AND MALWARE TRIAGE

Challenge: As alert numbers grow, analysts find it tough to keep up with the repetitive, high-quantity tasks that encompass malware triage and sandbox detonation 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 when certain alerts are ingested from Threat Grid. These playbooks can perform checks to initiate triage, run detonation actions, and return the reports to the analysts for subsequent investigation.

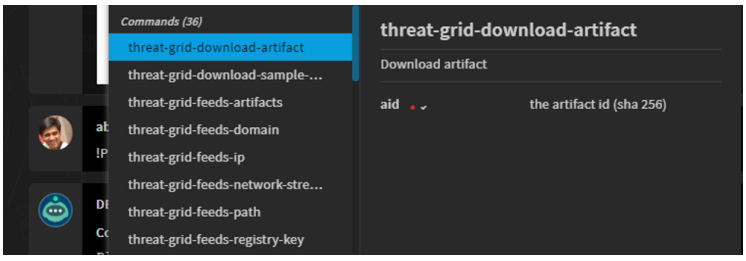
Benefit: Analysts will save lots of time and redundant effort by automating triage and detonation tasks, saving their energies for more cerebral and sophisticated investigation tasks. This will also ensure standardized response, reduced error rate, and no alerts slipping through the cracks.

USE CASE #3

INTERACTIVE INVESTIGATIONS FOR DEEPER MALWARE STUDY

Challenge: While conducting joint investigations, analysts struggle with attaching task-level accountability, documenting actions in one source, and learning from each other's actions to reduce marginal time to incident resolution.

Solution: After the playbooks have run, analysts can conduct joint investigations in the Demisto War Room and run 35+ Threat Grid specific commands – apart from hundreds of others – to carry out an interactive investigation for more sophisticated alerts. For example, analysts can run commands to get network stream data, PCAP data, and reports specific to an alert ID.



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

About Demisto

Demisto is the only Security Orchestration, Automation and Response (SOAR) Platform that combines orchestration, incident management and interactive investigation into a seamless experience. Demisto's orchestration engine automates security product tasks and weaves in human analyst tasks and workflows. Demisto Enterprise, powered by its machine learning technology, acquires knowledge from the real-life analyst interactions and past investigations to help SOC teams with analyst assignment suggestions, playbook enhancements, and best next steps for investigations. For more information, visit www.demisto.com oremail info@demisto.com.

About Cisco Threat Grid

Cisco® Threat Grid combines two of the leading malware protection solutions: unified malware analysis and context-rich intelligence. It empowers security professionals to proactively defend against and quickly recover from cyber attacks.