In Partnership with

McAfee™

Key Benefits

Detect and respond to security alerts quickly by using McAfee® Enterprise Security Manager with ServiceNow® Security Operations:

- Automate creation and resolution tracking of security incidents.
- Perform incident record enrichment with bi-directional sightings search capabilities and threat intelligence.

Respond Faster to Security Threats with ServiceNow and McAfee

Automated triage and remediation

The Challenge

Security teams are inundated with alerts while being overburdened with other maintenance and management tasks. Having to manually triage and track security incidents only delays the time-to-resolution and causes more damage to the customer environment. According to a study by the $(ISC)^2$, 62% of organizations are currently understaffed—it takes three to six months to fill open positions for cybersecurity personnel, and 10% of positions go unfilled. Clearly, we cannot keep up with the increasing volume of attacks through manual labor alone. Adding to the complexity are often highly manual remediation processes involving multiple consoles and multiple communication methods. This results in long response times and poor visibility across multiple systems and teams. Prioritized, real-time data and actionable intelligence are crucial in fighting the cybersecurity battle effectively and efficiently in a rapidly changing threat landscape.

McAfee and ServiceNow Joint Solution

Leading the fight against cybersecurity threats is McAfee® Enterprise Security Manager, which combines and correlates hundreds of data sources to provide real-time visibility into all activity on systems, networks, databases, and applications. It delivers certified integrations and easy customizations for the security operations center (SOC), enabling security professionals to prioritize, investigate, and respond to threats, while the embedded compliance framework and built-in security content packs simplify analyst and compliance operations.

McAfee Enterprise Security Manager is now integrated with ServiceNow Security Operations. ServiceNow Security Operations offers security incident response, vulnerability response, and threat intelligence. It's built using intelligent workflows, automation, orchestration, and deep connection with IT—all part of the Now Platform.

By connecting security with IT, security operations enriches security alerts and events with deep organization context and asset information, making it easier and faster for the SOC to prioritize, collaborate, and respond to security incidents more effectively. Through its intelligent automation engine, remediation tasks can be dispatched based on organizational roles and policies, orchestrating the next mile of workflow triggered by McAfee Enterprise Security Manager. This effectively reduces or eliminates the manual intervention previously required of security or IT personnel. Your security staff is free to focus on high-priority incidents and problem resolution.

Use Case

Security events detected by McAfee Enterprise Security Manager can trigger new events or security incidents to be created in ServiceNow Security Operations. Security Operations correlates the incident or event data with the ServiceNow Configuration Management Database (CMDB) and uses the asset data as part of a risk score calculation to prioritize the incident. This prioritization allows analysts to focus on security incidents that pose the greatest risk to their organization.

Next, Security Operations initiates pre-defined workflows based on the data received from McAfee Enterprise Security Manager, including routing the incident to the appropriate person or team for remediation and automating threat enrichment. For example, observables and indicators of compromise can be correlated against threat intelligence data. Security Operations can also automatically perform additional analysis on the security incident, ranging from retrieving running processes from the affected endpoints to sending a file hash for additional malware reporting. This makes information ready for further investigation or triage.

A sightings search into McAfee Enterprise Security Manager can also be initiated via orchestration for observables that may be present in the environment. This is useful if threat intelligence indicates a new threat that may not have been detected by your existing security tools. A sightings count is returned from McAfee Enterprise Security Manager to Security Operations.

As the ServiceNow platform spans security and IT, it's easy to collaborate across teams to resolve security incidents. Related IT tasks are linked to the security incident, and service-level agreements ensure accountability across teams.

When a security incident is resolved and closed, Security Operations automatically generates a timestamped post-incident review containing all actions related to the incident taken by ServiceNow. This can be used for audits or future learning as a knowledge base article. Customizable dashboards and reports track security posture and performance.

Together is power

In the cybersecurity defense lifecycle of protect, detect, correct, analyze, and adapt, McAfee and ServiceNow work together to shorten the iterations needed to detect and resolve security incidents. Via workflow automation and orchestration, you can do more with less, resulting in better security defenses in the ever-changing security threat landscape.

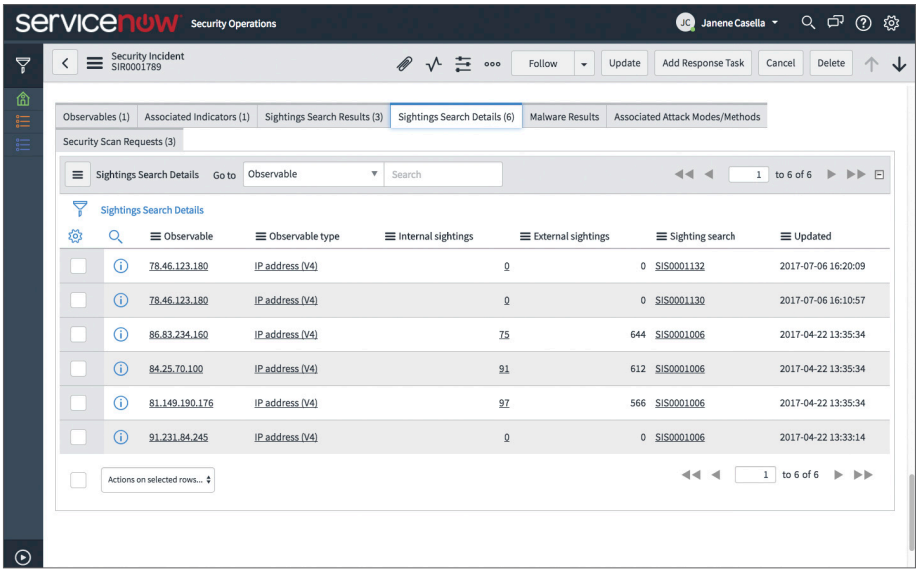
Going forward, McAfee and ServiceNow plan to build deeper and broader collaboration in order to provide additional threat response capabilities to our joint customers.

About ServiceNow

ServiceNow is changing the way people work. We help the modern enterprise operate at lightspeed and become more scalable than ever before. Customers use our platform to define, structure, and automate the flow of work, removing dependencies on email, spreadsheets, and other manual processes to transform the delivery of service to the enterprise. With ServiceNow Security Operations, customers can bring incident data from their security tools into a structured enterprise security response engine that uses intelligent workflows, automation, and a deep connection with IT to prioritize and resolve threats based on the impact they pose to your organization.

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.



Sightings search results from McAfee Enterprise Security Manager are displayed in ServiceNow Security Operations.