Siemplify & McAfee

JOINT SOLUTION **BRIEF**

SOAR + MVISION

Integrate McAfee MVISION ePO and EDR into the Siemplify Cloud SOAR platform to slash response times

Challenge

Security operations teams need to be better empowered to simplify the orchestration of disparate tools for automated alert triage, investigation and remediation. There is an enormous amount of pressure applied to security analysts to investigate and respond to an unprecedented volume of alerts from disparate tools in the hope of detecting and containing the next cyberattack. In many cases, incident response processes are largely manual, leaving these teams more resource-constrained than ever.

Solution Overview

McAfee® MVISION ePolicy Orchestrator® (McAfee MVISION ePO™) is used as an effective tool for automating workflows that identify, manage and respond to endpoint vulnerabilities identified by MVISION EDR. Siemplify's cloud-native Security Operations Platform integrates with MVISION ePO and MVISION EDR to extend McAfee policy enforcement into workflows that integrate with your entire security stack.

The technical integration between Siemplify and McAfee allows our joint users to group McAfee alerts with alerts from other tools to create threat-centric cases that analysts can investigate. Siemplify enables playbook-driven responses that reduce analyst time and effort spent on responding to individual alerts and reduces manual activities for faster and more effective investigation and response.

Product Integrations

Siemplify is listed as a featured partner within the **MVISION Marketplace**. The Siemplify Security Operations Platform integrates with the following McAfee MVISION platform capabilities.

MVISION INTEGRATIONS

- McAfee MVISION ePO™
- McAfee MVISION EDR

more use case details on page 2

Joint Solution Benefits

Slash Investigation Time and Effort

Run playbooks that automate data collection using MVISION ePO and MVISION EDR inputs to limit the amount of time spent manually cross-referencing information before making decisions.

Automate Response and Enable Threat Hunting

Integrate MVISION data with your other tools for remediation actions such as resetting accounts, isolating hosts or killing processes, without having to pivot between systems.

Unify Case Management

Ingest MVISION data directly or via SIEM into the Siemplify Security Operations Platform. Siemplify's patented threat-centric technology automatically groups related alerts into threat-centric cases.

Joint Playbook

- Virus alert trigger from MVISION EDR generates automatic enrichment of endpoint entity data from MVISION ePO
- Enrich cases with threat intelligence data by scanning the file hash within VirusTotal and querying other 3rd party tools in your environment
- Collaborate with analysts on the case if manual input or reviews are required by using multiple-choice question steps
- Take response actions such as adding tags to devices, adding insights to a case, launching investigations, killing processes, removing files and/or quarantining hosts
- Automatically close alerts as false positives if all enrichment data comes back negative
- Send email updates or instant messages to a specific team member per your standard incident workflows

Siemplify & McAfee

JOINT SOLUTION **BRIEF**

Joint Use Case

Automate MVISION EDR Response to Malware Detections

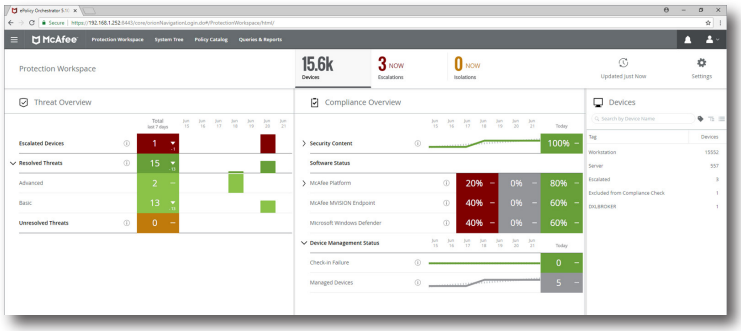
In this use case, an endpoint on your network is acting in a highly suspicious manner. MVISION EDR has detected a few behaviors such as background file activities that contain powershell.exe commands that are connecting the endpoint to a suspicious external host. These process activities generate an alert regarding the suspicious file and additional context on the device such as the hostname, operating system, and IP address.

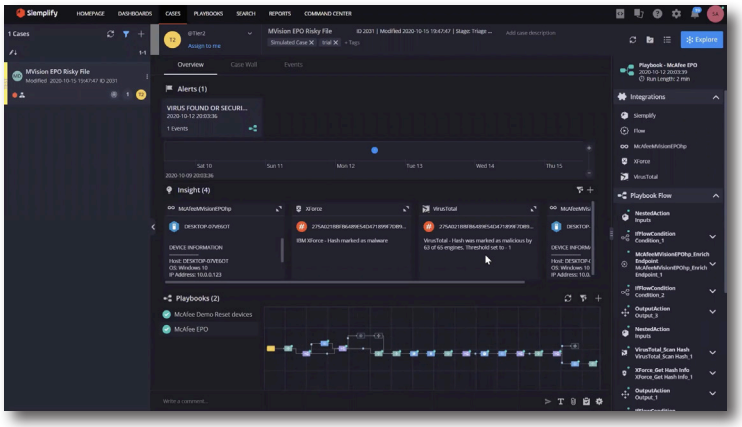
While the alert is generated by an MVISION EDR detection, it is centrally managed alongside other McAfee alerts within the McAfee ePO management platform. Siemplify's API-based integration with MVISION ePO creates the ability to ingest the ePO alert data into a new case investigation. Siemplify will group this alert along with other alerts with the same entity into a single case for further analyst investigation.

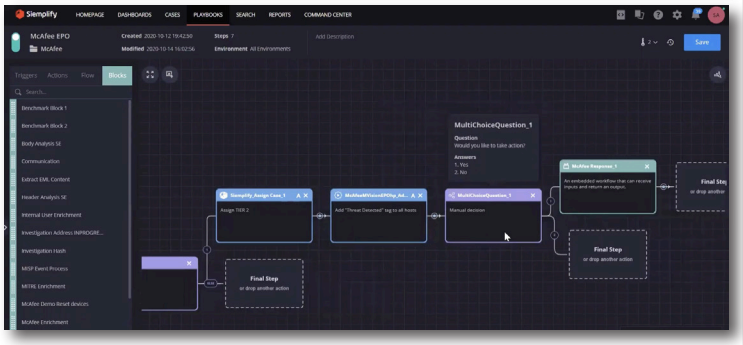
As a vendor-agnostic SOAR platform, Siemplify is able to integrate with the other security tools in your stack to provide insights within the case. These can include using the file hash to check your 3rd party threat intelligence feeds or scanning the file hash with VirusTotal.

At the heart of the case investigation are Siemplify playbooks that tie all of your tools together to create a series of logical actions in an automated workflow. In this case, the playbook drives the previously mentioned enrichment actions and can progress the investigation forward and assign a case depending on the enrichment data.

A well-constructed playbook helps reduce the effort an analyst would normally need to take in terms of updating the status of the case, sending confirmation emails to the IT team, and/or posting a Slack message with a status update. It can utilize manual intervention conditions such as using 'yes or no' multiple-choice questions like "Do you want to quarantine the affected endpoint?" Finally, the playbook can make a false positive decision and automatically close a case based on the enrichment information received early in the process.







Siemplify

About Siemplify

The Siemplify Security Operations Platform is an intuitive, holistic workbench that makes security operations smarter, more efficient and more effective. Siemplify combines security orchestration, automation and response (SOAR) with context-driven case management, investigation, and machine learning to make analysts more productive, security engineers more effective, and managers more informed about SOC performance.

Learn more at www.siemplify.co or follow us on Twitter at @Siemplify.

McAfee

About McAfee

McAfee is the device-to-cloud cybersecurity company. Inspired by the power of working together, McAfee creates consumer and business solutions that make our world a safer place.

Learn more at www.mcafee.com.

Try it out for free at siemplify.co/community

© Copyright 2020 Siemplify