3 Ways to Align Your SecOps and Business Priorities Using Cisco Endpoint Security

Executive Summary

Long remediation cycles are top of mind for many organizations. Security managers and practitioners are making strides, and detection times have been improving. Yet the majority of security pros still feel that threat actors have the upper hand[1].

This sentiment is not surprising. While time to detection is decreasing, it doesn’t necessarily translate into a shorter remediation cycle. There’s a disconnect between how fast security teams are detecting threats and how fast they can eradicate them.

Increased efficiency, better actionable insights, and a bigger focus on proactive security can help improve security operations (SecOps) effectiveness and reduce time to remediation. These objectives are shared between security practitioners and business operations, even though the results are measured differently.

As both security managers and technologists are tasked to do more with less, the question becomes: How can they leverage the same tools to meet both the business and the operational goals?

This paper explores how you can achieve both business and operations objectives with endpoint security from Cisco. Learn how you can expand visibility to further decrease time to detection and remediation, improve your SecOps efficiencies and effectiveness, and become more proactive against the riskiest threats to your business.

The Struggle Behind Long Remediation Cycles

A 2018 incident response survey by SANS[2] showed an increase in the number of organizations detecting incidents within 24 hours, along with a general move to shorter detection. However, despite 53% of organizations detecting incidents within 24 hours, 61% took two or more days to remediate.

A long remediation cycle doesn't just affect your security team's time and resources. It increases the likelihood of an incident turning into a data or systems breach.

Containing a breach in fewer than 30 days could save you more than $1 million[3]. No small change, even for a large enterprise. The longer your time to remediate, the bigger the hit on your bottom line.

Cisco noted a new trend for 2019: an increased focus on mean time to remediate and a decreased focus on mean time to detect as a key performance indicator (KPI) that CISOs use to measure cybersecurity effectiveness. In our 2019 CISO Benchmark Report[4], 48% of respondents indicated they used mean time to remediate as a KPI, compared to 30% in the 2018 study. At the same time, the number of respondents using mean time to detection as a metric dropped from 61% in 2018 to 51% in 2019.

Improving this KPI is imperative both for the C-level stakeholders including the CISO (business side) and the practitioner (operations side). Yet both camps grapple with issues like shortage of security talent, high number of alerts and false positives, and lack of insights into what's happening across their environment.

To break this cycle, you don't need more tools – you need automated and integrated technologies that give you economies of scale and help solve both the business and the operational challenges.

Business vs. Operations Objectives

BUSINESS

- Combating the most critical threats.
- Lowering risks of financial loss, data breaches, and business disruption.
- Reducing impact of security risks on the bottom line.

OPERATIONS

- Identifying the most critical threats.
- Defending against threats without extra overhead.
- Simplifying complexity of security defenses.

Decreasing Time to Remediation

Responding to Threats more Efficiently

Getting Economies of Scale

Two Sides of the Same Coin

"Are we protected?" "How quickly can we contain threats?" Those are the questions that keep CISOs up at night. Without the luxury of "protection at any cost," the next question is, are they giving their security teams the best tools to protect the business assets and to contain incidents with less time, money, and other resources?

But security practitioners don't want yet another tool that will generate more alerts. Especially since 74% percent of organizations struggle with the talent shortage, and 66% of those that have this struggle increase the workload on existing staff[1].

The existing staff, however, is already overwhelmed – and with an average of more than 5,000 alerts every 24 hours[5], who wouldn't be? Worse still, according to the CISO Benchmark Report, 41% of organizations get more than 10,000 security alerts daily.

While the challenges and priorities of the two camps seem different, they're closely related.

Aligning their objectives can be achieved by:

- Getting better and faster insights into your environment and security posture
- Improving efficiency and effectiveness of security operations and management
- Enhancing proactive tactics that eliminate threats

Getting Better Insights

One of the biggest challenges for incident responders is scoping a malware infection – figuring out where it's been and where it currently resides. Visibility is a common struggle, and endpoint data historically has been the hardest to collect. At the same time, endpoints come in second among the types of systems most commonly involved in a data breach[2].

Only 35% of the CISOs in our benchmark report said it's easy to determine the scope of a compromise, as well as contain it and remediate exploits. Yet without proper scoping, you can't be certain that you've completely removed a threat actor.

In the SANS survey, 26% of incident responders said their organization has been breached multiple times by the same actors using the same tactics, techniques, and procedures (TTPs). This leaves the welcome mat for attackers to come back.

During an attack, threat actors often breach multiple points of entry, dropping payloads that exhibit different behaviors and that don't track back to the same source location. This keeps the threat in stealth mode and difficult to detect. Even if you stomp out the infection in one location, it's easy to miss it somewhere else in your environment.

With Cisco AMP for Endpoints, you can perform in-depth search for information that other tools collect across the environment, so you can confirm whether that data directly relates to the attack. These insights improve your scoping and significantly reduce remediation time.

Cisco AMP for Endpoints also enables you to perform advanced search – on a schedule, or on-demand – for any data across the entire environment using SQL and treating each endpoint as a database to be queried. The query engine enables you to search on one, many, or all endpoints for forensic information, malware artifacts, and other data.

With increased automated actions capability, AMP for Endpoints boosts your security investigation efforts by allowing you to quickly execute a query, based on triggers such as detection of indicators of compromise.

Other AMP for Endpoints capabilities that provide actionable insights include:

Continuous monitoring and retrospective detection

Continuous analysis beyond the event horizon retrospectively protects against malware that evades initial defenses. As new threat information becomes available and a file is identified as malicious, AMP for Endpoints automatically quarantines the file and alerts you about the malicious behavior.

Using the file trajectory feature, you can see the file's lifespan across all endpoints, including malware movement from the initial infected host to other devices. Another feature, device trajectory, shows you how hosts interact with files, including an event timeline. Together, they give you a complete timeline and scope of the threat.

Integrated threat intelligence

AMP for Endpoints automatically receives actionable intelligence from past and newly discovered threats from across the globe, provided from sources such as Talos, Threat Grid, and Umbrella, as well as from outside parties like VirusTotal.

Our Cisco Talos Intelligence Group is comprised of more than 300 researchers who collect telemetry from 94 million AMP-enabled sources, 600 billion emails, and thousands of honeypots and sensors; and they analyze 2 million malware samples and tens of billions of DNS requests daily. To rapidly distill these massive volumes of data into actionable insights, Talos uses supervised and unsupervised machine learning that's overseen by data scientists and analysts.

The result of the multisource data is deeply contextual threat intelligence that is automatically applied to your environment. And because we see more threats, we block more.

Machine learning

AMP for Endpoints is trained by algorithms to "learn" to identify malicious files and activity based on the attributes of known malware. Machine learning capabilities in AMP for Endpoints are fed by the comprehensive data set of Cisco Talos™ to ensure a better, more accurate model. Together, the machine learning in AMP for Endpoints can help detect never-before-seen malware at the point of entry.

Through machine learning and artificial intelligence, AMP for Endpoints uses an agentless web proxy to identify command-and-control traffic, data exfiltration, and possibly unwanted applications operating on the endpoint. The agentless feature also provides administrators visibility into any internet-connected device that can't have a traditional endpoint security agent.

Improving Efficiency and Effectiveness

Alert fatigue is old news, except that this topic still comes up consistently. In the quest to build up layered defenses, organizations have ended up with a kitchen-sink array of tools, and both CISOs and practitioners are weary of the results: an endless number of alerts to sift through.

The sheer number is overwhelming, but correlating the data to understand the whole story is even more difficult. Nearly 80% of CISOs in our benchmarking survey told us that alert orchestration from multiple vendors remains a challenge. Likewise, 66% of IT and security practitioners surveyed by the Enterprise Strategy Group found threat detection and response challenging because of multiple independent point tools, while 64% called out the high number of manual processes[6].

Part of the inefficiency stems from the difficulty of quickly getting the answers you need – how do you prioritize incident response? If you could identify which assets are the most exposed, you could remediate those threats first.

Let's say you've learned about a new critical threat, and you're trying to determine which endpoints have a piece of legacy software with a specific CVE (Common Vulnerabilities and Exposures) entry. Typical endpoint solutions can identify which endpoints have that outdated app when it's been launched. But what happens if the software hasn't run on an endpoint in some time?

With the ability of AMP for Endpoints to perform advanced search, you can query all endpoints across the entire environment for the SHA-256 hash executable. Regardless of when the application ran last, if at all, you can identify all the endpoints where it resides and create a report. If the vulnerability is critical, you can choose to isolate those endpoints from the network and mitigate the weakness before attackers can exploit it.

Other Cisco Endpoint Security capabilities that make your security operations more efficient include:

Automated workflows

Conducting threat hunting and security investigations require many repetitive, tedious tasks. This slows down the workflow while giving a threat actor more time to cause damage. Automation can make these crucial processes more efficient and effective.

One example is retrospective analysis, which automatically quarantines a malicious file that originally presented itself as benign. Net-new, unknown threats don't get blocked when they first enter the environment, but AMP for Endpoints tracks and monitors the file and its behavior. When new threat intelligence indicates the file is malicious, the retrospective feature doesn't wait for a human to discover it – it quickly blocks the file while triggering an alert so you can review the incident and mitigate it.

Endpoint isolation

Even when you have visibility into your environment, removing a threat and remediating a compromised endpoint takes time. This leaves a wider window for a threat to escalate while increasing your remediation time and consequently, your costs. Endpoint isolation enables you to quickly block incoming and outgoing network activity, eliminating the risk of an infection spreading across your network.

During isolation, which can be triggered manually or automatically via APIs, you can maintain complete visibility into the endpoint through the cloud, as well as allow IP address whitelisting. Once you've mitigated the threat, you can quickly enable the healthy endpoint to rejoin the network.

Integrated security architecture

When doing more with less is both the business and operations mandate, how can you achieve economies of scale? With Cisco's integrated security architecture, you only have to see a threat once in your environment, and it's blocked everywhere. This saves you a tremendous amount of time, shortening your remediation timeline and shrinking costs.

AMP for Endpoints integrates with various Cisco security components on the back end while its integration with Cisco Threat Response provides a user interface (UI) for the front end. The Cisco Threat Response UI correlates data collected from the network, email, and the web to provide a comprehensive view of a threat. It enables analysts to enrich their investigations with local context and relevant endpoint events, as well as perform advanced custom detections.

Focusing on Proactive Tactics to Eliminate Threats

Like the old military-combat adage says, best defense is a good offense. When you engage with the adversary lurking inside your endpoints, rather than waiting for an event alert, you can contain a threat before it wreaks havoc. That's where threat hunting comes in, enabling your proactive defense.

When done right, threat hunting reduces the overall burden on security teams by minimizing the number and scope of their incident response activities. Proactive security also helps alleviate some of the alert fatigue that plagues most security teams.

More organizations are using threat hunting as a tool for reducing dwell time. According to a 2018 SANS threat hunting survey[7], 43% of respondents performed continuous threat hunting, compared to 35% the year before. Gartner estimates that by 2022, 50% of all security operations centers (SOCs) "will transform into modern SOCs with integrated incident response, threat intelligence, and threat hunting capabilities," which is an increase from under 10% in 2015[8].

While threat hunting is a human-driven activity, the right tools give you the ability to shift from a reactive to a proactive approach. However, that doesn't necessarily mean investing into yet another solution – AMP for Endpoints has built-in threat hunting capabilities.

Lack of staff with more advanced skill sets is often a barrier to implementing a threat hunting program. Using advanced search capabilities simplify some of the investigation steps, enabling you to get economies of scale by assigning the simpler tasks to junior level staff.

For example, we found that 90% of incidents are related to malware[4], so you may be trying to identify malware beaconing behavior in your environment. Once you know which endpoints are associated with the beacon you're tracking, you can create live queries to track the files associated with the beginning of the behavior and where that file came from.

Improve Efficiency, Add More Layers of Context Via Integrated Architecture

When you're trying to make your SecOps more efficient and effective, the problem of siloed point products is a difficult one to solve. And the sheer volume of alerts and false positives, along with the juggling of multiple consoles, are not necessarily the biggest concern. A more important one is the gap that these disparate products leave by giving you only slices of your security posture.

The true value of an integrated security architecture comes from having the complete security story across your environment. An integrated workflow doesn't just eliminate endless manual processes and save you hours of investigation and remediation work – it also gives you deeper context while sharing the latest threat intelligence among the integrated technologies. You're creating a security ecosystem that can respond automatically and systematically to advanced threats, so you can lower overall risk by closing the gaps, and also make your SecOps team's lives easier by empowering them to defend against threats faster.

Context is paramount during incident response because standalone pieces of data only help you identify a threat. They don't help you answer questions such as what type of attack you're dealing with, how sophisticated it is, what the attackers' objectives are, was the target remediated, and so on.

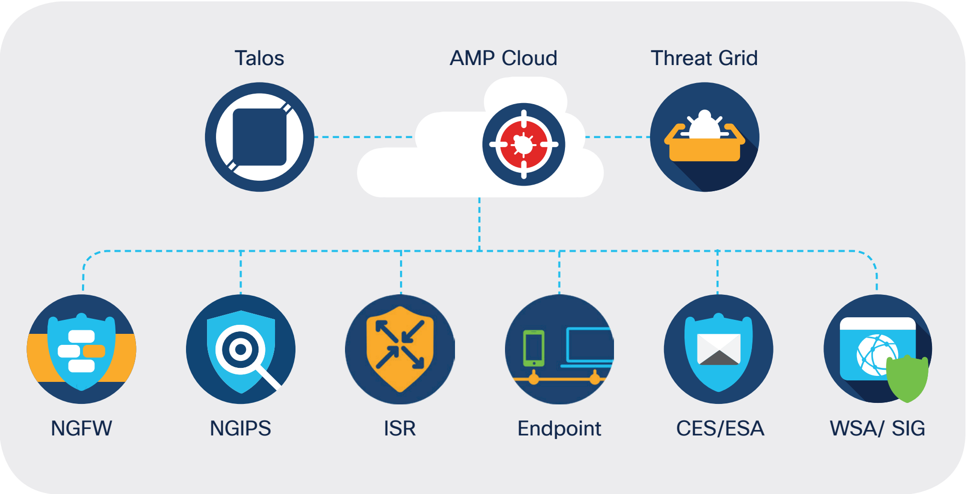
Without context, isolated events don't have much meaning and only add to alert fatigue, while data enrichment from correlating multiple sources reduces the scope of your investigation so you can focus faster on the real threat. Cisco Threat Response brings together data from across the architecture into one console. It gives you a data-enrichment tool for a more comprehensive story across multiple vectors.

Security that Works Together

See once, block everywhere

Investigate and respond to threats across network, web, email and endpoints

Drive zero-trust for organizations with SecOps journey well underway



Sources

1. "The Life and Times of Cybersecurity Professionals 2018," ESG/ISSA
2. "Results of the 2018 Incident Response Survey," SANS
3. "2018 Cost of a Data Breach Study," IBM/Ponemon Institute
4. "Anticipating the Unknowns: CISO Benchmark Study," Cisco (2019)
5. "24 hours in security," Cisco (2017)
6. "Threat Detection and Response Landscape," ESG Report (2019)
7. "SANS Threat Hunting Survey Results," SANS (2018)
8. "Gartner Top 7 Security and Risk Trends 2019," Gartner

Final Thoughts

Meeting both the business and SecOps goals without additional resources is possible. Defending against evolving threats is a complicated responsibility, but you can reduce the complexity and increase efficiency with advanced solutions that are designed to solve today's complicated security challenges.

Cisco's comprehensive security portfolio amplifies your security team's abilities to defend your organization against the riskiest threats. It enables both CISOs and SecOps to do more with less while improving your security posture – and your bottom line.