McAfee | DEMISTO

McAfee and Demisto

Automated Security Operations and Security Policy Management

Benefits

- Automate incident response and security policy actions through playbooks
- Tighten oversight over SLAs, metrics, KPIs, and incident evidence
- Shorten decision-making cycle by automating key tasks with analyst review

Compatibility

- **Products:** McAfee Enterprise Security Manager, McAfee ePolicy Orchestrator 5.1 & above, McAfee Advanced Threat Defense, McAfee Threat Intelligence Exchange, McAfee Active Response, McAfee DXL

SOC teams today are lost in a sea of alerts, logs, and data while trying to manage incident response lifecycles. In the complex corporate security environment, automation is increasingly the “go-to” answer for organizations. According to Gartner, the number of midsize and large enterprises that automate their security operations and make them intelligence-driven will increase from 5% to 30% by 2019.

In this world primed for automation, analysts can now combine the incident management, threat intelligence, threat defense, and security policy management capabilities of McAfee’s products with the automation and orchestration features of Demisto Enterprise into one comprehensive solution.

By automating both incident response to ESM-generated alerts and security policy actions for those alerts, as well as orchestrating threat intelligence and response actions in one window, analysts can avoid mundane, repeatable tasks and focus on more strategic, productive work.

McAfee and Demisto integration features:

- Ingest and triage alert data from McAfee ESM into Demisto Enterprise
- Trigger specific playbooks in Demisto to gather more information about ESM alerts and to respond to these alerts
- Trigger Demisto playbooks to run and check security policy actions from McAfee ePO
- Triage and map alerts as incidents from McAfee Enterprise Security Manager
- Enrich incident data like IP, hashes, filenames, and URLs using McAfee Threat Intelligence Defense
- Detonate unknown samples using McAfee Advanced Threat Exchange
- Respond by orchestrating changed security policies using McAfee ePolicy Orchestrator and McAfee Active Response

USE CASE #1 AUTOMATED INCIDENT INGESTION AND RESPONSE

Challenge: If a security analyst uses different solutions for incident logging and specific investigation actions, it's tough to track the lifecycle of an incident due to toggling between screens, fragmented information, and lack of single-window documentation.

Solution: If SOCs use McAfee ESM for incident management and Demisto Enterprise for security orchestration and automation, they can trigger actions for specific alert types in ESM to create an incident and trigger a playbook in Demisto. The playbook will orchestrate investigation actions across the suite of products that a SOC uses – including threat feeds, endpoint solutions, ticket management, and malware analysis – in a single screen and seamless workflow.

Benefit: Demisto playbooks and investigation toolkits gather additional information needed for triage and resolution of ESM 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 while performing investigation actions.

USE CASE #2 ORCHESTRATING SECURITY POLICY ACTIONS

Challenge: As organizations scale, coordinating security policy and software management across heterogenous systems and 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: SOCs can integrate usage of McAfee ESM, McAfee ePO, and Demisto for seamless incident response and policy management.For instance, an ESM alert can trigger a playbook in Demisto that, among other things, also checks the ePO system tree for additional system details. If the incident resolution involves an update to security policy actions, this playbook can also orchestrate those tasks instead of leaving them to security policy managers.

Benefit: Demisto acts as a bridge between ESM, ePO, 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, andarchived documentation for future learning.

ABOUT MCAFEE EPOLICY ORCHESTRATOR SOFTWARE

McAfee ePO software is the industry-leading security and compliance management platform. With its single-agent and single-console architecture, McAfee ePO software provides intelligent protection that is automated and actionable, enabling organizations to reduce costs and improve threat protection and compliance.

ABOUT MCAFEE ENTERPRISE SECURITY MANAGER

McAfee Enterprise Security Manager—the foundation of the security information and event management (SIEM) solution family from McAfee—delivers the performance, actionable intelligence, and real-time situational awareness at the speed and scale required for security organizations to identify, understand, and respond to stealthy threats, while the embedded compliance framework simplifies compliance.

ABOUT DEMISTO

Demisto Enterprise is the first and only comprehensive Security Operations Platform to combine security orchestration, incident management, machine learning from analyst activities, and interactive investigation. Demisto's orchestration engine automates security product tasks and weaves in the human analyst tasks and workflows. Demisto enables security teams to reduce mean time to resolution (MTTR), create consistent incident management process, and increase analyst productivity. Demisto is backed by Accel and other prominent investors and has offices in Silicon Valley and Tel Aviv. For more information, visit www.demisto.com or email info@demisto.com.