Solution Brief

Optimizing Security Operations

Integrate and automate for more effective threat and risk management

Headlines continue to illustrate the growing threat and risk management challenge. An increasing number of sophisticated attacks are countered with a finite pool of security operations resources. Detecting and managing these events is more difficult than ever as analysts grapple with siloed, distributed, and complex security and IT infrastructure. Analysts must surf the flood of data available from endpoints, cloud services, and critical environments, including data centers, manufacturing floors, and integrated control systems. Organizational and technical boundaries can make access to security data slow and erratic, impeding response and delaying remediation.

A recent Intel® Security survey of 565 security decision makers found that it takes an average of eight working days, or 64 hours, for a security investigation, from detection to return to health. And, on average, security decision makers use four tools to get the job done, with many using more than a dozen. The gaps between data sources, systems, and people lead to siloed decisions—which make sense for one group but might not support the best interests of the organization as a whole. Overall, closing these gaps through improved collaboration could increase efficiency by an average 38%, with even bigger gains for larger organizations.[1]

Figure 1. The gaps between data sources, systems, and people that lead to siloed decisions. (Source: ***Make Your Security Operations More Efficient)***

intel Security

A Shift to Adaptability

While dealing with attacks may monopolize the security operations center (SOC), the security operations team and the CISO must also oversee the larger organizational picture of risk and compliance. To bridge operational and data silos across these functions, an effective strategy requires an adaptive security architecture. This approach enables intelligent security operations that can support the current status quo, but are still able to evolve and embrace new technologies while mitigating new risks and supporting new compliance requirements. Adaptive security encourages a balance of preventative, detective, corrective, and predictive investments.

However, the greatest strategic implication of adaptability is the connection of the component features into a system. Centralized visibility, threat analytics, and orchestration create an efficient hub that enables critical outcomes. You can detect more threats faster, with fewer resources. This is just the beginning. Optimized security operations can seamlessly integrate threat and incident management processes with monitoring and compliance workflows and resources. This integration unlocks efficiency. The security team finally has a command-and-control center to optimize overall security operations.

The Intel Security System

Optimized security operations transform real-time security data and threat information into actionable intelligence, which feeds security management processes and guides continuous improvement. Intel Security makes this possible through an integrated security operations system that increases your efficiency and effectiveness.

As a system, it combines products and services from Intel Security as well as certified partners. An outside opinion is often the first step on the road to success. Intel Security and our alliance ecosystem partners provide strategic consulting and security infrastructure functionality to help you move to an intelligent security operations architecture. In these efforts, we find certain areas routinely need investment.

First, a well-defined response plan is key to optimizing threat management practices and minimizing the damage from a data breach. Many companies have a plan, but do not maintain or practice it. Additionally, threat management processes are overly manual and ad hoc. Security systems do not sufficiently identify and feed prioritized cases into incident response processes. Finally, organizations routinely do not record, share, or use lessons learned to improve processes, policies, and security controls.

Strategic Advice

Foundstone® Professional Services experts and accredited partners can help you identify gaps like these and determine the right course of action for your organization. Foundstone consultants benchmark the processes, products, and data you have in place with new capabilities and best practices. These assessments can guide your prioritization on where to invest to make your threat management implementation match your goals and improve operational performance.

Figure 2. An open design enables sustainable operations.

A True Platform

Enabling this transformation, Intel Security's SIEM solution, McAfee® Enterprise Security Manager, provides the core of a modular security operations platform that can include:

- McAfee Advanced Threat Defense for faster visibility into high priority events specific to your environment.
- McAfee Threat Intelligence Exchange to aggregate low-prevalence attack data, leveraging global, third-party, and local threat intelligence.
- McAfee Active Response for context-aware visibility of how security events affect real business processes and policies.
- Other Intel Security network and endpoint products to provide improved visibility, monitoring, and remediation.
- Certified partner product integrations, including user behavior analysis, vulnerability management, and data loss prevention.
- Threat intelligence sources (automated ingestion via Structured Threat Information eXpression (STIX)/Trusted Automated Exchange of Indicator Information (TAXII)).
- More than 450 off-the-shelf connectors to third-party security monitoring and reporting devices.

Off-the-shelf, certified integrations provide many ways to optimize security operations according to your needs, without the overhead and uncertainty of custom integrations. In addition, open interfaces and remote command and scripting increase the ways to merge new capabilities with existing systems and processes. Integrations enable more effective threat detection, triage, and analysis, orchestrating the data, systems, and decision-making required for intelligent security operations.

Expedited Results

Through this open environment, McAfee Enterprise Security Manager can add real-time visibility, integrate emerging intelligence and contextual data types most relevant to day-to-day security operations, and assist with advanced analytics that help security operations efficiently interpret what they see. You can identify if it is a threat, a compliance violation, if your organization has seen activity like this before, or if others in your industry have seen it.

McAfee Enterprise Security Manager offers many analytics within the core platform, as well as add-on modules that help you manage incident response for specific infrastructure and concerns. Analytics available today go far beyond black-and-white rules and simple correlations.

- Statistical deviations can flag anomalous behavior.
- Risk-based correlation monitors for changes that threaten critical systems and assets.
- Application layer inspection offers visibility into the content of each application for accurate analysis of usage, validation of application use policies, and detection of malicious or covert traffic.
- Non-intrusive database event monitoring shows database transactions, including all access to sensitive data and reporting on who is accessing your data and how.

The Network Effect

Optionally, McAfee Advanced Threat Defense can evaluate suspicious files taken from endpoints and network gateways and then send this data to McAfee Enterprise Security Manager. As part of ingestion from McAfee Advanced Threat Defense or another indicator of compromise (IoC) feed, the indicators are compared to existing data sets to see if an event has occurred previously. Teams can also set a watch list to monitor for future occurrences.

McAfee Active Response integrates with McAfee Enterprise Security Manager and the Intel Security endpoint portfolio to provide visibility into files, processes, system changes, and IoCs on endpoints. Quick searches can reveal dormant files, deleted files, and active processes in memory. With this insight, analysts and administrators can take action directly.

An Assist from Automation

Partial or full automation can expand the benefits of integration. While automation does not ever fully replace human judgment, it does remove some of the friction from the system and reduce the “tier 1” workload to lighten the burden on analysts and responders. For instance, automated workflows, scripts, and tasks can translate approved processes into efficient and timely actions. Each immediate, automated response can compress triage, scoping, and containment times—and even stop an attack in progress within seconds.

Some of the most obvious examples include quarantining a host or blacklisting an IP address, but our survey showed many organizations have multiple ways they are willing optimize incident response. The flexibility, extensibility, and tight integration of the Intel Security platform make these and many other tasks easier.

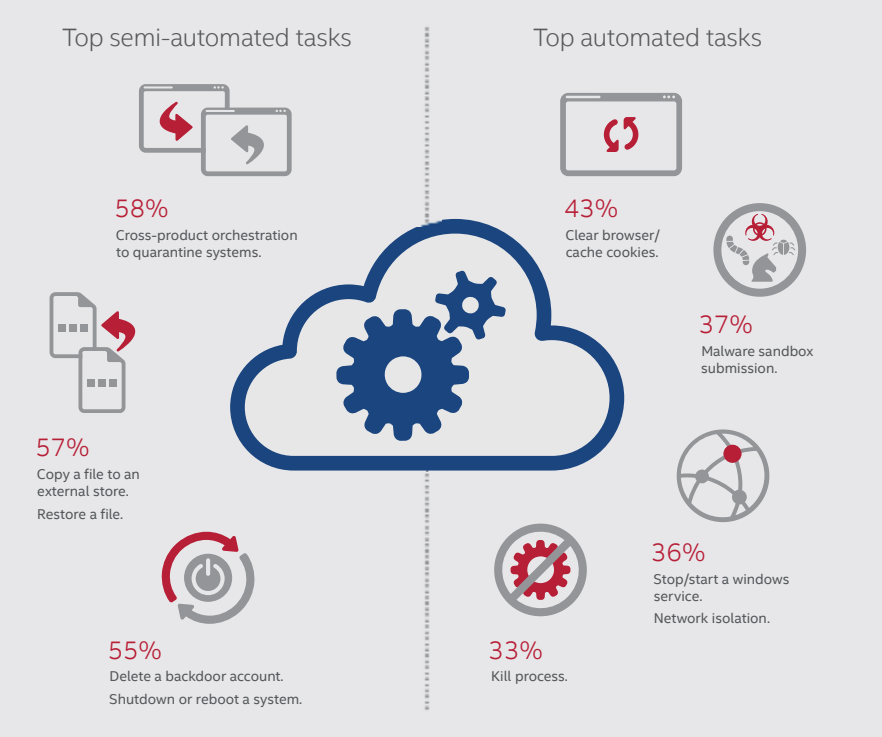

Figure 3. What manual tasks are you willing to automate or semi-automate? (Source: ***Make Your Security Operations More Efficient***)

A Sustainable Advantage

An open architecture that facilitates a flexible continuum from human-driven to full automation will offer you the most organizational resilience over the long term. For rapid success, we have integrated and developed centralized management to give you the greatest efficiency with the least effort and error. We offer mix-and-match solution components with certified partner offerings to fit within your existing security and IT infrastructure. This sustainable design lets you adapt operations based on your current and desired risk posture, your industry's threat profile, and changing compliance regulations.

Get Started

Security operations must find a practical way to overcome the increasing volume and velocity of external attacks, while mitigating the risks and damage from insider errors and compliance violations. This is not a request for short-term fixes. It is a demand to look at long-term operational processes and enable long-term efficiencies. By understanding and facilitating visibility, analytics, and orchestration across domains and organizational boundaries, Intel Security offers services and an open platform to help you achieve ongoing operational success.

To learn more about optimized security operations solutions from Intel Security, visit **www.mcafee.com/SecOps**.

1. Intel Security Special Report: *How Collaboration Can Optimize Security Operations* **http://www.mcafee.com/us/resources/reports/rp-soc-collaboration-advanced-threats.pdf**

Why Intel Security?

- **Short time-to-value:** Unlike services-heavy offerings that can take weeks or months to deliver value, Intel Security solutions feature off-the-shelf integrations and content to provide immediate visibility and control over what is happening in your infrastructure.
- **Eliminate the noise:** You can turn raw data, business asset context, and confirmed threat data into prioritized, actionable insights and security intelligence.
- **Easy investigations:** Fast, detailed analysis and instant response to security event queries provide real-time visibility into critical events and enable rapid and focused response.
- **Simplified management:** Manage event and threat feed ingestion, policies, and deployment through a single dashboard for visibility and workflow efficiency.
- **Sustainable advantage:** Seamless integration of Intel Security and partner products with existing and developing cloud, management, and advanced analytics solutions results in much more efficient, effective overall security.
- **Focus on outcomes:** We are committed to helping you get the results that matter to your business, which means resolving more threats faster, with fewer resources.

McAfee. Part of Intel Security.
2821 Mission College Boulevard
Santa Clara, CA 95054
888 847 8766
www.intelsecurity.com