SIEM Orchestration

How McAfee Enterprise Security Manager can drive action, automate remediation, and increase situational awareness

Scott Taschler, Solution Architect, McAfee
# Table of Contents

<table>
<thead>
<tr>
<th>Section</th>
<th>Page</th>
</tr>
</thead>
<tbody>
<tr>
<td>Introduction</td>
<td>3</td>
</tr>
<tr>
<td>Orchestration Triggers</td>
<td>4</td>
</tr>
<tr>
<td>Orchestrationing Action</td>
<td>4</td>
</tr>
<tr>
<td>McAfee® ePolicy Orchestrator (McAfee ePO™)</td>
<td>5</td>
</tr>
<tr>
<td>Reporting on Suspicious Systems</td>
<td>5</td>
</tr>
<tr>
<td>Practical Example: Flagging suspicious systems for follow-up</td>
<td>5</td>
</tr>
<tr>
<td>Dynamic McAfee ePO Policy Changes</td>
<td>7</td>
</tr>
<tr>
<td>Trigger McAfee ePO Client Task Execution</td>
<td>7</td>
</tr>
<tr>
<td>Practical Example: Quarantine and remediation of compromised system</td>
<td>8</td>
</tr>
<tr>
<td>McAfee ePO Configuration</td>
<td>11</td>
</tr>
<tr>
<td>McAfee® Network Security Platform (NSP)</td>
<td>12</td>
</tr>
<tr>
<td>Configuring McAfee Network Security Platform</td>
<td>13</td>
</tr>
<tr>
<td>Practical Example: Behavior-based blacklisting</td>
<td>14</td>
</tr>
<tr>
<td>McAfee® Vulnerability Manager (MVM)</td>
<td>16</td>
</tr>
<tr>
<td>Configuring McAfee Vulnerability Manager</td>
<td>16</td>
</tr>
<tr>
<td>Orchestrating actions with other tools</td>
<td>16</td>
</tr>
<tr>
<td>Configuring Scripting</td>
<td>17</td>
</tr>
<tr>
<td>Other Examples</td>
<td>18</td>
</tr>
<tr>
<td>Next Steps</td>
<td>18</td>
</tr>
</tbody>
</table>
Over the last 2 decades, Security Information and Event Management (SIEM) adoption has increased dramatically, driven largely by compliance requirements such as PCI DSS and SOX, as well as the needs of incident response teams. As adoption increased, enterprises quickly realized the value of the SIEM in providing “situational awareness;” visibility into activities occurring around the enterprise, and the ability to identify and track security incidents as they occur. Good situational awareness allows enterprises to detect attacks sooner, and as a result react more nimbly.

Introduction

Times change. According to Verizon’s 2013 Data Breach report, 84 percent of today’s exploits and 69 percent of data exfiltrations are executed in hours or less. However, from the time attacks are detected, 77 percent of incidents took days, weeks, or months to contain. 1

This slow response is driven largely by processes and tools that have not kept up with the rapid acceleration in attack speed. Attack responses often are loosely coordinated affairs, requiring the cooperation of multiple teams across the enterprise. Efforts follow manual workflows that require human intervention at multiple steps along the way. If there is to be any hope of stopping intrusions before the damage is done, we must find ways to optimize and automate these processes as much as possible.

Similar evolution occurred in the Network Intrusion Detection System (NIDS) space in the early 2000s. At that time, NIDS were well-established methods of identifying network-based attacks, based largely on attack signatures. As detection methodologies improved, administrators realized that it was feasible to rely on these tools to make policy enforcement decisions, and actually block known attacks; the Network Intrusion Prevention System (NIPS) was born. While not a silver bullet, NIPS significantly raised the bar that an attacker needed to cross in order to execute a successful attack.

Ten years later, SIEM is at the same crossroads. No longer is it sufficient to simply detect threats to our networks. SIEM can be used not just to improve situational awareness, but as a platform to orchestrate responses, and to stop attacks well before they become breaches.

This document begins by outlining the kinds of activities that are well suited to orchestration. Following this, we’ll take a deep look at McAfee® Enterprise Security Manager, the McAfee SIEM, and examine how it works as part of the McAfee Security Connected platform to optimize incident response processes.

1 http://www.verizonenterprise.com/DBIR/2013/
**Orchestration Triggers**

The first step in effectively responding to an attack is identifying triggers that will begin the process. The best triggers clearly describe a suspicious or malicious behavior, with enough precision that the reaction to it is clear. Triggers must also be highly accurate, if they are to be relied upon for automated responses. Below are a few examples.

- **Anti-social behaviors.** Most enterprises will see activities coming from within or outside their networks that, while not immediately alarming, are clearly not related to their business. Often times these behaviors are the precursors to an actual attack.
- **Password guessing.** High volumes of incorrect passwords are indicators of automated tools used by attackers to attempt to guess user credentials.
- **Network Reconnaissance.** Host scans, port scans, and similar activities are equivalent to jiggling the doorknob of a house to see if it’s locked. This kind of activity should only originate from very trusted partners.
- **Application Reconnaissance.** Attackers will often begin a campaign with a series of probes designed to understand the attack surface of their target. This activity may be seen in application logs as high volumes of requests from a host, often for resources that do not exist.

These activities happen so frequently in most organizations that it is not feasible for human analysts to follow up on each one. As a result, the records of these activities become simple fodder for regular executive rollup reports, or perhaps part of the evidence chain uncovered while investigating a breach. However, an effective SIEM platform can take appropriate actions in response to these behaviors, and stop attacks at their earliest stages.

- **Signs of malware infection.** Fighting malware is a daily part of the job for any enterprise security professional. Most malware is detected and dealt with efficiently by technologies at the endpoint (such as McAfee® Endpoint Protection Suites) and malware detection in network devices, including next-generation firewalls (McAfee® Next Generation Firewall powered by Stonesoft), network intrusion prevention systems (McAfee® Network Security Platform), web protection gateways (McAfee® Web Gateway), and advanced threat protection appliances (McAfee® Advanced Threat Defense). However, when especially targeted or evasive malware does get around these defenses, it can be difficult to detect and eradicate. Signs of malware infection include:
  - **Alerts and blocking based on IPS events.** Most IPS products include signatures designed to identify traffic associated with botnet command-and-control networks, and similar behaviors.
  - **Communication with suspicious hosts.** Many IPSs and SIEMs today incorporate geolocation, reputation feeds, and other contextual feeds that allow enterprises to track known malicious hosts and communication patterns within the enterprise. Internal hosts seen to be communicating with suspect hosts in other parts of the world merit additional follow-up as these activities are indicators of infected hosts.
  - **DNS requests.** DNS requests for resolution of domain names that are associated with known purveyors of malware are clear signs of infection.
- **Anomalous behaviors.** In any network there are unexplained, outlier behaviors that can be excellent signs of systems that have been subverted or are otherwise not being used for their intended purpose.
  - **NetFlow volumes and patterns.** NetFlow records provide useful metadata about what systems are communicating, and how much, in the enterprise. While individual NetFlow records may provide little useful information, over time, NetFlow records can be aggregated to establish a unique fingerprint that identifies how and when a system (or a class of systems) communicates. Deviations from this baseline can provide useful indicators of compromise.
  - **Suspicious network traffic.** Tools such as McAfee® Network Threat Behavior Analysis (used with the McAfee Network Security Platform) collect and analyze traffic from the entire network—host and applications—to detect unusual behavior resulting from worms, botnets, zero-day threats, spam, and reconnaissance attacks.

While most enterprises strive to investigate these types of events, the sheer volume can quickly become overwhelming to incident responders. Even running a simple malware scan on a likely infected host may take hours or days to get scheduled, depending on the organization’s operational maturity. All the while, the malware is free to execute the attacker’s payload, perhaps exfiltrating data, or free simply to spread more deeply into the enterprise. What’s needed is a simple, automated method to stop attacks as soon as they are detected. Freezing the attack gives responders breathing room to investigate the scope and take advanced remediation steps as needed.

**Orchestrating Action**

McAfee® Enterprise Security Manager provides a rich platform to automate responses to the kinds of triggers discussed above. McAfee Enterprise Security Manager has direct ties into many pieces of the McAfee Security Connected Platform, which allows administrators to orchestrate responses easily without complicated custom integrations. In addition, McAfee Enterprise Security Manager provides open interfaces to allow integration with third-party products.
McAfee Enterprise Security Manager actions are driven by alarms triggered by a wide range of events, including those described above. You can configure each alarm to launch a variety of actions. Below we'll discuss some of the orchestration options possible with McAfee® Enterprise Security Manager and its complementary products.

**McAfee ePolicy Orchestrator® (McAfee ePO™)**

Integrated closely with McAfee Enterprise Security Manager, McAfee ePO provides policy-based management of a wide range of endpoint, data center, and network security countermeasures, including antivirus, host intrusion prevention, whitelisting, activity monitoring, and data loss prevention.

McAfee ePO lets administrators categorize systems via manual or criteria-based “tags,” which may then be used as the basis for assigning configuration profiles to assets, launching tasks on managed endpoints, or filtering dashboards and reports.

McAfee Enterprise Security Manager integrates with McAfee ePO via the ePO Web API. Through this channel, McAfee® Enterprise Security Manager can assign tags to systems in ePO in response to triggers seen by McAfee Enterprise Security Manager, just as a McAfee ePO admin might do via the ePO GUI. Through tags, McAfee Enterprise Security Manager can automate many “first response” actions, helping organizations respond to attacks more quickly and efficiently than would be possible when relying on SOC staff to drive incident responses.

**Reporting on Suspicious Systems**

In one of the simplest use cases, a tag may be used as a filter for a dashboard or a report in McAfee ePO. Security operations staff often use a custom dashboard or role-based report to regularly monitor the status of the technologies managed via McAfee ePO, and to identify events where a response may be necessary. This process provides excellent visibility into the different security countermeasures that McAfee ePO manages, but is blind to the rest of the enterprise environment.

McAfee Enterprise Security Manager provides deep situational awareness to complement standard McAfee ePO visibility. By assigning the proper tags, McAfee Enterprise Security Manager can quickly and automatically bring systems exhibiting suspicious behaviors to the attention of endpoint security operations. Security operations can then take appropriate actions as needed.

**Practical Example: Flagging suspicious systems for follow-up**

In many enterprises, the team that handles endpoint security leverages McAfee ePO as a tool to drive day-to-day workflow for incident response. For example, a system that reports large volumes of repeated malware infections in a short time often has additional undetected malware running behind the scenes. In this circumstance, the system requires human analysis to review its state and health, and identify additional remediation steps needed.

Tagging helps incident response staff track systems that require investigation. A specified McAfee ePO tag may be used as a filter for a McAfee ePO dashboard or report, which in turn is monitored by incident response staff to drive daily remediation activities. This approach may be extended easily to allow McAfee Enterprise Security Manager to tag suspicious systems based on a wide variety of criteria.
Endpoint security staff gain greater awareness of enterprise security posture and can prioritize remediation efforts on the systems with the most severe security issues.

- **Setup: McAfee ePO.** In order to take advantage of this use case, it’s first necessary to perform appropriate setup in McAfee ePO.
  - Identify or create a McAfee ePO tag to use as a means to flag systems that require manual analysis. For purposes of discussion, we’ll name this tag “FILTER: Suspicious Systems”. Set up this tag as a manual tag in McAfee ePO.
  - Identify or create a dashboard in McAfee ePO that will be used to track suspicious systems. Each query in the dashboard should include the “FILTER: Suspicious Systems” tag as a filter, ensuring only data associated with tagged systems are displayed. For our purposes, we will use the tag as a filter for the McAfee ePO System Tree.

- **Identify SIEM Trigger.** The next step is to identify the conditions seen by McAfee Enterprise Security Manager on which you would like to trigger. The potential triggers here are virtually limitless. They depend largely on the data sources that are present in your SIEM; the correlation rules that you have at your disposal; and the types of things into which the endpoint security team would like visibility. For our purposes, we’d like to notify the McAfee ePO team anytime the enterprise web proxy (such as McAfee Web Gateway) detects an attempt to download a malicious file. These systems deserve inspection since systems that attempt to download malware are often already infected with malware.

  - **Enable alarm.** While it’s certainly possible to manually trigger the McAfee ePO tagging action (via the McAfee Enterprise Security Manager action menu), in our example we will automate this process to ensure that the endpoint security ops team has immediate visibility to the latest threats. As the final configuration step, we must configure McAfee Enterprise Security Manager with an alarm that is triggered by the event we’ve identified above, and takes the action of applying the “FILTER: Suspicious Systems” on the target systems.
• Monitor dashboard in McAfee ePO. Once the alarm is configured, you should begin to see systems tagged appropriately in McAfee ePO, and they should automatically begin to appear in the "Suspicious Systems" dashboard. After the analyst reviews the systems and takes appropriate remediation steps taken, the analyst can remove the tag, and the system will be removed from the dashboard.

![System with web malware detections flagged as suspicious in McAfee ePO.](image)

**Dynamic McAfee ePO Policy Changes**

In the context of McAfee ePO, a "policy" is a collection of settings that you create and configure, then enforce on a set of managed systems. The McAfee ePO console allows administrators to configure user- and systems-based policy settings for all products and systems from a central location. For example, McAfee ePO policies provide complete control over all aspects of endpoint security, from the aggressiveness of on-access scanning to the network connections allowed by the endpoint firewall.

McAfee McAfee ePO policies may be assigned in a number of different ways. One highly flexible method is via Policy Assignment Rules. With McAfee ePO Policy Assignment Rules, policies may be assigned to managed systems using a flexible set of criteria and updated on the fly as those criteria change. Asset tags are one of the criteria supported by Policy Assignment Rules in McAfee ePO. By leveraging McAfee Enterprise Security Manager to manipulate McAfee ePO asset tags in response to triggers, we can modify policies on those assets in near real time in response to changing conditions or detected threats.

Essentially, we can take the incremental data that becomes visible through McAfee Enterprise Security Manager-to-McAfee ePO integration, and use that data to modify policies that, in turn, affect countermeasures.

![McAfee ePO Policy Assignment Rules.](image)

**Trigger McAfee ePO Client Task Execution**

A client task in McAfee ePO is an action that is pushed to and executed on a managed endpoint. Examples of client tasks include scheduled antimalware scans and deployment of security agent software. Like policies, a client task may be assigned to a system in a variety of ways within McAfee ePO. For example, client tasks may be tied to asset tags, such that assigning a tag to a system brings with it a set of associated client tasks.
Client task assigned to systems based on McAfee ePO asset tags.

By leveraging McAfee Enterprise Security Manager to manipulate McAfee ePO asset tags in response to triggers, we can immediately execute tasks on managed systems in response to changing conditions or detected threats.

**Practical Example: Quarantine and remediation of compromised system**

In the course of investigating an ongoing attack or breach, it sometimes becomes clear that there is a definitive pattern of behaviors that indicate a compromised system. Examples might include communication with a specific IP address, repeated brute-force password guessing attempts, or specific malware detections. Regardless of the indicators, the first step for incident responders should be to isolate the compromised system from the enterprise network as quickly as possible, to minimize the amount of damage that will be done.

In this example, we will leverage the SIEM to orchestrate a real-time response with McAfee ePO, effectively quarantining the compromised host and launching an aggressive malware scan. These remediation actions should neuter the threat in real time, minimizing the impact much more quickly and effectively than would be possible when relying on human analyst response.

- **Setup: McAfee ePO policies and tasks.** The first step in meeting this use case is to define a set of “lockdown” policies and tasks in McAfee ePO that will be engaged when McAfee Enterprise Security Manager detects the compromise. Your optimal set of policies will be dictated by the managed products you have in McAfee ePO. Below you will find some suggestions:
  
  - **McAfee Host Intrusion Prevention (HIPS) Firewall:** Enable firewall, with highly restrictive rule set
  - **VirusScan Access Protection:** Enable “Maximum Protection” rules. Consider implementing custom rules to block network traffic if HIPS is not deployed in your environment.
  - **VirusScan On-Access:** Enable scanning inside archives, eliminate scanning exclusions, and set Artemis to “Very High” sensitivity level.
  - **VirusScan On-Demand Scan Task:** Define a scan task to deeply assess all drives and files, with no exclusions.

- **Setup: Map McAfee ePO policies and tasks to tags.** Once you define client tasks and lockdown policies, the next step will be to tie these to one or more tags. In our example, we will define two separate tags:
  
  - **POLICY:** Lockdown
  - **TASK:** Aggressive Scan. The first of these tags will be tied to the various lockdown policies via a McAfee ePO Policy Assignment Rule, as shown in the screenshots below.
In the case of the On-Demand client task, we will leverage client task assignment criteria in order to automatically enable the Emergency Scan task on any systems with the "TASK: Aggressive Scan" tag.

We have now completed the setup within McAfee ePO. Any systems that are assigned to the relevant tags in McAfee ePO will automatically have the proper policies and tasks pushed down the next time the system communicates with McAfee ePO.

- **Identify SIEM Trigger.** The conditions that are used to trigger the actions in this use case are entirely dependent on the specifics of the threat you wish to respond to. In our example, we will deal with a hypothetical threat, which has three behaviors that are easily observable:
  - Communication with known malicious IP addresses
  - Multiple attempts to guess root account passwords
  - Attempts to download and install malware

Given this information, we will define a simple correlation rule that triggers when we see these behaviors together, associated with a single host.
A correlation rule can be defined for individual systems.

- **Enable alarm.** All that remains is to define a set of actions that will be executed when our triggering rule fires. We will do this by defining an alarm tied to the correlation rule. This alarm will take the primary action of “Assign Tag with McAfee ePO.”

We will leverage this alarm to assign both our “POLICY” and “TASK” tags to the affected system. We will also check the box labeled “Wake up client” in the McAfee ePO Tagging configuration. By default, McAfee ePO clients check in with McAfee ePO on a regular interval, which is typically every 1-2 hours. Checking the “Wake up client” box will ensure that the affected client immediately
communicates with McAfee ePO, and receives its updated policies and tasks in near real-time. In practice, policy enforcement should occur in less than 1 minute from the time the alarm is triggered.

Define Actions: Associate Policy and Task with an Action.

McAfee ePO Configuration

McAfee Enterprise Security Manager can leverage McAfee ePO tagging actions for any internal hosts (defined by the "Homenet" variable in the Network Discovery tab of the ESM Asset Manager). McAfee Enterprise Security Manager can drive McAfee ePO tagging actions in two ways. First, McAfee ePO tags may be assigned manually by a SIEM analyst, via the actions menu in the McAfee Enterprise Security Manager UI. In this model, a SIEM analyst identifies a triggering event via manual review and leverages McAfee ePO tagging to orchestrate follow-up activity on the affected system.

Manual Assignment of McAfee ePO Tags.

When the “McAfee ePO Tagging” option is selected by the analyst, he or she is presented with a list of tags that have been defined in McAfee ePO, and is then free to select the tags appropriate for the actions the analyst wishes to take.

McAfee ePO tags may also be applied to systems in McAfee ePO automatically, by leveraging McAfee Enterprise Security Manager alarms. Alarms are triggered by a wide range of conditions, and each alarm has a set of actions associated with it that are executed when the alarm triggers. “Assign Tag with McAfee ePO” is one of the supported options.
Automated Assignment of McAfee ePO Tags via Alarm Actions.

As in the manual case described above, when a system administrator clicks the “Configure” button seen above, the system presents a list of tags that have been defined in McAfee ePO. The administrator can then select the appropriate tags for the actions desired in response to the defined conditions.

As you can see, with proper configuration within McAfee ePO, asset tags can be used to allow McAfee Enterprise Security Manager to exert a high degree of control over the security posture of a system managed by McAfee ePO, either as part of a manual incident analysis process, or automatically.

**McAfee Network Security Platform (NSP)**

The McAfee Network Security Platform provides a full range of network-based intrusion detection and prevention features. The Network Security Platform includes a number of components:

- **McAfee Network Security Manager (NSM)**. The McAfee Network Security Manager provides centralized management, analysis, and reporting capabilities for McAfee Network Security Platform.

- **NSP Sensors**. Sensors are deployed on network segments to monitor traffic and enforce security policy as configured in the McAfee Network Security Manager. McAfee Network Security Platform sensors, when deployed inline on a network segment, provide the ability to block attacks in real time.

- **McAfee Network Threat Behavior Analysis (NTBA)**. McAfee Network Threat Behavior Analysis collects and analyzes traffic from the entire network—host and applications—to detect worms, botnets, zero-day threats, spam, and reconnaissance attacks. It reports any unusual behavior to help you maintain a comprehensive and efficient network security infrastructure.

McAfee Network Security Platform provides a highly intelligent security solution that discovers and blocks sophisticated threats in the network. However, like any IPS, its visibility (and ability to react) is limited based on where McAfee Network Security Platform Sensors are deployed.

McAfee Enterprise Security Manager is a natural complement to McAfee Network Security Platform. The McAfee Enterprise Security Manager access to activity logs from the entire enterprise gives it global visibility that is often missing in network-based security controls. McAfee Enterprise Security Manager integrates to McAfee Network Security Manager via the McAfee Network Security Platform Open API.
Overview of McAfee Enterprise Security Manager/McAfee Network Security Platform Operational Workflow.

Configuring McAfee Network Security Platform

From within the McAfee Enterprise Security Manager Console, McAfee Network Security Platform blacklist actions are available for any hosts, internal or external. Successful blacklisting requires a McAfee Network Security Platform sensor to be deployed inline; only network traffic that traverses an McAfee Network Security Platform sensor can be blocked in this manner. In practice, this tends to limit blacklisting to network choke points, such as perimeter links or data center boundaries.

In addition to inline deployment, a few configuration steps are necessary within McAfee Network Security Platform before McAfee Network Security Platform blacklisting can be enforced. On the McAfee Network Security Manager, an appropriate Network Access Zone should be defined, which outlines precisely what traffic is blocked and allowed for any blacklisted hosts. Network Access Zones are defined in the NSM UI under “Policy/Intrusion Prevention/IPS Quarantine/Network Access Zones.” In addition, the IPS Quarantine feature must be enabled on desired network interfaces. This selection is located under “Devices/Policy/IPS Quarantine/Port Settings”.

McAfee Network Security Platform blacklisting may be driven by McAfee Enterprise Security Manager in two ways. First, blacklist entries may be assigned manually by a SIEM analyst, via the actions menu in the McAfee Enterprise Security Manager UI. In this model, a SIEM analyst identifies a triggering incident via manual review, and leverages NSP blacklisting to block traffic to/from the affected system.

When you select the “Blacklist” option, you see a list of McAfee Network Security Platform sensors where the blacklist should be enforced. The blacklist entry can be applied to all sensors in your enterprise, via the Global Blacklist, or to an individual sensor you select.
For an orchestrated approach, blacklist entries may also be implemented automatically, by leveraging McAfee Enterprise Security Manager alarms. As discussed above under “Orchestration Triggers”, a wide range of conditions can trigger alarms, with associated actions that execute when the alarm triggers; “Blacklist” is one of the supported options.

As in the manual case described above, when you click the “Configure” button seen above, the system presents a list of McAfee Network Security Platform sensors. You are then free to select the sensor where the automated blacklist is to be enforced, or to apply the new entry to the Global Blacklist.

When integrated with McAfee Network Security Platform, McAfee Enterprise Security Manager becomes a powerful extension of the McAfee Network Security Platform detection engines. McAfee Enterprise Security Manager provides actionable intelligence to the McAfee Network Security Platform Sensor, which can then block attacks in real time.

Practical Example: Behavior-based blacklisting
Reconnaissance attacks represent one of the most frequently seen types of alerts coming from network-based IDS and firewalls. Reconnaissance activities indicate an adversary is gathering useful information about an enterprise, such as IP addresses in use, open ports, applications, and possible weak passwords. Data gathered during reconnaissance may then be used in later phases of a targeted attack.

While reconnaissance activity is seen frequently, it can be difficult to act upon. High volumes of this kind of activity make it impossible for security analysts to follow up directly on each incident. The nature of reconnaissance techniques makes it very difficult to block outright without also affecting authorized traffic coming from customers and trusted partners. However, once an attacker has tipped his hat by showing this kind of behavior, we can leverage SIEM to orchestrate an automated response at the network layer, blocking future connections from the attacker.

- **Setup: McAfee Network Security Manager.** In this use case we will leverage a McAfee Network Security Platform Sensor to block traffic from the attacker. In order to properly execute the blacklist, we will assume we have a McAfee Network Security Platform Sensor deployed inline on the perimeter Internet connection. You must also define a tightly restricted Network Access Zone, and enable quarantine on the relevant McAfee Network Security Platform Sensor interface.

- **Identify SIEM Trigger.** There are wide ranges of reconnaissance activities that represent reasonable triggers for a McAfee Network Security Manager quarantine action. While it might be tempting to aggressively block based on any type of reconnaissance activity, care must be taken to avoid reacting to potential false positive events. Initially, it's best to focus on a small number of behaviors that represent clear and accurate signs of bad intent. Good candidates include activities such as repeated failed login attempts, or repeated connections from known malicious IPs, which are unlikely to be triggered benignly.

In our example, we will look for high volumes of HTTP 404 (File not Found) logs coming from an Apache web server. High volumes of these logs are very good indicators that an adversary is fingerprinting a web application, identifying the surface area available for a future attack. In order to provide flexibility in tuning this behavior pattern, we'll define a custom correlation rule in McAfee Enterprise Security Manager.
HTTP Reconnaissance Correlation Rule.

- **Enable alarm**: Finally, we will configure an alarm in McAfee Enterprise Security Manager. Our alarm will be triggered based on our custom correlation rule defined above. When the alarm is triggered, we will signal the McAfee Network Security Platform Sensor to block traffic for a duration of 60 minutes. In addition, we will trigger a report to run against the McAfee Enterprise Security Manager database and automatically sent via email to a security analyst. This report will include a summary of all activity seen from the source of the reconnaissance activity, for review by security analyst staff.

McAfee® Vulnerability Manager (MVM)

McAfee Vulnerability Manager provides enterprises with a comprehensive, network-based vulnerability scanner, as well as tools and workflow to manage vulnerability remediation. Vulnerability data can be very useful to incident responders, as it helps to verify whether
individual hosts are at risk to specific attacks. In many circumstances, though, vulnerability scan data can be quite out-of-date; most enterprises tend to scan monthly or quarterly, in order to meet compliance requirements. During an incident response, it’s critical to have immediate access to the most current, accurate information on security posture.

**Configuring McAfee Vulnerability Manager**

McAfee Enterprise Security Manager integrates with McAfee Vulnerability Manager via the McAfee Vulnerability Manager OpenAPI and is easily configured by entering proper McAfee Vulnerability Manager credentials into the McAfee Enterprise Security Manager UI. Once connected, McAfee Enterprise Security Manager provides the ability to initiate a real-time vulnerability scan directly from the McAfee Enterprise Security Manager console. This integration ensures that analysts always have immediate access to the detailed information needed in order to make intelligent decisions while responding to security incidents.

![Diagram of ESM/MVM Operational Workflow]

Overview of ESM/MVM Operational Workflow.

Via the actions menu in the McAfee Enterprise Security Manager UI, you can initiate McAfee Vulnerability Manager scans manually for any internal hosts (defined by the “Homenet” variable in the Network Discovery tab of the ESM Asset Manager).

![Screenshot of ESM UI with MVM Scan option]

When triggered, the McAfee Vulnerability Manager Quickscan feature executes a comprehensive vulnerability scan against the selected target host. Scan results are available in the MVM dashboards immediately, and are imported into McAfee Enterprise Security Manager on the next McAfee Vulnerability Manager data synchronization.

**Orchestrating actions with other tools**

While McAfee provides simple, pre-built connectivity to many McAfee technologies via existing APIs, McAfee Enterprise Security Manager also provides an open interface to allow orchestrating action with other technologies from third parties. McAfee Enterprise Security Manager can be configured to execute custom scripts in response to triggers. You can write scripts in any scripting language that is supported on the Scripting Host, and then run scripts on a designated Scripting Host or launch them via SSH.
Configuring Scripting

Automated scripts may be set up as an alarm action in the McAfee Enterprise Security Manager UI. Within McAfee Enterprise Security Manager, you enter the information necessary to establish SSH communication with the Scripting Host, as well as the path to the script and any needed command-line parameters.

Once enabled, McAfee Enterprise Security Manager will execute the configured script each time the relevant McAfee Enterprise Security Manager alarm conditions are satisfied. This interface provides a highly flexible means to drive automated actions with a wide range of third party platforms. Common targets for third-party integration include: workflow and ticketing systems, firewalls, and Network Access Control platforms.
Other Examples
Below are a few additional use case ideas.

- Tracking infected systems during a malware outbreak
  - Trigger: DNS request for specified malware domain associated with the outbreak.
  - Action 1: Apply McAfee ePO filter tag to system, causing it to appear in McAfee ePO dashboard and drive McAfee ePO-based remediation workflow.
  - Action 2: Use custom script to push ACL to third-party firewall or NAC solution, blocking communication with external hosts.

- Stopping data exfiltration in progress
  - Trigger: Flow anomaly indicates unusually large volumes of data leaving the network from a single host.
  - Action: Apply McAfee ePO policy tag that brings restrictive Data Loss Prevention policies, to provide enhanced visibility of what’s happening on the endpoint. Quarantine if warranted.

- Alert on unauthorized changes
  - Trigger: configuration or policy change event coming from a switch, router, or mission-critical application.
  - Action: Custom script queries change management system to verify that the change was expected. Alerts threat responders if change is not authorized.

Next Steps
In this paper we have discussed the reality that today’s incident responders cannot continue to react manually in time to deal effectively with the expanding threat landscape. The concept of SIEM orchestration provides immediate, automated responses. It is the only way for a modern enterprise to protect against advanced attacks.

Consider the examples above and determine how they apply to your organization. Look for activities that take up significant time, and leverage orchestration concepts to automate and optimize where it makes sense.

Finally, please share your questions, thoughts, successes, and failures with others in the McAfee Community:

https://community.mcafee.com/community/business/siem