Sustainable Security Operations

Optimize processes and tools to make the most of your team's time and talent

The number and types of security incidents organizations face daily are steadily increasing, as is the cost of complying with regulations and managing policies. An unintegrated, distributed, and complex security and IT infrastructure makes it difficult to detect and act on important events. It also impairs a security administrator's ability to identify, understand, and respond to risk factors 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 four tools to get the job done.[1]

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

While dealing with incidents monopolizes much of a security operations center's resources, they are also responsible for the larger picture of risk management and compliance. To do this, they need an effective strategy with an adaptive security architecture that optimizes security operations. This approach increases efficiency through integration, automation, and orchestration. It reduces the amount of labor required, while improving your security posture. 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 involved complex techniques wielded by motivated external and internal attackers.[2]
- These techniques enabled an increase in targeted attacks from 26% to 32% between January 2015 and January 2016.[3]
- Many organizations lack adequate, let alone optimized, systems for threat management.

- Siloed detection, analysis, and investigation systems prevent the effective delivery of actionable intelligence to incident responders, who need these insights to create a precise diagnosis and accelerate containment and remediation efforts.
- Better collaboration between 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.[4]

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.

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 to help integrate threat data to keep operations and management apprised of evolving events and activities.
- Threat management linked with other systems to better manage your overall risk posture, gain continuous visibility across systems and domains, and have 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 better prepared to leverage existing resources, from talented teams and surge staffing to dashboards, case management workflows, and procedures. Beyond more efficient analysts and responders, optimized systems improve your ability to measure and report progress to interested parties, such as the board and executive leadership.

The Intel Security Optimized Security Operations Platform

Optimized for threat management, the open security operations platform from Intel Security 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. This allows your security staff to:

- **Collect organizational data—**The modular Intel Security platform quickly ingests event and flow information from hundreds of sources and third-party devices, so you can collect relevant data and then pick out the signals from the noise.
- **Automate first response using threat intelligence—**An adaptive security architecture 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. 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.
- **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. 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.

The Intel Security platform provides 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.

- **Increase accuracy using behavioral analysis—**Moving beyond simple rules enables higher precision in identifying meaningful events and patterns. The 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. Establishing formalized incident response processes for containment and remediation and automating routine processes with your adaptive security framework greatly improves your ability to streamline security operations.
- **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 and security countermeasures with other security and IT systems.

Reap the Benefits of Optimized Security Operations

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.

- Responders need to integrate threat-driven changes into compliance auditing and reporting practices as they upgrade technical and procedural controls to prevent recurrence.
- 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.
- 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 of 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

Integrating threat intelligence, local and organizational data, plus processes allows your operational teams to achieve visibility; assess threat, risk, and security posture; then prioritize and take action in near real time. At the center of the extensible security operations solution, McAfee Enterprise Security Manager supports over 400 third party security devices with APIs for bidirectional integration with endpoint, network, management, and operational systems, as well as third-party or Intel Security threat intelligence sources.

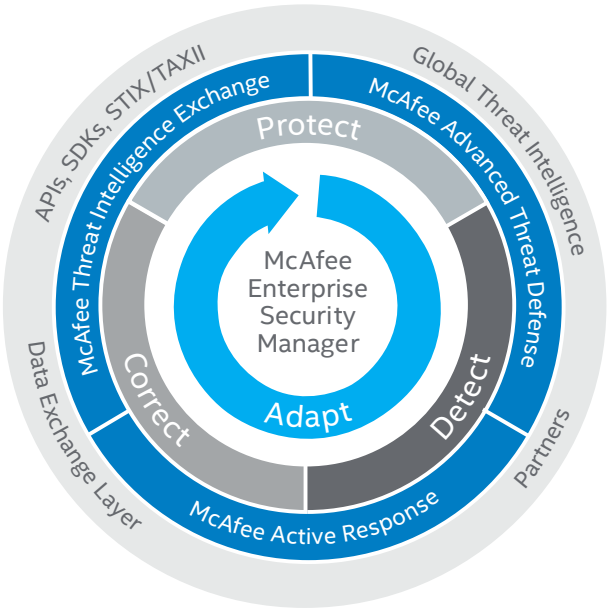

Figure 1. Integrating continuous visibility and analytics with response and remediation enhances speed and efficiency.

Rapid Time to Value, Sustainable Design

The modular security operations platform from Intel Security provides solution components that can scale to meet growing needs. The open design gives you the flexibility to use off the shelf, pre-certified integrations from Intel Security and its partners, or mix and match solutions using open interfaces to integrate with your existing security and IT products.

This lets you take a practical approach to adoption based on 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 them to expect.

Today, 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 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.

Intel Security provides an integrated, connected architecture that dramatically increases the speed and capacity to prevent and respond to external attacks and internal incidents. The optimized security operations platform helps reduce complexity and improve operational effectiveness by providing integrated, adaptive, and orchestrated intelligence and response capabilities. This efficiency empowers you to take your security operations from reactive to proactive.

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.

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