SOLUTION BRIEF

Automate Full Security Operation Management Lifecycle

Automate incident management, investigation, and response

Demisto and McAfee have teamed up to provide a complete incident management, investigation, and response offering for security operations managers and responders by integrating Demisto Enterprise Platform with McAfee® Enterprise Security Manager and McAfee® ePolicy Orchestrator® (McAfee ePO™) software. Together, these industry-leading platforms form an enterprise-grade solution to manage and automate incident investigation tasks. Playbooks can be executed in response to alerts generated by McAfee Enterprise Security Manager, and security policies can be modified for the incident via McAfee ePO software. The result is a reliable, fast, and automated investigation response process against cybersecurity threats. This effectively eases the burden of mundane tasks for incident responders and frees up their time for deeper investigations.

McAfee Compatible Solution

- Demisto Enterprise v1.6
- McAfee Enterprise Security Manager 9.6 and above
- McAfee ePolicy Orchestrator 5.1 and above

When it comes to the incident management cycle, security operations (SOC) teams today are lost in a sea of alerts, logs, and data. In complex corporate security environments, automation is increasingly the "go-to" answer. For many, homegrown middleware is the only way to address their most critical processes.

According to Gartner, by 2019, 30% of medium-size and large enterprises will leverage SOC automation technologies to automate their security operations and make them intelligence-driven, up from 5% in 2015.

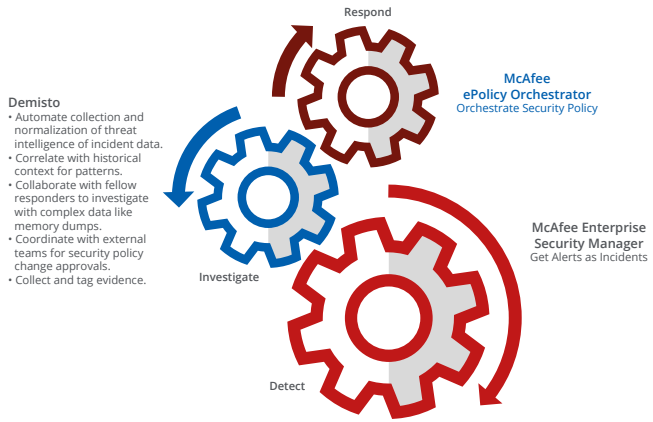

Figure 1. McAfee integration with Demisto detects, investigates, and responds to threats.

McAfee and Demisto Provide an Integrated Incident Response Platform

Demisto Enterprise Platform is a single place to implement and automate your entire incident response plan. The platform offers the right mix of automation and manual run capability so that mundane tasks can be automated and critical steps can be approved after human intervention.

SOC management teams use Demisto platform to streamline the incident management lifecycle:

- Triage alerts from McAfee Enterprise Security Manager
- Assign incidents to appropriate teams based on Incident type and severity
- Track service-level agreements (SLAs)
- Review evidence post-incident closure to ensure that prescribed incident response procedure is being followed
- Measure and improve key performance indicators (KPIs) for SOC efficiency

Incidence responders use Demisto platform's automated playbooks to guide them through the incident investigation process. A typical playbook is a mix of automated and manual tasks such as:

- Mapping alerts as incidents from McAfee Enterprise Security Manager
- Enriching incident data like IP, hashes, filenames, and URLs using threat feeds
- Communicating with impacted users
- Doing deep manual investigations in war rooms with existing incident data or collected evidence, such as memory dumps and more
- Collaborating with internal and external team members
- Orchestrating response by changing security policy using McAfee ePO software

About Demisto

Demisto Enterprise is the industry's first bot-powered security "conversations, put to work" (ChatOps) platform to automate and streamline security operations and incident management processes. With Demisto, security analysts can maximize their time and reduce their effort during incident investigations while sharing knowledge and working collaboratively for faster resolution.

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 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 delivers actionable intelligence, and situational awareness in near real time, allowing security organizations to identify and respond to stealthy threats and maintain compliance.

McAfee™
Together is power.

2821 Mission College Boulevard
Santa Clara, CA 95054
888 847 8766
www.mcafee.com