White Paper

Sustainable Security Operations

Optimize Processes and Tools to Make the Most of Your Team's Time and Talent

intel Security

Table of Contents

Introduction

The number and types of incidents organizations face daily are steadily increasing, as is the cost of complying with regulations and managing policies. Yet an unintegrated, distributed, and complex security and IT infrastructure makes it difficult for analysts to notice and act on important events, trends, and changes. It also impairs the security administrator's ability to identify, understand, and respond to risk factors and trends in a proactive and timely manner. In fact, a recent Intel Security survey of 565 security decision makers found that it takes eight working days, or 64 hours, for a security investigation, from detection to a return to health. And on average, security decision makers use 4 tools to get the job done.[1]

"Enterprises are coming to the realization that a fragmented or compartmentalized security operations design is ineffective against today's advanced security threats. The exponential increase in threat counts and complexity continues to add to the existing heavy burden of security operations."[2]

—*How Collaboration Can Optimize Security Operations*, Intel Security research, Jan. 2016.

Further compounding this challenge is an ever-growing volume of data. Threat intelligence and contextual data comes in from multiple separate sources and solutions—from the cloud, network, and endpoints—making it almost impossible to get a complete and coherent view of the security state across the environment.

While dealing with incidents monopolizes much of the security operations center (SOC)'s resources, the CISO is responsible for the larger picture of risk and compliance. In order to bridge operational and data silos across these functions, an effective strategy requires an adaptive security architecture that enables organizations to enact optimized security operations. This approach increases efficiency through integration, automation, and orchestration, and reduces the amount of labor-hours required while improving your security posture. This paper explores how you can successfully adopt sustainable security operations with optimized processes and tools. The goal is to compress decision making and action cycles to more quickly detect, contain, and remediate attacks, insider threats, and compliance infractions.

Optimized Security Operations

The most pressing activity for security operations is threat management. This urgency comes from the fact that cyberattacks are becoming more advanced, stealthy, and frequent. According to threat managers at enterprises worldwide, almost 6 out of 10 attacks in 2015 were not based on generic malware or caused by accidents, but involved more complex techniques wielded by motivated external and internal attackers.[3] These techniques enabled a 6% increase in targeted attacks, up from 26% to 32% between January 2015 and January 2016.[4]

However, many organizations recognize they lack adequate, let alone optimized, systems for threat management. In the 2016 SANS Incident Response Survey, 82% of respondents say their SOC abilities are still immature or maturing.[5] The reality is that organizations are complex. Navigating between operational and data silos results in too much scrambling, decisions made with too little information, and no way to scale. Siloed detection, analysis, and investigation systems prevent the effective delivery of actionable intelligence to incident responders or endpoint and network operations teams, who need these insights to create a precise diagnosis in order to accelerate containment and remediation efforts. Enterprises have cited this internal information sharing as an important missing link: better collaboration between SOC analysts, incident responders, and endpoint administrators is expected to improve incident response effectiveness by 38%, on average, and as much as 76–100% for the largest entities.[6]

Threat management may be the most visible challenge, but security operations are also responsible for managing overall business risk. Intel Security encourages an optimized security operations model that enables best practices for threat management as part of efficient security operations. This requires the adoption of a security framework that makes it easy to integrate security solutions and threat intelligence into day-to-day processes. Tools like centralized and actionable dashboards help integrate threat data into security monitoring dashboards and reports to keep operations and management apprised of evolving events and activities. By linking threat management with other systems for managing risk and compliance, you can better manage

Reap the benefits of optimized security operations:

- Identify and disrupt complex attacks underway
- Leverage vendor-provided, internally-generated, and industry-proven threat intelligence to identify potential risk exposure
- Scale limited resources to handle the expanded volume of security data and frequency and complexity of incidents
- Integrate threat management into other security operations to ease overall management and better leverage resources
- Provide actionable intelligence and effective attack responses to accelerate containment and remediation
- Integrate case data to enable efficient collaboration for incident response and compliance workflows

your overall risk posture. You gain continuous visibility across systems and domains and can use actionable intelligence to drive better accuracy and consistency into your security operations. Centralized functions reduce the burden of manual data sharing, auditing, and reporting throughout.

These actions optimize and operationalize threat management. When a high priority incident occurs, you are best prepared to leverage existing resources, from talented teams and surge staffing to dashboards, case management workflows, and procedures. Beyond more efficient use of analysts and responders, optimized systems improve the ability to measure and report progress to interested parties, such as the board and executive leadership, using standardized dashboards and communication tools.

Of course, you can't build this all in a day; a practical approach to your adoption process will achieve better results. Select a security infrastructure that makes it easy for you to progress in a modular fashion, based on your readiness to advance your maturity model, your current and expected risk posture, and your industry's threat profile and compliance regulations.

Design Principles

Evaluate Your Organizational Maturity

Operationalizing threat management should start with a thoughtful assessment. In addition to your defenses, evaluate your processes and policies. Where is your organization strong? What are your gaps? What is your risk posture? What data do you collect, and how much of that data do you use?

While every organization is different, certain core capabilities and best practices represent due care today. A reasonable threat management process starts with a plan, and includes discovery (including baseline calculation to promote anomaly detection, normalization, and correlation), triage (based on risk and asset value), analysis (including contextualization), and scoping (including iterative investigation). Threat management processes feed prioritized and characterized cases into incident response programs. A well-defined response plan is absolutely key to containing a threat or minimizing the damage from a data breach.

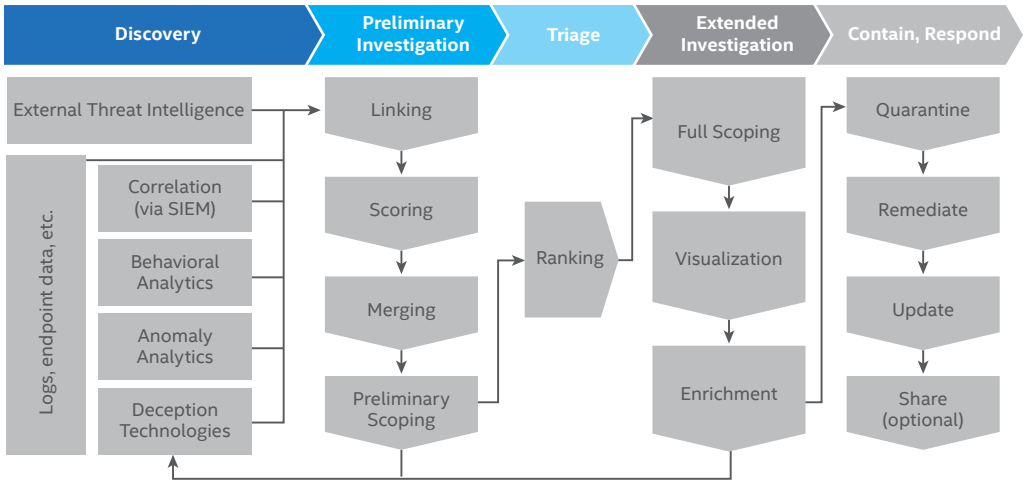

Figure 1. Threat management plans integrate and structure many processes across security and IT operations.

Effective visibility and threat management will draw on many data sources, but it can be hard to sort out the useful and timely information. The most valuable data has proven to be event data produced by countermeasures and IT assets, indicators of compromise (IoCs) produced internally (via malware analysis) and externally (via threat intelligence feeds), and system data available from sensors (e.g., host, network, database, etc.).

Data sources like these are not just an input to threat management. They add context and make the information valuable and actionable for more precise, accurate, and speedy assessment throughout the iterative and interactive threat management effort. Your access to, and effective use of, the right data to support your plans and procedures is a measure of your organizational maturity. A "mature" scenario would include a workflow that hands off the right information or permits direct action within operational consoles and across products. This flow integrates your IT operations and security teams and tools into incident response when you have a critical event.

All of these assessments will help you prioritize where you need to increase investment or reduce friction in order to make your threat management implementation match your goals. Consultants and penetration tests can help you benchmark your strategy and organizational maturity and health check your security response against attacks to obtain a current measure of your ability to detect and contain malicious events. By comparing against peer enterprises, this vetted review can help justify and explain the need to redirect or invest in security resources.

While it's helpful to understand the prioritizations of your industry peers, ensure you refine them based on your environment. This comes from knowing your business, your priorities, your valuable data, and where it is.

Integrate for Better "Time to Results"

As you move to adopt an adaptive security architecture, the metrics switch from emphasizing volume to emphasizing time to results. Tracking and measuring meaningful incident response metrics—such as the time required to investigate, contain, and remediate events—will help, over time, to direct your attention to where you should make improvements. For example, the number one metric organizations use to track the effectiveness of security operations is the time from detection to containment. With 81.9% of breach compromises occurring within minutes and exfiltrations executed in a matter of days (67.8%),[7] time is of the essence. If your goal is to shrink this timeframe, your architecture should prioritize advanced threat analytics tied to process and data integration for a good balance of new attack comprehension and operational efficiency.

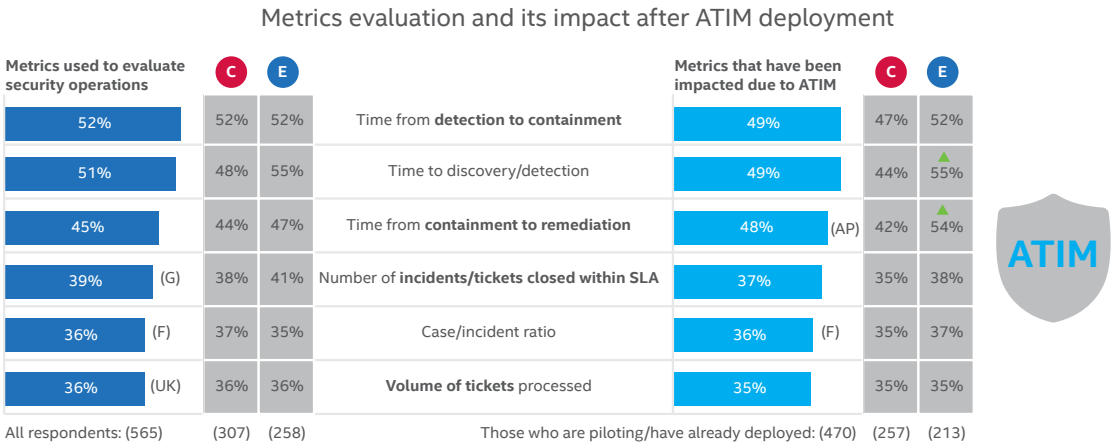

Figure 2. Intel Security research on security operations and impact following deployment of Advanced Threat and Incident Management (ATIM) tools.

The easiest time savings typically come from process integrations and increased use of workflows and automation. Whereas in the past an individual or team might work to improve their individual steps, tools, and results, you should now be looking for ways to integrate threat management overall—as a process and as a part of everyday operations. Consider your approach to threat management as a whole and identify where you can reduce the number of steps and human-driven decisions involved by integrating tools and processes. Look at where your threat management processes duplicate other operational processes and can be merged together or streamlined with other workflows.

Why integrate? Each step slows the process and may introduce error. Enabling process integrations across your IT security environment and third-party software and resources, including threat intelligence feeds, empowers your security layers to collaborate and deliver stronger protection, detection, and response.

For instance, integrated analysis helps normalize the flood of threat intelligence data to achieve true actionable intelligence. Threat and event data (i.e., who, what) couched in context (i.e., where, when) helps your analysts navigate an event stream to interpret and investigate relationships (i.e., why, how).

To close the loop, your threat management architecture should take advantage of integration with and between security countermeasures. This is the essence of the threat defense lifecycle, where information about the attack you detect and correct feeds back into your defensive controls to improve prediction and protection.

Considering integration early in the design is crucial to achieving your goals and will affect your vendor decisions. Some vendors offer open interfaces, ship pre-tested integrations, and maintain integrations at the factory. Others require you to pay for and maintain custom integrations.

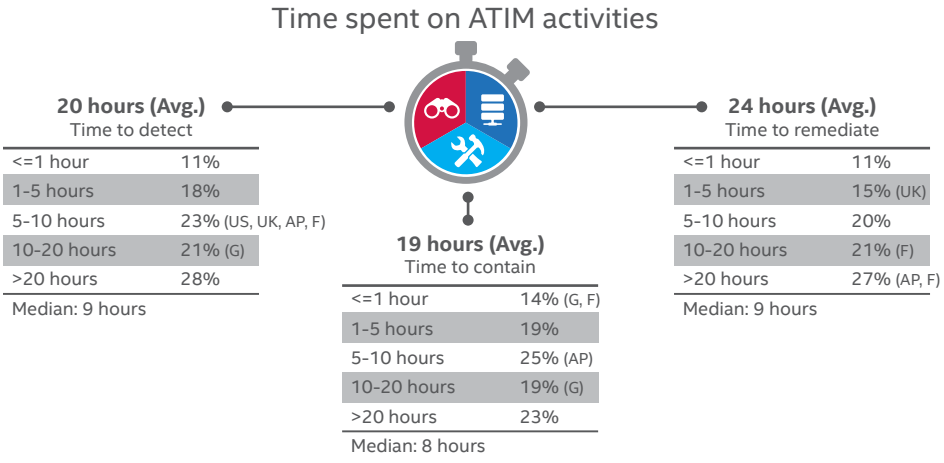

Figure 3. Intel Security research shows it takes an average of 63 hours and a median of 23 hours to move from detection through remediation.

Automate for Increased Efficiency and Accuracy

Another requirement driving your architecture should be your ability to automate. Over time, you will want to automate more tasks as a survival strategy to stretch your resources.

Given the volume of incidents and the scarcity of incident responders, CISOs and their security operations teams must find ways to be more efficient, more accurate, and more systematic about enlisting and enabling endpoint and security operational teams, surge resources, and general IT personnel with approved response actions. According to the SANS Institute,[8] 70% of organizations are drawing team members from their internal staff assigned to other functions for surge team augmentation. Since surge personnel aren't as well trained in what to do and are not security experts, they should be given a plan to guide their activities along approved paths.

Formalized processes, optimized with automation, reduce incident response times and permit less knowledgeable staff to contribute effectively. Developing and maintaining a formal incident response plan and program is a must, so that your processes and people can support your program's policies. You can update your plan and evaluate existing solutions and anticipated purchases against this plan.

Once you've enabled integrations to speed analysis, optimize with automation. Automated workflows, scripts, and tasks can translate approved processes into efficient actions. Any immediate automated response can compress your triage, scoping, and containment times—and even stop an attack in progress within seconds. An open architecture that facilitates a continuum from human-driven to full automation will provide the most organizational resilience over the long term.

Automation can begin with the low-risk tasks and assets where confidence is high. However, continuing human scrutiny makes sense for incidents that rank as a high priority against your organizational needs and policies. This risk-aware approach helps you apply resources to achieve the best result and greatest ROI for your organization.

Repeatability is critical. By using automation to replace manual effort, such as creating required case and compliance reports, you free up your personnel to do the "artisan-level" work that truly requires their talents. Breaking out your security program into routine and non-routine functions will help identify opportunities for automation. Fully- and semi-automated tasks happen in less time, with fewer errors, and can be tracked and reported against more systematically. Input quality and efficiency go hand in hand so consistently tune and evolve your detection and automation capabilities to make continued improvements that advance your security operations.

These design considerations provide the foundation to tackle evolving threats while supporting business requirements for new and secure services.

The Intel Security Optimized Security Operations Platform

Intel Security and its partners provide a wealth of strategic consulting and security infrastructure functionality to support this adaptive architecture. Foundstone Professional Services experts can help you determine the right course of action for your organization, connecting the processes, products, and data you have in place with new capabilities that suit your organizational goals and improve operational performance.

Enabling this transformation, the open security operations platform from Intel Security pre-integrates Intel Security threat management products, including McAfee Enterprise Security Manager, McAfee Advanced Threat Defense, McAfee Threat Intelligence Exchange, and McAfee Active Response, with Intel Security countermeasures.

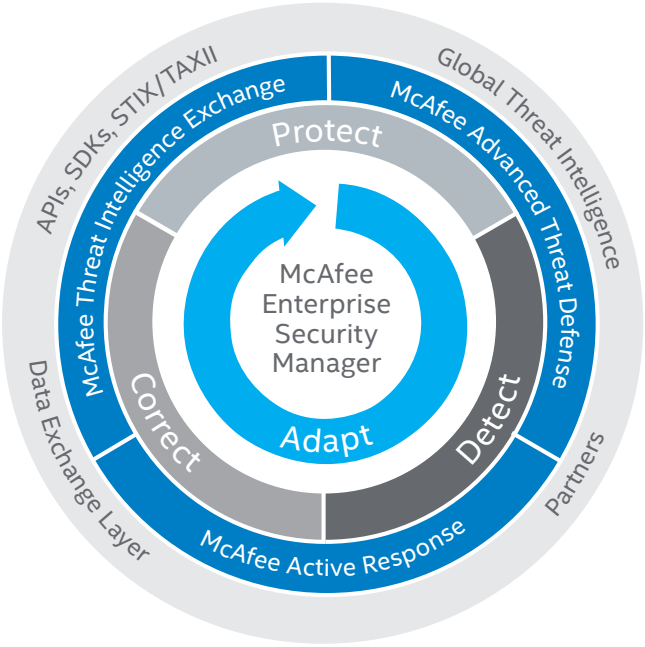

Figure 4. Integrating continuous visibility and analytics with response and remediation enhances speed and efficiency.

Since no implementation involves just one vendor, this extensible platform also integrates with over 100 certified partner products and includes more than 400 off-the-shelf connectors to security and IT software. Through open interfaces and support for standards, these capabilities can be mixed and matched with your existing tools and systems to support and extend your current strategies.

Optimized for threat management, the platform transforms real-time data and threat intelligence into accurate and prioritized insight. As the connective tissue between protection, detection, and correction, it provides visibility, workflows, and reports that nurture continuous, adaptive, and automated response.

Collect Organizational Data

Effective detection begins with collecting relevant data and then picking out the signals from the noise. The modular Intel Security platform has the capacity for high-speed ingestion of event and flow information from hundreds of sources and third-party devices. At a minimum, data can stream in from the six core log sources (Windows Events, DHCP, DNS, Proxy, SMTP, and VPN), endpoint and gateway countermeasures, applications that publish data in standard formats, as well as parser- or partner-based integrations.

Normalize and store this data according to your policies, locally for interactive analysis or archived for historical querying via big data sources like Hadoop. Data retention required for compliance and attack analysis can include raw log data storage that supports court evidence norms.

Automate First Response using Threat Intelligence

In addition to IT and security data, the Intel Security optimized security operations platform has an adaptive security architecture that lets your team make the most of any available threat intelligence. The platform provides ingestion of global threat intelligence feeds, creation of local intelligence, aggregation of low-prevalence attack data, as well as real-time sharing of threat information across your IT infrastructure. This integrated and collaborative approach minimizes the opportunity and impact of emerging attack tactics.

- If your organization is using external threat intelligence, McAfee Enterprise Security Manager (ESM) can ingest these feeds using STIX/TAXII and automatically perform remediation actions, such as endpoint quarantine and gateway blacklisting.
- To improve local intelligence about unknown and zero-day malware, McAfee Threat Intelligence Exchange (TIE) collects, manages, and shares file and application reputations in real time among controls and analysis systems. Reputation changes published over the McAfee Data Exchange Layer (DXL) can update Intel Security solutions and other McAfee DXL-integrated partner solutions, so they immediately detect a newly identified threat.
- McAfee Advanced Threat Defense (ATD) can reveal IOC content and intent in malware detected in your environment. An array of static and dynamic inspections, including sandboxing capabilities, thoroughly analyzes suspicious files from endpoints (via McAfee Threat Intelligence Exchange) and gateways, and third-party sources through RESTful APIs. This data can be ingested directly by McAfee Enterprise Security Manager and processed as any other threat feed.
- McAfee Active Response can search on endpoints for attack indicators identified by McAfee ESM or McAfee ATD, such as communication with newly uncovered command and control centers.

"Hands Free" Clean Up of Malicious Executables

One of the strengths of the Intel Security approach is the ability to clear away newly identified bad files without requiring human involvement. This process is a very low risk first response action that reduces the impact of known and emerging malware, including files masquerading as applications. McAfee Threat Intelligence Exchange integrates with Intel Security endpoint protection products and network gateways to give a second opinion. It provides an additional line of defense by maintaining a database of file reputations for unknown, suspicious files detected at an endpoint. After a new contact (post-execution), all subsequent contacts are captured. In environments with McAfee Advanced Threat Defense the file is passed along for evaluation and conviction or dismissal.

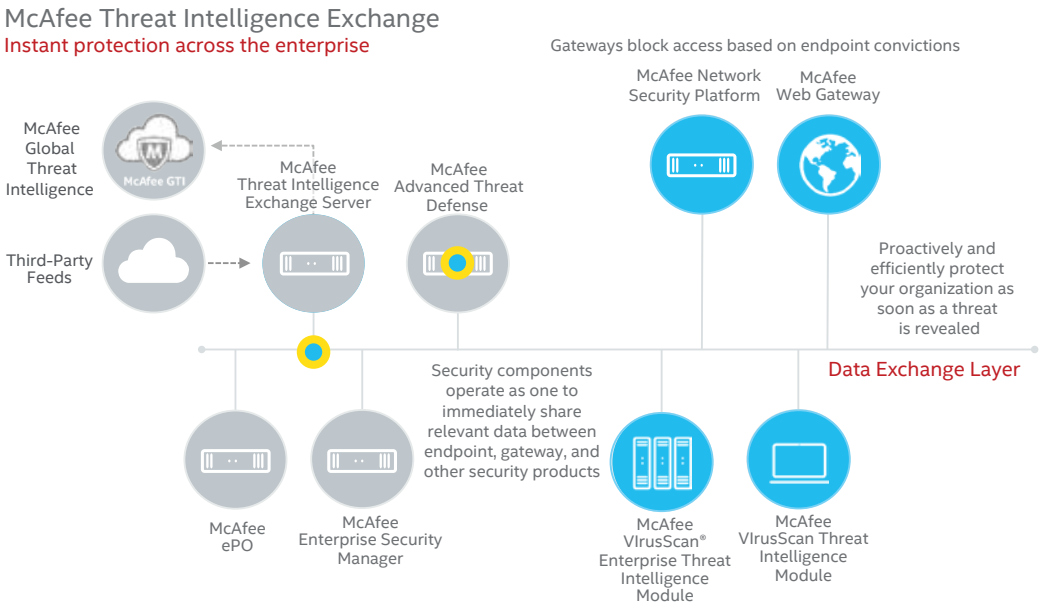

Figure 5. Integration simplicity reduces implementation and operational costs and enables unmatched operational effectiveness.

With each new verdict, McAfee Threat Intelligence Exchange distributes reputation updates to initiate immediate detection, containment, and cleanup by countermeasures, including Intel Security and partner products. While these updates happen automatically, an investigator can also see any other systems that have been in contact with the newly convicted file.

Contain the Attack

In addition to cleaning up malware, the security operations platform from Intel Security helps you automate other low-risk and high confidence containment steps to mitigate damage. Freezing the attack gives your responders breathing room to investigate the scope and take advanced remediation steps as needed. Through integrated workflows, tasks, and scripts the platform automatically takes obvious containment actions, such as quarantining an infected system or blacklisting newly discovered malicious domains, IPs, or URLs. The Security Connected framework also allows you to respond automatically to zero-day malware, coordinated through real-time information sharing from McAfee Threat Intelligence Exchange.

Pinpoint and Elevate Historic Attack Events

Intel Security can also use threat intelligence to identify system compromises and attack activities that require further investigation. Through support for STIX/TAXII formats, McAfee Enterprise Security Manager's Cyber Threat Manager receives and automatically hunts for matching events in its historical database. McAfee ESM correlates external intelligence sources against local data sets to detect past and active attack artifacts. McAfee ESM also parses the IOCs into an easily readable format displayed in the Cyber Threat Indicator dashboards. The individual components of an IOC are identified within this view, and any events that have elements of the IOC are displayed.

McAfee Enterprise Security Manager also features Backtrace, which automatically provides details of historical events corresponding to IOC data. It uses the indicator and seeks out matches with events in the past six months. The Cyber Threat Indicator dashboard displays the number of Backtrace hits and shows all of the events that contain the IOC. IOC matches help analysts identify and increase the confidence level of the most useful threat feeds. Additionally, McAfee ESM's pre-defined, advanced correlation rules can automate workflows for prioritized events, taking approved actions without delay and extra review.

For example, if an IOC contains a malicious file hash, McAfee ESM can review past events and alert if the file hash is present in an existing event. This thorough review doesn't consume new time or resources from the analyst team since it is fully automated. The analyst sees the resulting prioritized incident data and can explore a time-based sequence of events before and after the suspicious event. This attack trail can be shared with others in dashboards, alerts, and reports for further collaboration.

Triage using Behaviors, Proven Rules, and Risk Scores

While threat intelligence helps identify "known bad" indicators and events, organizations also need to hunt for indicators of attacks (IoAs). These events may not appear malicious when evaluated separately, but viewed together they represent a likely or known attack pattern. This is where enrichment, correlation, and behavior and anomaly analysis improve threat operations.

One common indicator involves reconnaissance attacks, which represent one of the most frequently seen types of alerts coming from network-based intrusion detection systems (IDS) and firewalls. Reconnaissance activities indicate that an adversary is gathering useful information about your 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 on. 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, McAfee ESM can orchestrate an automated response at the network layer, blocking future connections from the attacker.

Several options provided by Intel Security make it easier to surface and pivot around potential incidents, like reconnaissance. First, analysts can activate preconfigured McAfee ESM use case templates (content packs) that provide correlation rules, alarms, views (dashboards), workflows, and watchlists (proactive monitoring). This content is developed and tested by Intel Security experts, eliminating guesswork and ensuring the most effective and fast queries. This improves your threat analysis by prioritizing key techniques, event groups, and typical targets of an attack, including events that may not appear to be unusual on their own. For threat management, analysts might choose:

- **Reconnaissance**—Identify external scanning, sweeps, and interactions with your network and computing resources, including details on protocol use and reconnaissance events from local and remote hosts.
- **Malware**—Visualize and filter known infections, monitor trending malware (based on zones and geolocation) and malware handling workflows.
- **McAfee Threat Intelligence Exchange Content Packs**—Discover, see, and visually track McAfee TIE events to monitor infections, reputation changes, and local risk posture
- **Web Filtering**—Identify unusual levels of user and application activity and traffic to known bad or suspicious domains and IP addresses.
- **Exploits**—Detect initial and subsequent exploit event patterns that indicate compromised hosts, as well as potential exploit activity.
- **Windows Monitoring**—Gain visibility into Windows Management events that can indicate compromised hosts.
- **Firewall and Access Control List (ACL) Monitoring**—Identify and normalize firewall data to reveal abnormal traffic patterns, including top blocked and allowed ports and addresses, unusual DNS traffic, firewall events after reconnaissance events, excessive host activities, and policy changes.

- **Database Monitoring**—Used with passive monitoring to identify suspicious, malicious, and unusual database activities, such as failed and successful logon events, geolocation-based activities, bulk data transfers after exploit activity, and SQL injection activity.
- **Authentication**—Detect unusual user behavior, such as failed and successful events, that could signal compromised credentials, attempted privilege escalations, and disgruntled or malicious insiders.
- **Denial of Service**—Identify attacks that can either disrupt critical services or provide a smokescreen to permit malicious activities.
- **Data Exfiltration**—Monitor status of sensitive data locations, detect user interaction with sensitive data (e.g., who is viewing, what is being viewed, and to whom data is being distributed), and obtain rapid insight into specific user activity that can indicate potential insider threats.

Organizations can start with these content packs and refine the granularity and focus of rules, alerts, and views over time. Within these packs, rule- and risk-based correlation engines will help reveal the important events to investigate further. Ongoing updates to the content packs keep them current and relevant.

Increase Accuracy using Behavioral Analysis

Moving beyond simple rules enables higher precision in identifying meaningful events and patterns. McAfee ESM includes several methods of correlation, from simple rule-based (e.g., five login failures within 10 minutes = brute force attempt) to more complex standard deviations (e.g., service account usage increases 20% above normal baseline). Furthermore, McAfee ESM automatically performs more useful analytics by combining these two, complimentary methods of correlation. Consider the following scenario: event(s) from "Endpoint 1" indicate potential malware. Shortly after, statistical flow analysis identifies an increased volume of network traffic sourced by "Endpoint 1," which is destined for an external IP address. This combination of rule- and anomaly-based correlation can be used to detect (and potentially remediate) unwanted data exfiltration caused by a malware infection.

Investigate Freely

Once data is normalized and prioritized into actionable intelligence, organizations can move into action with greater confidence that their containment and remediation efforts are focused in the right areas. This is a race you need to win. Establish formalized incident response processes for containment and remediation and automate routine processes with your adaptive security framework. This greatly improves your ability to streamline security operations in the face of limited resources.

Content packs help you establish an efficient operational foundation that takes full advantage of best practices and automation. In addition, McAfee ESM's investigative features help you navigate incidents to scope the attack sequence and characterize the appropriate containment and mitigation actions.

Summarize weeks to years of context on demand

While some SIEM solutions are licensed on a consumption model (i.e., the more you collect and store, the more you pay), this creates an environment in which customers must choose which high-volume log sources to collect, or to filter out data perceived to be less relevant. This difficult decision constrains the data set available for investigations, which means important data is not collected or stored.

In order to provide a truly effective security analysis architecture, you must enforce the "no log left behind" approach. Forensic investigation and incident response practices require the highest fidelity of event and flow data—preserved for the longest possible time—to support detailed analytics and historical investigations. Most breach analysis tells us that detection would have been possible if the right logs had been present within a platform that was able to perform extensive analytics of event data across months, or even years. Most SIEM solutions restrict the analyst to real-time searches across 90 or 180 days of historical events, logs, and flows. To effectively identify or investigate a stealthy attack, SIEM operators cannot be restricted by the limitations of an ineffective SIEM data management architecture.

To support this historical data management requirement, McAfee Enterprise Security Manager offers highly tuned appliances that collect, process, and correlate log events from multiple years with other data streams at the speed enterprises require. McAfee Enterprise Security Manager can store billions of events and flows, keeping all information available for immediate ad hoc queries, forensics, rules validation, and compliance.

"Every security team I have spoken with is trying to do more with less, and the increasing volume of alerts and attack surface is certainly contributing to the more part. As we are inundated with security event info, we need to quickly filter that flood to focus on what is most credible and most important. Reducing time to detection and time to containment or remediation are the goals, and SIEM automation is at least part of the answer."[9]

Michael Leland, Technology Evangelist, Intel Security

Look Around and Pivot

The McAfee ESM data management architecture helps facilitate a combination of real-time investigation and historical data mining. The Cyber Threat Manager includes an interactive timeline to explore the period of an event or set of events. It lets you identify the events that led up to a compromise, for example, or events preceding or following an outbound communication to a command and control center. Users can automatically detect if the organization has already been impacted by analyzing data against a threat feed and then looking around. You can get a historical view in real-time, looking at 60 minutes, 60 days, or unlimited historical data depending on the view and your deployment.

Navigate Data with Ease

McAfee Enterprise Security Manager provides actionable dashboards that help your teams navigate incidents and drill down to investigate and take action on the right systems based on accurate and current information. In many enterprises, the security team leverages the dashboard, accessed through McAfee ePolicy Orchestrator (ePO), to drive day-to-day workflow for incident response. Beyond just detecting suspicious and risky events, the dashboard helps you interpret severity and focus on your high-value, high-risk assets. The McAfee Advanced Correlation Engine (ACE) provides event-centric risk scoring based on user or IP address history related to the event, as well as via McAfee Threat Intelligence Services, user vulnerability assessment data, and asset criticality. This array of contextual data supports computation of the individual threat asset risk score and helps you prioritize response based on if the asset is at risk to the vulnerability.

McAfee Enterprise Security Manager can tag suspicious systems based on a wide variety of criteria, enabling you to filter the dashboard to provide greater awareness of your enterprise security posture and effectively drive your remediation efforts. In addition, you can search to understand the scope of the attack, and look for things such as other compromised or affected assets, lateral motion, and historical touch points.

Remediate Effectively

With your dashboards providing actionable intelligence on the most important threats requiring action, your time to containment is critical. The Intel Security optimized security operations platform enables immediate response by integrating centralized operational systems (McAfee Enterprise Security Manager, McAfee Active Response, and McAfee ePO) and security countermeasures (endpoints, gateways, databases) with other security and IT systems.

In addition to the automated "first response" actions described earlier, responders can perform many real-time remediation tasks, run scripts to act on multiple systems, direct policy changes via McAfee ePO, run exports to a third-party case management solution, or use the case management system within McAfee ESM to get required information into the hands of operational teams.

While McAfee ESM can take action enterprise–wide, McAfee Active Response provides additional centralized tools to deeply assess and remediate endpoints. Through McAfee ePO or McAfee EMS, the administrator receives an alert that there was an active threat attempt. The team member can then use McAfee Active Response to hunt across the environment for the associated file hash. This is in less than a minute from a single pane of glass.

Any approved member of the team can remotely isolate one or more hosts, kill a process, submit malware to a sandbox, restore a file, shutdown or reboot a system, delete a backdoor, uninstall software, start a Windows service, delete a file, and clear a browser cache. These options make it straightforward to perform critical remediation actions as quickly and accurately as possible.

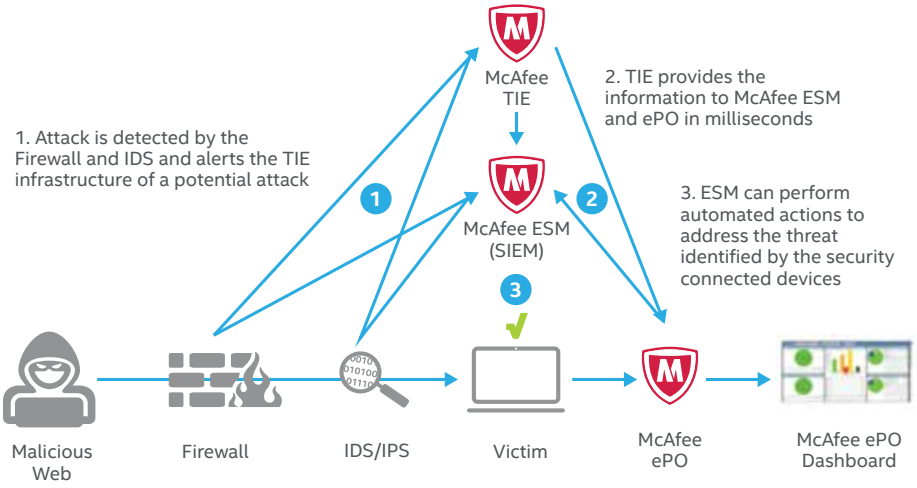

Figure 6. Security operations can benefit from integrated and automated threat management.

Continuous Monitoring and Compliance

Since organizations are under constant attack, incident response processes can no longer end with remediation and clean up—they need to feed lessons learned back into preventative controls. According to an Intel Security survey, after the CISO's office, incident responders and SOC analysts are the most likely roles to be involved with prevention.

	Prevention	Detection	Triage	Analysis	Containment	Remediation
Security Engineer/Architect (CISO office)	53% 1	48% 1	48% 1	45% 1 C	48% 1	45% 1
Incident Responder	36% 2	29% 3	24%	24%	22%	22%
SOC Analyst	33% 3	36% 2	33% 2	36% 2	27%	26% 3
Network Administrator/Engineer	25%	27%	27% 3	27% 3	31% 2	35% 2
Endpoint Administrator	21%	22%	26%	25%	28% 3	23%
Application Support/Operations	17%	22%	23%	24%	25%	25%
Contractor/Consultant/Third Party Responder	6%	7%	8%	10%	10%	15% E
Other	3%	2%	2%	2%	2%	3%

Figure 7. Intel Security research on who owns primary responsibility for each threat management scenario.[10]

The primary involvement from the CISO's office can be explained since many incidents intersect with other security, compliance, and business operations, which make decision-making, implementation, and reporting complex. For instance, it's common for an incident to involve a regulated system or sensitive data, so responders need to integrate threat-driven changes into compliance auditing and reporting practices as they upgrade technical and procedural controls to prevent recurrence.

Security operations leaders, including architects, must bring these hunting and hygiene processes together. For example, after an attack is discovered or when a regulation changes, you may need to review and adjust your enterprise policies or controls. When security researchers and vendors identify a new threat, your system should allow you to check if it has already affected your environment.

Build on Your Baseline

As you address this challenge, any original strategic baselines and assessments should provide good ideas on where to start. Most organizations have at least a checkbox level of compliance and auditability, along with ad hoc or periodic reports. Integrate underlying threat, compliance, and risk management systems to support an ongoing model of continuous monitoring and analysis. This iterative loop (i.e., the threat defense lifecycle) will help you proactively identify malicious changes, adjust your protection strategies, and improve your security posture.

Further, a strategic approach to integrated processes enables efficiency. When your discovery process is set up in advance to detect and normalize the right security, compliance, and threat data, more of the data processing and distribution can be automated and optimized. Your system even has the ability to detect attacks and worrisome trends in real time, presenting the most important information with the context needed for rapid risk recognition.

Leverage Compliance Expertise

Intel Security facilitates detection, monitoring, maintenance, auditing, and reporting of ongoing infrastructure health using McAfee Enterprise Security Manager as a foundation. To establish initial compliance and maintain checks as regulations change, Intel Security supports the Unified Compliance Framework (UCF). Integration with the UCF enables a "collect once, comply with many" methodology for meeting compliance requirements and keeping audit efforts and expense to a minimum. Beyond its extensive out-of-the-box support, all McAfee Enterprise Security Manager compliance reports, rules, and dashboards are fully customizable. This helps you facilitate executive education and internal governance priorities. By not altering the original log files, McAfee ESM supports chain of custody and non-repudiation efforts for meeting legal requirements.

As regulations change, the UCF automatically updates and pushes changes to McAfee ESM, enabling you to easily assess status and consistently report on the latest compliance requirements. This continuous compliance monitoring and reporting, as opposed to one-time audit driven compliance, is achieved via McAfee ESM's real-time collection and analysis of logs, events, and flows. Real-time compliance monitoring dashboards complement static reports and provide analysts with an instant view of the company's most up-to-date compliance posture.

For continuous visibility into changing events and their impact, threat dashboards can be integrated with compliance data to suit the needs of the user, auditor, or executive.

Deliver Visibility

McAfee ESM is designed around achieving understanding and taking action. From a dashboard view, continuous visibility, validated security intelligence, and continuous monitoring enable you to detect and prioritize threat, anomalous activity, and compliance events effectively. Views build on the fly as users drill down into events and pursue relationships. Each dashboard can be stored, or shared via email as reports. Thresholds can trigger alerts based on key events or risk items.

To help identify changes from the desired baseline, McAfee ESM offers "watchlists." Users can define specific events, values, or conditions to trigger an alarm or an action, such as an investigative workflow or case management process. Similarly, McAfee Active Response uses a trigger to monitor for events that you prioritize within endpoints. These functions serve as ongoing patrols to look for attack or risk conditions that might signal an insider threat, compliance violation, or lateral movement, as well as endpoint attack indicators such as specific hashes and registry key changes.

Since the management and reporting systems of Intel Security solutions work together from endpoint to gateway to information and event management, approved users can get access to or create specialized dashboards for their roles, accessing a consistent data set that remains up to date.

Overlaying broad visibility and continuous monitoring onto the threat defense lifecycle elevates organizational risk management from compliant to optimized. It also provides transparency to engender appropriate confidence in the organization's efforts to meet due care standards and mitigate risk.

Advantages to the Intel Security Approach

The Intel Security optimized and extensible security operations model transforms real-time data and threat intelligence, both from Intel Security and third party sources, into actionable intelligence that feeds and facilitates effective risk and threat management. Intel Security makes this possible through a combination of intelligent analytics, automation, and integration.

Integration of data—including threat intelligence as well as local and organizational data—and processes help your operational teams achieve visibility, assess threat, risk, and security posture, and prioritize and take action in near real time. At the center of the extensible security operations solution, McAfee Enterprise Security Manager supports over 400 data sources, from hundreds of types of third party security devices across an infrastructure, with APIs for bidirectional integration with endpoint, network, management, and operational systems, as well as any third party or Intel Security threat intelligence sources.

Rapid Time to Value, Sustainable Design

The security operations platform from Intel Security lets you integrate and advance your security model, pragmatically, in a modular fashion. Content packs deliver core tools, tuned rules, and views to jump-start the most common and important use cases. The solution components can also be used with off the shelf, pre-certified integrations from Intel Security and its partners, or mixed and matched using open interfaces to integrate with your existing security and IT products. This lets you take a practical approach to adoption based on your current and desired risk posture and your industry's threat profile and compliance regulations. Intel Security customers repeatedly confirm they get value in days, as compared to the longer time periods other vendors had cautioned to expect.

The modular and open design supports sustainable security to adapt with you as business, risk, threat, and compliance requirements dictate changes in controls, processes, and reporting. Sustainability is important. As attacks have become more complex and attackers more crafty and agile, no point defense solution offers long-term value any more. Point-to-point integrations get expensive fast and break down quickly. The Intel Security platform provides a conscious design for simple integration, long-term protection effectiveness, and operations efficiency. This model delivers value year in and year out, regardless of the elements in your existing environment and the changes you anticipate.

Summary

Threat management and remediation have traditionally been manual processes built on reactive, ad hoc procedures that disrupted other security and risk management functions. Intel Security enables your organization to mature its security operations and make proactive threat management an integral part of your day-to-day security operations.

Intel Security delivers an integrated, connected architecture that dramatically increases "time to" metrics: the speed and capacity of organizations to prevent and respond to external attacks and internal incidents. The Intel Security optimized security operations platform helps apply threat intelligence and bridge operational silos to reduce complexity and improve operational effectiveness. As a platform it provides integrated, adaptive, and orchestrated intelligence and response capabilities. This efficiency empowers you to take your security operations from scrambling to scale.

Learn More

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

1. **"How Collaboration Can Optimize Security Operations,"** Intel Security research, Jan. 2016.
2. **Ibid.**
3. **Ibid.**
4. **Ibid.**
5. **The 2016 SANS Incident Response Survey**
6. **"How Collaboration Can Optimize Security Operations,"** Intel Security research, Jan. 2016.
7. **Verizon 2016 Data Breach Investigations Report**
8. **The 2016 SANS Incident Response Survey**
9. "***When You're Overwhelmed With Alerts, It's Time to Automate***" Intel Security blog, March 8, 2016
10. "**How Collaboration Can Optimize Security Operations**," Intel Security research, Jan. 2016.

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

859_0716_us_wp-sustainable-security-operations