COMPREHENSIVE GUIDE TO SECURITY OPERATIONS

How to minimize risk and continuously improve your security posture

Foreword by Mark Manglicmot

ARCTIC WOLF

About Arctic Wolf

Arctic Wolf® is the market leader in security operations. Using the cloud-native Arctic Wolf® Platform, highly trained Concierge Security® experts work as an extension of your team to help end cyber risk. We make it fast and easy for organizations of any size to stand up world-class security operations that continually guard against attacks in an efficient and sustainable way.

For more information about Arctic Wolf, visit arcticwolf.com.

COMPREHENSIVE GUIDE TO SECURITY OPERATIONS

How to minimize risk
and continuously improve
your security posture

Crystal Bedell

Foreword by Mark Manglicmot

CYBEREDGE
PRESS

Comprehensive Guide to Security Operations

Published by:
CyberEdge Group, LLC
1997 Annapolis Exchange Parkway
Suite 300
Annapolis, MD 21401
(800) 327-8711
www.cyber-edge.com

LIMIT OF LIABILITY/DISCLAIMER OF WARRANTY: THE PUBLISHER AND THE AUTHOR MAKE NO REPRESENTATIONS OR WARRANTIES WITH RESPECT TO THE ACCURACY OR COMPLETENESS OF THE CONTENTS OF THIS WORK AND SPECIFICALLY DISCLAIM ALL WARRANTIES, INCLUDING WITHOUT LIMITATION WARRANTIES OF FITNESS FOR A PARTICULAR PURPOSE. THE ADVICE AND STRATEGIES CONTAINED HEREIN MAY NOT BE SUITABLE FOR EVERY SITUATION. NEITHER THE PUBLISHER NOR THE AUTHOR SHALL BE LIABLE FOR DAMAGES ARISING HEREFROM. THE FACT THAT AN ORGANIZATION OR WEBSITE IS REFERRED TO IN THIS WORK AS A CITATION AND/OR A POTENTIAL SOURCE OF FURTHER INFORMATION DOES NOT MEAN THAT THE AUTHOR OR THE PUBLISHER ENDORSES THE INFORMATION THE ORGANIZATION OR WEBSITE MAY PROVIDE OR RECOMMENDATIONS IT MAY MAKE. FURTHER, READERS SHOULD BE AWARE THAT INTERNET WEBSITES LISTED IN THIS WORK MAY HAVE CHANGED OR DISAPPEARED BETWEEN WHEN THIS WORK WAS WRITTEN AND WHEN IT IS READ.

For general information on CyberEdge Group research and marketing consulting services, or to create a custom *Definitive Guide* book for your organization, contact our sales department at 800-327-8711 or info@cyber-edge.com.

ISBN: 978-1-948939-29-4 (Paperback)
ISBN: 978-1-948939-30-0 (eBook)

Printed in the United States of America.

10 9 8 7 6 5 4 3 2 1

Publisher's Acknowledgements

CyberEdge Group thanks the following individuals for their respective contributions:

Editor: Susan Shuttleworth
Graphic Design: Debbi Stocco
Arctic Wolf Contributors: Mark Manglicmot and Con Mallon

Table of Contents

Foreword v

Introduction vii

Chapters at a Glance vii

Helpful Icons viii

Chapter 1: What Do We Mean by Cyber Risk? 1

A Tale of Two Companies 1

Chapter 2: What Do We Mean by Security Operations? 5

The Need for Security Operations 6

Chapter 3: How Security Operations Can Reduce the Likelihood of a Cyber Incident 11

Know Thyself 11

Gather Threat Intelligence 13

Vulnerability Management 14

Human Security 15

The "Care and Feeding" of Your Security Team 16

Chapter 4: How Security Operations Can Reduce the Business Impact of a Cyberattack 17

Right of Boom 17

Leverage Strategic Guidance 19

Chapter 5: Achieving World-class Security Operations 21

What It Takes to Implement Security Operations 21

Options for Obtaining Security Operations 25

But Where Do We Start? 29

Chapter 6: 10 Requirements for Choosing a Security Operations Partner 31

Breadth of Service Offerings 31

Security Operations Platform 32

Dedicated Team 33

No Noise 34

Organizational Understanding 34

Value 34

24x7 Monitoring 34
Comprehensive and Centralized View of Security Posture 35
More than Technology 35
Flexibility 36
Bonus: Cultural Fit 36

Foreword

An employee clicked a malicious link in a phishing email and an attacker, armed with ransomware, breaks into your enterprise. It's 5:30 a.m. Do you trust that your enterprise and security team are resilient enough to fight the attack without significantly impacting the business?

Resiliency, in this case, means detecting the attack with well-configured tools across endpoints, the network, and cloud working in harmony to raise the right alarms. It means having skilled security engineers on duty at 5:30 a.m. to quickly grab and investigate the alert. They have the know-how and business buy-in to act independently to remove or contain the first workstation from the network, plus revoke and reset the user permissions for the tricked employee. All these steps must happen in minutes to successfully fight the attack.

Finally, the security team needs the time and context to holistically fix the defenses that led to this minor breach versus playing whack-a-mole, system by system.

This is a very common scenario, but it's difficult to get it right every single time. Attackers only have to get it right once. Defenders must be right every single time.

Cybersecurity operations is built on trust. Trust that the best-of-breed tools have been acquired, installed, patched, and configured correctly to maximize their investment. Trust that the security operations team is at the console and ready to respond when the attack alarm is sounded. Trust that the processes established have been sufficiently tested and work when needed. Trust that employees recognize and don't fall for the common tricks used to lure them into opening a crack in your defenses.

This trust is established over time via successes and continuous improvement. It's established by taking a team approach to security, leveraging trusted external partners and industry expertise. Amateurs go it alone. Professionals are part of a team with coaches and advisors.

In cybersecurity operations, trust is not enough. You additionally need verification, repeatedly, that all those defenses are still effective. This verification needs to be benchmarked against an accepted framework with external assistance for the most critical areas.

Security operations is hard to get right. This book is designed to help organizations moving deeper into security understand the common pitfalls and lessons learned. For larger organizations that have been at this for a while, the value is in the verification that your program is still on track. Attackers continually evolve their tactics, so enterprises must continually evolve their defenses.

The responsibility entrusted in security operations leaders is immense. From the first documented incident response case study by Clifford Stoll in "*The Cuckoo's Egg*," the key has been to have a good foundation of current technologies, optimized processes, and skilled professionals with a detective personality. An operations mindset versus a tools-first mindset has proven to be the most effective way to keep pace with adversaries.

While the task at hand may seem daunting, try to remember that when all the pieces of a well-tuned security operations function are in place, security operations will add trust in the business' resilience of a 5:30 a.m. attack at the highest levels of the organization and even be fun for the team striving to end cyber risk.

Mark Manglicmot
Vice President, Security Services
Arctic Wolf

Introduction

The more things change, the more they stay the same.

Nowhere is that truer than in cybersecurity. Every year it's the same story: enterprise security budgets are increasing, security vendors are selling more tools, and cyberattacks… well, they continue to increase in number and severity despite the cybersecurity industry's best efforts.

This book sets out to change all that, once and for all, by giving you a framework for implementing a security operations function. Security operations can be thought of as all the pieces of a security framework working in concert to effectively reduce risk to a negligible level. That's right. Effective security operations will help you arrive at a place where you finally feel in control – and that starts to feel like an end to your cyber risk.

We don't blame you if that sounds too good to be true – especially after all the effort you've put into your security program to date. The way we see it, you have two options: continue throwing more money and technology at the problem to get the same results or try a different approach for a different outcome. Join us on a journey to end cyber risk. You'll be glad you did.

Chapters at a Glance

Chapter 1, "What Do We Mean by Cyber Risk," explains why a company can spend hundreds of thousands of dollars on security and still succumb to an attack.

Chapter 2, "What Do We Mean by Security Operations?" reviews the critical components that comprise an effective security operations function.

Chapter 3, "How Security Operations Can Reduce the Likelihood of a Cyber Incident," outlines how security operations lowers the risk of being an attack target.

Chapter 4, "How Security Operations Can Reduce the Business Impact of a Cyberattack," describes how security operations minimize the business risk of an attack.

Chapter 5, "Achieving World-class Security Operations," explores how companies can implement their own security operations to eliminate cyber risk.

Chapter 6, "10 Requirements for Choosing a Security Partner," examines the importance of cultural fit, a dedicated team, and other factors when choosing a partner.

Helpful Icons

TIP

Tips provide practical advice that you can apply in your own organization.

DON'T FORGET

When you see this icon, take note as the related content contains key information that you won't want to forget.

CAUTION

Proceed with caution because if you don't it may prove costly to you and your organization.

TECH TALK

Content associated with this icon is more technical in nature and is intended for IT practitioners.

ON THE WEB

Want to learn more? Follow the corresponding URL to discover additional content available on the Web.

Chapter 1

What Do We Mean by Cyber Risk?

In this chapter

- Learn how the cybersecurity market is growing
- Understand the formula for risk
- Read how two companies hit by the same ransomware can have radically different experiences

Every year, companies spend hundreds of thousands of dollars on cybersecurity tools in the hopes of reducing the risk of a security breach. And yet every year brings new breach headlines, even though these unfortunate companies had their fair share of cybersecurity tools. What did they miss? And how did they miss it? In this chapter, we look at how proper preparation can reduce the likelihood of threat actors' getting into the enterprise and lessen the impact of a cyberattack.

A Tale of Two Companies

There's a lot more involved in how well you'll weather a cyberattack than how much you've spent on cybersecurity tools. It all comes down to risk.

DON'T FORGET

In cybersecurity, risk is defined using a commonly accepted formula: Risk = probability x impact

In other words, cyber risk is the likelihood of an incident occurring, multiplied by the impact on the business. If either the probability or the impact is zero, then there's no cyber risk and you can sleep easy knowing that you're safe and secure. But we know that's rarely the case. In reality, there is an entire spectrum of cyber risk, and the risk profile of different organizations falls somewhere along that continuum.

To help illustrate this concept, let's look at how two companies experience a ransomware attack. For this scenario, let's imagine that Company A and Company B are competitors. They are similar in many ways except for one major difference: their risk profile.

Company A: High risk profile

Company A is hit with a ransomware attack. The company can't access any of its networked resources. The business is completely inoperable.

The company calls up a security response team to help them recover. When the team arrives, they ask for a list of assets. Company A, however, doesn't have asset identification or asset management processes in place. No one knows what assets are on the network, the number of endpoints the organization has, or what servers are critical. They don't even know where services and data files are stored.

The lack of information makes finding the initial point of impact extremely challenging. The security response team works nearly 48 continuous hours to determine root cause. Delaying remediation by nearly two full days costs the company almost $600,000 in employee downtime and another $1.2 million in lost production. The only business decision is to pay the ransom or disconnect from the ISP and hope to be back online sooner than later.

Company B: Low risk profile

Company B is hit by the same strain of ransomware as Company A, but the impact on Company B's operations and recovery experience are radically different. At Company B, a frantic user calls the help desk to report that they've been locked out of their machine. After a quick call between IT and the security operations center (SOC), a member of IT gives the 'All clear,' and the user is back to business as usual in a matter of minutes. That's it. End of story. Or is it?

So, how do Company A and B differ? It's not just one thing, but a host of things, as you can see in Figure 1-1.

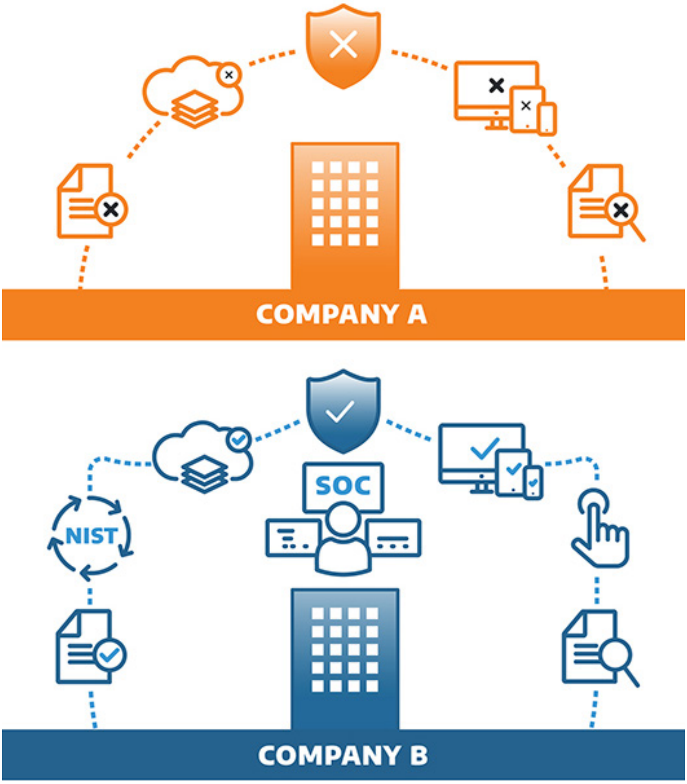


Figure 1-1: Company B has the people, technologies, and processes in place to mitigate the risk and impact of an attack.

Unlike Company A, Company B has made an effort to understand and secure its IT environment. To begin with, the company has a process for inventorying and managing its assets. It knows what types of devices are on the network, the quantity of those devices, and which ones are considered critical.

Company B's SOC has also implemented security controls and best practices according to the National Institute of Standards and Technology (NIST) Cybersecurity Framework. Company B ensures that these controls are implemented properly, the network is architected correctly, and all known attack vectors are addressed. For example, data is secured not just in transit but also at rest.

TIP

Company B's backup policy includes both hot and cold storage backups. The hot backup is easily accessible while the cold storage backup is completely removed from the network to ensure its protection. If the hot backup becomes compromised, the company can recover the data using the cold storage backup.

Security awareness training is also a key component of Company B's cybersecurity strategy. The organization understands that all its investments in technology are of little help if end users don't think twice before responding to a phishing email.

Finally, Company B has a documented incident response plan that includes a contact list with assigned duties so that when an attack happens – and it does – everyone in the organization knows how to respond to lessen the impact.

After an attack, Company B performs a post-incident analysis. The goal of this exercise is to review lessons learned and determine what they need to do differently to prevent the attack from recurring. The organization determines how the attack occurred and fills the gaps in its security posture to build resilience and ensure that it doesn't happen again.

Company A and B are similar companies hit by the same ransomware, but with very different outcomes. In the next chapter, we'll look at the role security operations played in determining those outcomes.

Chapter 2

What Do We Mean by Security Operations?

In this chapter

- Learn who needs security operations
- Understand why security operations is necessary to end risk
- Explore the security journey

The amount of work Company B put into reducing the risk and impact of a security breach may seem overwhelming. For a lot of security teams, staying up to date on the newest security technologies and best practices while also staying ahead of the latest cyberthreats and attack vectors is an ongoing endurance test with no end in sight. Others, like those at Company A, don't know where to even begin. However, the lack of security operations can lead to devastating consequences. A breached company can spend hundreds of thousands of dollars on incident response and regulatory fines alone, never mind the cost of implementing the tools, people, and processes – the security operations – required to reduce the risk of a future attack.

The good news is, when done well, security operations can do much more than simply reduce the risk and impact of an attack. It can be part of your ultimate journey towards ending cyber risk. So please stick with us, and by the end of the book it will all be clear. For now, let's dig into what we mean by security operations.

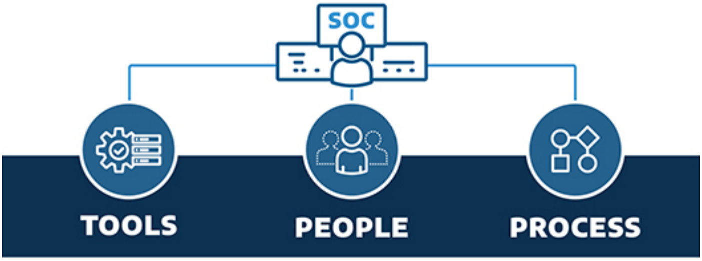


Figure 2-1: Security operations consists of tools, people, and processes working in harmony.

The Need for Security Operations

To finally solve the effectiveness problem in cybersecurity, organizations need a solution that combines technology with human expertise and delivers it in a way that addresses day-to-day security needs while ensuring that the overall security posture gets stronger over time. The security industry's growing acceptance of this strategy has led to the emergence of security operations as its own discipline that aims to reduce the likelihood and impact of a breach and end cyber risk.

DON'T FORGET

As shown in Figure 2-1, *security operations* is the harmonious utilization of people, technology, and processes with the goal of reducing the likelihood and impact of cyberthreats by strengthening the overall security resiliency of an organization.

A security operations framework

Building security operations that strategically and tactically addresses likelihood and impact requirements can be overwhelming. It's best to have a point of reference to guide you along the way. We stand by the NIST Cybersecurity Framework, which provides the structure to build and run security operations. The framework, illustrated in Figure 2-2, includes the following five functions:

☑ The **identify** function entails identifying physical and software assets within your organization, as well as the threats and vulnerabilities to both internal and external resources. The outcome from this effort is an accurate understanding of your threat posture across all your attack surfaces.

☑ The **protect** function supports the ability to limit or contain the impact of a potential cybersecurity event. Examples include implementing access controls, patching systems in a timely manner, and conducting security awareness training.

☑ The **detect** function defines the appropriate activities to identify the occurrence of a cybersecurity event. They include implementing continuous security monitoring to ensure anomalies and events are detected and their potential impact is understood. The outcome from these efforts is the ability to spot all threats (both known and advanced persistent threats), and to do so quickly.

☑ The **respond** function supports the ability to contain the impact of a potential cybersecurity incident. Examples include activities that prevent the expansion of an attack, mitigate its effects, and resolve the incident. The result from these efforts is the ability to respond to threats both quickly and efficiently, thereby minimizing their impact and damage to your organization.

☑ The **recover** function is focused on implementing improvements based on lessons learned after an incident and reviews of existing strategies. The goal is to return to business fast and learn from mistakes so you can avoid them repeating in the future.

The tactical components

A security operations function leverages a number of tactical components including broad visibility, 24x7 coverage, and access to expertise. These tactical components largely address the day-by-day security tasks involved with threat detection and remediation. We will explore them in more depth in Chapters 4 and 5.

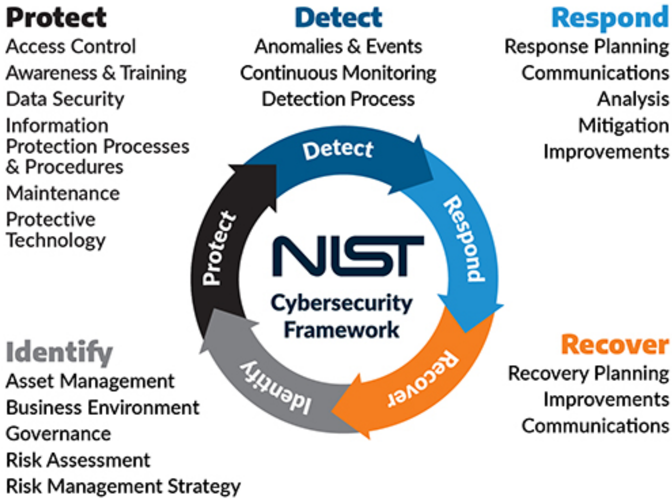


Figure 2-2: The NIST Cybersecurity Framework provides the structure to build and run security operations.

The strategic components

Equally important to ending risk are the strategic components of a security operations function. These include strategic guidance and continuous improvement to help you along your security journey.

The security journey

Just as in life, change is the only constant in cybersecurity. Technology advances, the IT environment evolves, business priorities shift, and new threats emerge. Securing your environment through static defensive measures — the “set it and forget it” approach — is not a viable option in this world of change. Your preventive and defensive measures must change, too. In fact, implementing cybersecurity defense measures is just the start of your security journey, which is the ongoing process of defense refinements and reviews designed to continually elevate your security posture. The term “security journey” acknowledges that what protects your organization today won’t necessarily protect it tomorrow.

Every security journey is unique, but they all require:

- ☑ **Observation** – It's critical to observe *all* activity in your environment – from the endpoints, to the network, and into the cloud – to gain a comprehensive view of the threats you face and your degree of risk. Any areas that lack visibility impact your ability to progress on the security journey.
- ☑ **Evolution** – Effective cybersecurity is an organic process requiring constant attention, reconfiguration, and updating of strategies and practices. As your company grows, your security controls must keep pace to address the growing attack surface and additional potential threats.
- ☑ **Refinement** – Attackers continually refine and modify their techniques to evade detection, so security teams must adjust their defenses to counter attackers' latest moves. Detection mechanisms must be realigned to eliminate noise and bring fresh context to generate more-relevant alerts.
- ☑ **Response** – To continually reduce your attack response time, you should tailor your approach to the unique needs of your organization. Having an exercised incident response plan is a minimum requirement. In addition, learning from prior experiences can improve your response capabilities in the future.
- ☑ **Resilience** – Reducing the likelihood and impact of future security events requires proactive effort. Building resilience ensures your overall security posture will become stronger over time.

Security operations outcomes

Effective security operations produces a number of outcomes, in addition to those we've previously mentioned.

Other outcomes from security operations include:

- ☑ **Improved efficiencies** — An effective security operations team functions like a well-oiled machine. With the people, technology, frameworks, and processes in place to address security threats, you can finally reduce your mean time to respond, giving attackers less time to do their dirty deeds.
- ☑ **Optimization of existing security technology** — Security tools require an investment beyond the initial capital expenditures for acquisition. You must spend time and effort to manage these tools and unlock their capabilities. Security operations analyzes the telemetry from your existing security solutions, allowing you to optimize the value you realize from these investments.
- ☑ **Continuous improvement** — Security operations looks at the big picture to derive strategic insights that can improve your overall security posture. As attackers evolve, defenders must continually improve their detections and investigative skills. Over time, this knowledge will help your environment grow increasingly robust and make it more difficult for an attacker to successfully breach your security.
- ☑ **Security assurance** — At last, you can get a full night's sleep, assured that the business is protected day and night, all year long. If you are woken, you know it's for a legitimate issue. Alert fatigue is replaced with confidence that you or your team didn't miss a critical issue during the day (or night).

Chapter 3

How Security Operations Can Reduce the Likelihood of a Cyber Incident

In this chapter

- Learn the importance of knowing your environment
- Understand how to leverage knowledge of the enemy
- Explore the value of educating your end users

Originally used by the military, “left and right of boom” is a phrase adopted by the cybersecurity industry to describe the time before and after a successful cyber incident (the boom). The security operations tasks and procedures left of boom help reduce the likelihood of a cyber incident. These efforts are all about making it harder for attackers to meet their objective.

In this chapter, we look at the security operations activities that should occur left of boom, including efforts to achieve visibility. A strategy to gain visibility into priority network assets aligned with your risk profile is necessary to understand where you need to direct resources and focus to strengthen your security and business resilience.

Know Thyself

There is no one-size-fits-all approach to security operations. In order to effectively reduce the likelihood of a security incident, you must tailor security operations to your business' specific mission and priorities. By extension, you must understand what assets are central to the business, thus what assets require protecting, and where your vulnerabilities lie within them. These efforts fall under NIST's *Identify* function, as we describe in Chapter 2.

Know your business and its priorities

CAUTION

The mission of your security operations function must align with your business' priorities. This alignment ensures that you're focused on protecting the *right* things. Knowing your business is key to understanding what's of value and where there's risk. For example, is your company's priority customer data or proprietary data? Knowing the business also helps you to determine your risk tolerance — how much risk you're willing to accept — as well as how much you'll be willing to invest in mitigating risk.

Know your assets

You need to know what requires protection. You must understand what assets you have, where they are, who accesses them, what data is on them, and their business purpose.

The next step is to classify your assets based on their business value. Ask yourself how much risk to each particular device or service you are willing to accept. This classification will help you prioritize investments in hardening your environment.

Know your attack surface

"Attack surface" refers to the potential entry points to attack in your company's digital assets. The attack surface includes physical devices, such as servers, users' mobile devices, and Internet of Things sensors, as well as software residing in the cloud and on premises. It's important to note that the attack surface is always changing. The implementation of digital initiatives and work-from-home policies, the adoption of the Internet of Things, and the continued move to the cloud are all examples of how the attack surface changes and grows.

As part of understanding the scope of your attack surface, you also need to determine what assets support key business priorities so that you can protect them with stronger investments.

Gain broad visibility

Visibility across the entire IT environment gives security operations the best chance of detecting an attack early. Otherwise, attackers can hide in blind spots — areas that lack visibility because the organization isn't collecting sufficient data to monitor the activity in that portion of the environment. Blind spots also occur when data is retained in silos and can't be correlated for analysis.

To achieve broad visibility, the data from endpoints, the network, and cloud environments is collected in a single platform. Centralizing the data provides the security operations team with a holistic view of the IT environment. It also eliminates data silos, enabling security analysts to correlate data and uncover anomalous behavior that might otherwise be missed.

Gather Threat Intelligence

Once you understand and have visibility into your environment, you need to know *whom* or *what* you're defending it against. These efforts to identify and understand the threats targeting your environment fall under NIST's protect function, which we describe in Chapter 2.

Layer 1

While you can't foresee all attacks, knowing the location, motive, and type of threat actors challenging your organization can help you improve your defenses and prepare for future attacks. Information on prevalent attacks and attacks on your industry, your competitors, and companies similar to yours provides valuable insights. It can indicate the types of security controls you should implement and the behavior you should look for when monitoring the environment for anomalies, hunting threats, and performing incident response.

Identify the types of attackers that are targeting your valuable assets and what those specific assets are. For example, are organized crime syndicates targeting you for quick monetary gains? Are nation-state attackers looking to steal your organization's trade secrets?

Layer 2

The more you know about an attacker's tactics, techniques, and procedures (TTPs), the better you can defend against them and detect them in your environment.

Understanding the enemy will give you a sense of what assets threat actors frequently target so you can focus your defense.

Vulnerability Management

A strong vulnerability management strategy helps prevent attacks before they occur by eliminating the weaknesses attackers can exploit to gain a foothold in your environment. Vulnerabilities range from software defects and misconfigurations to missing patches and weak credentials.

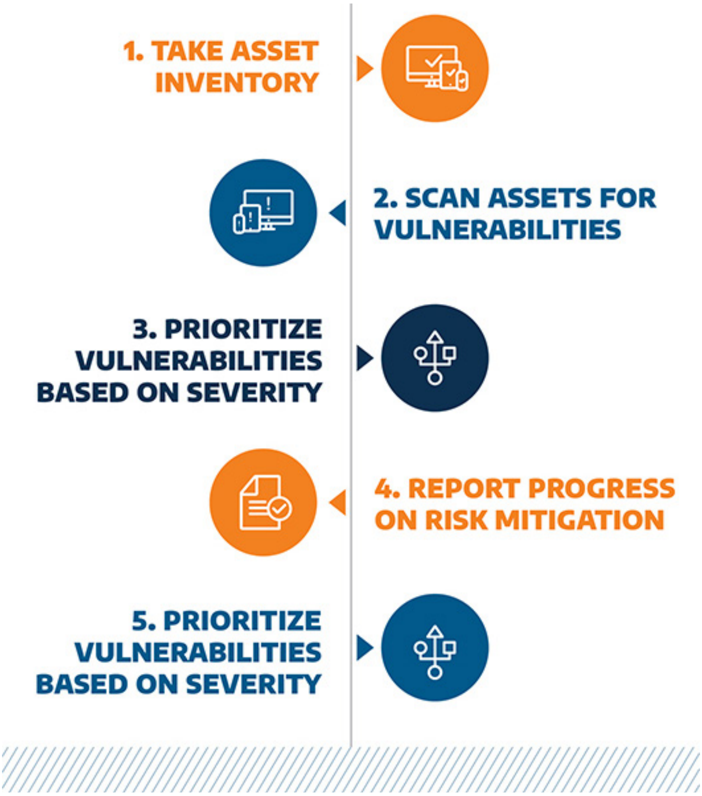

1. TAKE ASSET INVENTORY
2. SCAN ASSETS FOR VULNERABILITIES
3. PRIORITIZE VULNERABILITIES BASED ON SEVERITY
4. REPORT PROGRESS ON RISK MITIGATION
5. PRIORITIZE VULNERABILITIES BASED ON SEVERITY

Figure 3-1: Effective risk management is a five-step process.

Vulnerability management is a cyclical process that involves identifying, classifying, prioritizing, remediating, and mitigating weaknesses in the digital environment. An effective vulnerability management program requires complete, centralized visibility into the attack surface to ensure full coverage.

However, it's impractical to address every identified vulnerability in the environment. You need to take a risk based approach to prioritization. The longer a system is vulnerable, the greater the risk of exploit. Effective security operations helps to prioritize cyber risks and vulnerabilities so that your team is better equipped with complete context on what needs to be patched immediately.

Vulnerability management also necessitates coordination across the organization. For example, security operations staff must leverage their threat intelligence to coordinate with the IT team to determine if patches need to be more rapidly deployed.

Human Security

CAUTION

A discussion about cyber risk and vulnerability management is incomplete without addressing the human element. For many companies, people are both their greatest asset and their greatest risk. End users have their own business objective, and it's not security. Their focus is on getting their work done, sometimes at any cost. That could mean finding a workaround so they can access files from home or mindlessly clicking a phishing link they think will grant a manager access to a network resource. Addressing these risks is important to help prevent a cyberattack.

Consistent end-user awareness training and a culture of security can help turn people into a strong defense. To avoid contributing to cyberattacks, people must understand the important role they play in protecting the business and must be taught how to get their work done securely. Finally, to mitigate the impact of a human error, processes must be implemented to give end users the ability to report an event and allow security operations to remediate the issue as quickly as possible.

The "Care and Feeding" of Your Security Team

The job of a security operations team never ends. To operate effectively over the long term, the team requires its own "care and feeding."

DON'T FORGET

Taking care of the security operations team is important for job satisfaction and retention. Care can include recognition for a job well done and opportunities to demonstrate knowledge by, for example, mentoring junior staff members or writing for the corporate blog. These opportunities keep team members engaged in their work and feeling a sense of accomplishment. Another facet is keeping workloads reasonable to avoid burnout. Overworked, tired, and stressed security analysts aren't going to stick around for long and, in the meantime, their productivity and effectiveness may suffer, possibly resulting in overlooked security threats.

Feeding is accomplished through training to keep the security operations team current on new technologies and attack methods. With attacker techniques constantly changing, it's imperative that defenders also rapidly evolve. Training and development are also important pieces of a well-planned security journey. Training may be provided through formal classes followed by certification testing, via self-paced, independent learning, or by cross-training within the team itself.

Chapter 4

How Security Operations Can Reduce the Business Impact of a Cyberattack

In this chapter

- Explore security operations activities right of boom
- Understand how speed reduces the business impact of a cyberattack
- Learn how security operations leverages a cyberattack to prevent future attacks

As you well know, cyberattacks are inevitable. Regardless of how well your security operations team reduces the likelihood of an event, eventually there will be a successful cyberattack. At that point, their focus is on reducing the ramifications to the business, not just to IT. That means prioritizing containment and remediation. In this chapter, we look at the activities that take place right of boom – detect, respond, and recover – to reduce the impact of a cyberattack.

Right of Boom

DON'T FORGET

Reducing the effects of a cyberattack comes down to speed, as outlined in Figure 4-1. The goal is to detect and stop an attacker before they disrupt service, cause damage, or steal data. The longer it takes the security operations team to detect, respond to, and investigate an attack, the greater the likely impact to the business.

Detect quickly

The first step right of boom is detection. The security operations team relies on sensors across endpoints, the network, and cloud to quickly identify cyber threats. Continuous monitoring must be implemented to enable the team to detect anomalous activity with an understanding of the potential impact of the event. In addition, team members must understand their unique roles and responsibilities and how they align with compliance requirements.

Lively response

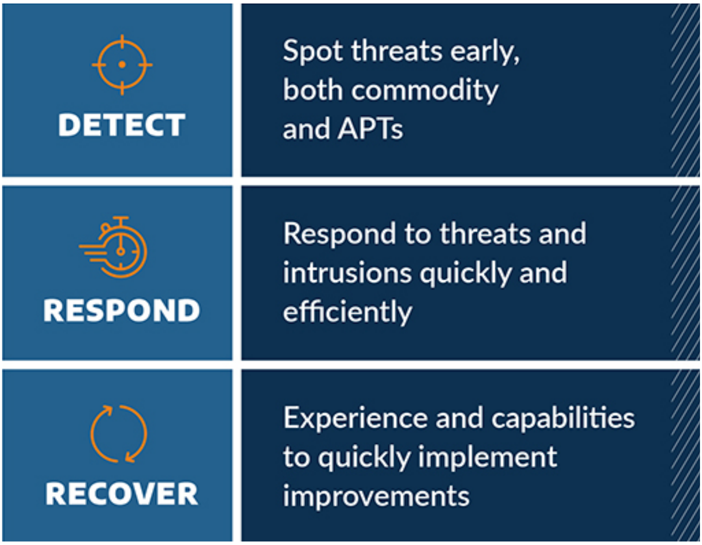
Once an attack is detected, security analysts quickly work to contain the threat and prevent it from spreading in the environment. For example, if the team detects malware, analysts take action to prevent lateral movement infecting other systems.

DON'T FORGET

The faster an attack is contained, the lower the impact to the business. Examples of containment measures include disconnecting devices from the Internet, disabling remote access, and changing passwords. However, the specific strategies and procedures used depend on the type of incident and the risk of the threat versus the business impact of the containment measures. A low-risk threat, for example, won't necessitate shutting down critical business services.

Rapid recovery

With the threat contained, the security operations team focuses on remediation. Remediation requires assessing the attack to determine its scope and severity: what systems have been affected, and what is the potential business impact? Perhaps just one server was compromised, but the business risk might be lateral movement to other critical assets. By comparison, ransomware spreads quickly and may require action to prevent further infection.



DETECT

Spot threats early, both commodity and APTs

RESPOND

Respond to threats and intrusions quickly and efficiently

RECOVER

Experience and capabilities to quickly implement improvements

Figure 4-1: Reducing the effects of a cyberattack comes down to speed.

The security operations team then eradicates the threat and cleans up the environment — by restoring services from backups, for example.

Restore swiftly

Finally, we come to the last function of NIST's Cybersecurity Framework: recover. The goal is to get back to business fast and learn from your mistakes to avoid similar incidents in the future. Recover activities include undertaking root-cause analysis focused on implementing improvements based on lessons learned; and reviewing existing strategies and identifying activities to maintain resilience and restore impaired capabilities.

Leverage Strategic Guidance

As you may recall from Chapter 1, one of the key differences between Company A and Company B was how Company B moved on from the attack. The company used the lessons learned to improve their overall security posture. These strategic moves brought the company closer to eliminating its cybersecurity risk.

Continuous improvement

TIP

Your security operations team can actively improve the organization's security posture by taking the time after an incident response to look at the big picture and making a strategic effort to reduce your attack surface. That means taking the lessons learned from security incidents and applying them to your overall security program.

Lessons learned is the feedback loop where every incident enables you to be better prepared for the next one. By documenting and sharing this information with leadership, you set the organization up to prioritize and proactively manage tactical and strategic vulnerabilities and improve weak areas.

Your security operations team also periodically reviews the security architecture and network configurations in an effort to minimize the attack surface and deploy proactive countermeasures to protect the environment against new threats.

Apply expertise

Security operations requires more than plugging in technology solutions and waiting for lights to blink green. To effectively reduce the business impact of a cyberattack, an effective team should consist of experienced and educated cybersecurity professionals who understand how attackers move through the kill chain and know the best way to stunt the attacker's efforts. They can respond to threats while reducing the risk of business impact.

DON'T FORGET

Attacks evolve, and your IT environment must evolve with them. The certified cybersecurity professionals on an effective security operations team, through their tenure, continue to develop pragmatic approaches to detecting and remediating threats while developing intuition that enables them to know where to look next. These people are by far your most important asset when it comes to building effective security operations that can eliminate cybersecurity risk.

Chapter 5

Achieving World-class Security Operations

In this chapter

- Understand some of the many processes needed for security operations
- Consider the challenges of building your own security operations function
- Explore the benefits of working with a security operations provider

No single tool or process defines security operations. As we saw in Chapter 1, Company B's success against the ransomware attack was due to a harmony of efforts. In this chapter, we break down security operations and explain the elements of this function, as well as options for obtaining security operations in your organization.

What It Takes to Implement Security Operations

Cybersecurity has an effectiveness problem – and it is compounded by an over-reliance on set-it-and-forget-it technology. Every year new technologies, vendors, and solutions emerge, yet despite this constant innovation we continue to see high-profile breaches in the headlines. We believe that organizations need to switch their thinking from a tools mindset and embrace an operational mindset.

A security operations function requires the right technology, frameworks, people, and processes, all working together to achieve agreed-upon outcomes. Let's take a closer look at each of these components.

Technology

Rest assured, we don't advise ripping and replacing your existing technology investments. The data from these tools is likely to have value. Instead, optimize IT and security controls and send the telemetry to a cloud platform for storage, enrichment, and analysis. Putting your security-related data in a centralized location allows it to be used to drive multiple security outcomes – "gather it once and use it many times" being the mantra here.

A platform is the primary piece of technology used by a security operations function to achieve visibility into the IT environment. The platform has three main functions:

1. **Collect data** – The platform works with your existing technology stack, spanning endpoints, the network, and cloud resources, to collect events from your IT environment. The platform centrally stores all security logs and telemetry to aid with regulatory compliance efforts and provides on-demand access to this event data.
2. **Enrich data** – The platform correlates the events from your IT environment with threat intelligence from commercial and open-source feeds. All event data is contextualized so you can quantify your digital risk with an understanding of vulnerabilities, system misconfigurations, and exposure to account takeovers. The platform also enables you to see security events from multiple perspectives, based on a broad set of telemetry sources.
3. **Analyze data** – The platform leverages machine learning and cloud-native detection engines to automatically detect advanced threats. To help reduce false positives, the security operations team writes custom detection rules for your environment. Finally, the platform aggregates alerts into incidents to eliminate alert fatigue.

TIP

To ensure scalability, it's recommended you take a best-of-breed approach to technology selection. Then, when considering external assistance, find a partner with a security operations platform that is cloud based and vendor agnostic. Ideally, the platform is developed and maintained by the service provider.

Frameworks

As discussed in Chapter 2, an industry-standard framework is helpful for guiding the efforts of a security operations function. Frameworks provide best practices and processes for risk assessment, threat lifecycle management, and more. By aligning your wholistic cyber program with, for example, the NIST Cybersecurity Framework, the security operations function can benchmark its efforts and gauge what changes need to be made for continuous improvement.

Specific security operations frameworks that may be used include the MITRE ATT&CK Framework (a globally accessible knowledge base of adversary tactics and techniques), and Lockheed Martin's Cyber Kill Chain® framework (part of the Intelligence Driven Defense® model for identifying and preventing cyber intrusions).

What is most important is focusing on the complete security operations framework. Look to implement a security program and outcomes that span the disciplines of identifying, protecting against, detecting, responding to, and recovering from threats against high-value assets. This approach should cover all attack surfaces: endpoint, network, cloud, identity, and human. The combination of visibility across your environment with a focus on key cybersecurity functions enables you to prevent, detect, and respond to any attack.

Processes

In addition to the processes described in industry frameworks, security operations requires others to function optimally. These additional processes include:

- ☑ **Skills-based routing** – Processes are needed to assign security issues to the individuals who are best equipped to address them. Skills-based routing reduces time to resolution by eliminating ticket escalation. The individual who receives the ticket can address it directly without further routing and delays.

☑ **Customizing off-the-shelf tools** – Processes are needed to configure commercial tools for the IT environment. Customization reduces the time it takes the security team to find true positive alerts – those that help but do not overburden the security operations team.

☑ **Establishing threat and business context** – To properly prioritize remediation efforts, the security operations function must gauge the risk level of an alert in relation to the threat and business context. Processes are needed to gather this threat and business information and correlate the data.

☑ **Tailoring outputs based on stakeholder preference** – The security operations function should understand the larger organization's preference for information quantity, format, and topic, and direct the proper outputs to the appropriate individuals.

☑ **Creating tailored escalation paths** – If a security alert comes in at 2 a.m., the security operations function must know whom to contact for that situation, be clear about the conditions under which they should wake up that person, and have the authority to do so.

☑ **Continuous improvement** – The organization must learn what is and is not working effectively so that they can reduce their detection and response times.

People

Last, but certainly not least, a security operations function requires certified security professionals with a variety of skill-sets. Security analysts, threat hunters, forensics investigators, systems administrators, and systems managers are just a few of the titles needed for effective security operations.

Security operations must be staffed for 24x7 coverage and then some to avoid employee burnout. Staff should be able to take sick or vacation time without forcing others to work a double shift. Also, people need space to learn and explore — to grow their own knowledge base and be innovative and effective in their work.

Options for Obtaining Security Operations

There are several options for obtaining a security operations function. You can take the DIY approach and build your own. Or you can outsource this function to a provider that specializes in security operations.

Build it yourself

CAUTION

When considering a new project or other endeavor, many people have the misconception that building it internally will reduce costs. However, building a security operations function requires resources that may already be difficult to come by. And without the proper resources, you're likely to fall short of achieving fully functional and effective security operations.

Budget constraints

Let's start with the most obvious challenge: cost. Security operations requires a significant investment. To build an effective function, you need to fully invest in the technology, tools, and people we described in the first half of this chapter. If you don't have the budget to hire 10-12 full-time employees (the minimum requirement for a fully staffed security operations team), to continually invest in the team's training, and to procure and manage the platform, then a DIY approach to security operations is a nonstarter.

Desire and effort

Let's imagine budget is not a problem. The executive team is willing to give you all the financial support you need to build a security operations function. Now it's up to you to hire the team, procure the technology, adopt the proper frameworks, and implement processes. Once all that's in place, someone must manage the security operations function to ensure that it continues to deliver on outcomes and operate effectively. These tasks aren't for everyone. In fact, they may simply be impossible to achieve if the need for security operations is immediate, as is usually the case.

Time investment

You simply can't build a security operations function overnight. Even if you receive financial resources, you need time to procure and set up technology, staff the team, and establish processes. This typically takes up to two years to complete. Meanwhile, the security team must continue its existing efforts to maintain the status quo.

Time continues to be a challenge even after the security operations team is functional. Faced with a constant barrage of cybersecurity attacks, security operations teams may find it difficult to do anything other than detect and respond. Organizations often find themselves in constant firefighting mode. They often can't step away long enough to apply lessons learned, reduce the attack surface, or deploy countermeasures, never mind assisting the business with new initiatives.

Evolving threats

Building an effective security operations function is also challenging because threats are constantly evolving. Malware morphs to evade detection, and attackers shift their focus to other parts of the environment. (The increasing number of attacks against the supply chain is a good example of how attackers evolve their tactics to target weaker areas in an environment.)

Organizations need threat intelligence and expertise to keep up with the latest TTPs attackers are using against their targets. This is an ongoing need that requires dedicated staff and budget.

Expanding landscape

SOCs face a challenge of staying current with expanding organizational requirements with limited staff. Threats multiply as new technology is added to the existing environment. This can be personally owned devices allowed under a bring your own device (BYOD) policy, cloud, or machine turnover. Evolving threats multiplied by a expanding landscape results in reduced security confidence and increased cyber risk.

Shortage of cybersecurity skills

The most important asset in security operations is also the most difficult to obtain: educated and experienced cybersecurity professionals. Every organization, across every industry, requires cybersecurity talent. And not just one or two trained cybersecurity professionals, but as we explained previously, a fully staffed team that can provide 24x7 coverage.

Operating with a short-staffed team exposes the organization to additional risk, including overworking existing staff (and still failing to achieve 24x7 coverage). A heavy workload can cause burnout, which can lead to sloppy errors, disgruntled employees, and rapid turnover. A staff shortage can also result in putting inexperienced professionals in charge of advanced security requirements and relying on technology solutions without the expertise to properly manage them.

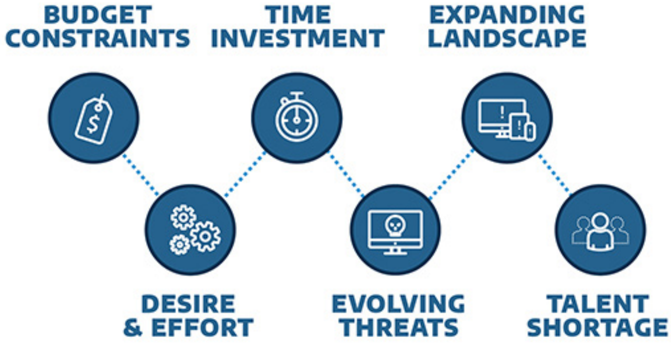


Figure 5-1: Organizations face a number of challenges when building an in-house security operations function.

Outsource to a security operations provider

The last and most viable option for the majority of organizations is to outsource to a security operations provider. Security operations providers are in the business of leveraging people, processes, and technology to eliminate risk. They understand the challenges of building your own security operations function, remove the complexity for you, and significantly reduce your time to value.

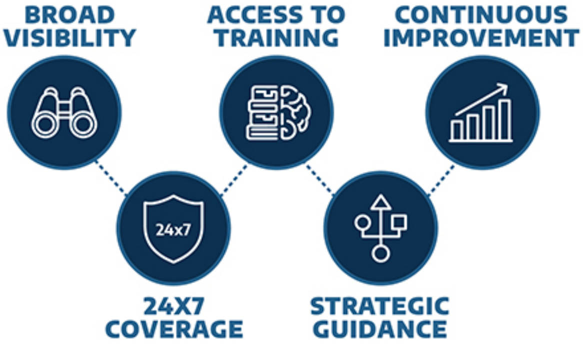


Figure 5-2: A security operations provider should deliver a variety of capabilities.

Broad visibility

Security operations providers collect and retain log data from your environment to achieve broad visibility into your endpoints, network, and cloud platform. This broad visibility enables the provider's security analysts to detect threats early.

TECH TALK

Centralizing the log data provides a holistic view of the IT environment. By eliminating data silos, security analysts can correlate data and uncover anomalous behavior that might otherwise be missed. A cloud-based platform ensures that scalability won't become a problem, regardless of how much your environment grows.

24x7 coverage

A security operations provider is fully staffed with experienced and knowledgeable security professionals to cover all time zones. You can rest assured you have continual protection.

The provider can attract top talent because its core business is security. A successful security operations provider has the resources to pay a competitive wage and offer its employees attractive benefits. In addition, the culture appeals to security professionals who are passionate about what they do.

Access to expertise and training

A good security operations provider invests in its team members to keep them motivated and developing professionally. This investment includes ensuring its people are current on latest threats, TTPs, security technologies, best practices, and other enterprise solutions (cloud, productivity apps, etc.).

The best providers offer new challenges and career paths to retain valuable staff and to keep them fresh and engaged. For you, a service provider's high retention rates mean continuity of services and added value over time as the partnership grows. When security professionals are satisfied in their job, they can focus on acquiring new skills and adding value in their current role, rather than looking for the next opportunity.

Strategic guidance

DON'T FORGET

Besides a big-picture perspective of your environment, business, and team, a good provider possesses vast experience and lessons learned from its other partnerships that translate into best practices for you. All of these assets come together in the form of strategic guidance designed to improve your security posture and minimize your attack surface.

Continuous improvement

The strategic guidance you receive from a security operations provider will result in continuous improvement. Your organization's security posture will grow stronger and the environment will become more resilient. The security partner will demonstrate this continuous improvement by benchmarking against a security strategy and framework tailored to your environment and business risk. Benchmarking enables you to understand where you are today, where you want to be tomorrow, and how you'll get there.

But Where Do We Start?

A security operations function should enable you to build resilience and sustain improvements in your security posture. If you don't already have this function, you can use external security operations expertise to continually monitor, review, and improve your cybersecurity posture 24x7. Smaller organizations often implement security operations as a turnkey service, while larger ones may choose to augment or enhance existing resources. Irrespective of the approach, the key is to work with experts who invest time to learn your environment well enough to recommend both tactical and strategic actions across the security operations framework that will make your organization more resilient and sustain improvements in your security posture.

Chapter 6

10 Requirements for Choosing a Security Operations Partner

In this chapter

- Understand the choice you need to make as a security leader
- Learn what to look for in a security operations provider
- Review the key features and capabilities that you need from a security operations provider to eliminate risk

As a security leader, you hold your company's cybersecurity fate in your hands. Like Company A, you can choose to do nothing and accept that you will be attacked with potentially dire consequences. Or you can follow in Company B's footsteps and eliminate risk with the help of a fully functioning security operations team. Assuming you choose to augment your security operations function for your best chance of success, here are 10 requirements that a leading provider should meet.

Breadth of Service Offerings

To ensure you get enterprise-grade security operations capabilities, look for a provider that delivers a variety of services in line with the NIST functions:

> ☑ **Identify** – The provider has the tools to help you complete an asset inventory, and coverage for endpoints, network assets, and the cloud.

☑ **Protect** – The provider performs vulnerability and configuration management and provides security awareness training for your team.

☑ **Detect, Respond, and Recover** – Managed detection and response (MDR) that eliminates alert fatigue by not burdening you with false positives while reducing detection and response times. Ideally, the provider works directly with you to perform threat hunting, incident response, and guided remediation.

☑ **Recover** – It's important for a provider to provide strategic guidance to recover beyond basic ticketing. Consider a provider that offers cyber assurance to help cover the impact of a cyberattack.

Security Operations Platform

Ask the security operations provider how it collects and analyzes the data from your environment. A traditional security information and event management (SIEM) or log management platform will not suffice. The security operations platform must have the power to collect, enrich, and analyze security data at scale. The platform should be able to ingest any required log source and retain data as needed, including endpoint, network, and cloud data, as shown in Figure 6-1.

Figure 6-1: A security operations platform should collect, enrich, and anlyze data from across your entire IT environment.

Dedicated Team

Day-to-day security operations requires a large team of security professionals working behind the scenes. But when it comes to interacting with the provider, you should have a dedicated point of contact who works on your behalf. In addition, a small group of named security operations experts should serve as an extension of your in-house team.

At the same time, the provider must respect its security professionals and the value they personally deliver to your organization. Look for a provider that invests in its people by providing training and paths for professional growth. These investments help with employee satisfaction and retention, which benefit you by maintaining continuity in the provider's security team.

As shown in Figure 6-2, the provider's team should provide you with the following:

- ☑ **Coverage** – Working around the clock to triage critical events and deliver actionable insights when you need them the most.
- ☑ **Expertise** – Delivering execution and operational excellence with the skills required to detect advanced threats, all customized to your environment.
- ☑ **Strategy** – Driving continuous improvement tailored to the specific needs of your organization with strategic security guidance.

COLLECT
ENRICH
ANALYZE

Figure 6-2: Look for a provider that can deliver coverage, expertise, and strategy.

No Noise

TIP

A security operations provider should properly tune its detection logic to keep false positives and alerts to a minimum. The only alerts you receive should be true, actionable alerts with guidance for remediation. You should be able to rest easy at night knowing that if the security operations provider wakes you with a critical alert, it is for good reason.

Organizational Understanding

The ideal security operations provider is much more than a partner. To eliminate risk, the provider must function as an extension of your organization. The provider's security team should understand your business operations and company culture. They should learn how these impact your network architecture and act accordingly.

Value

The security operations provider should deliver value from day one of your engagement and a return on your investment year over year. Most notably, the provider should reduce the time, effort, and money your organization must spend to manage cybersecurity incidents, freeing your security and IT operations people to work on other tasks. The provider should also improve your security maturity without the cost of additional staff or security tools.

In addition to the other items in this chapter, to help ensure a suitable return on investment, look for a provider that leverages your existing technology investments and offers predictable pricing and unlimited data collection.

24x7 Monitoring

DON'T FORGET

Around-the-clock monitoring is an absolute necessity. If a security operations provider only promises to monitor your environment during standard business hours, then their team will always be playing catch-up, triaging the previous night's alerts rather than looking at current activity. Look for a security operations provider that is fully staffed to operate both day and night, seven days a week, with enough wiggle room to accommodate its employees' vacation and sick time without causing burnout for the rest of the team.

Comprehensive and Centralized View of Security Posture

Given its knowledge of your business and visibility into your environment via a security operations platform, the provider should have its finger on the pulse of your organization's security posture. The ideal provider will assign you a dedicated by-name security team that leverages their security expertise along with knowledge of your environment to provide strategic guidance. The end result should be steady enhancements to your security posture as you proceed along your security journey, as shown in Figure 6-3.

Figure 6-3: The ideal partner should lead you on a security journey that results in a continuously improving security posture.

More than Technology

Ninety percent of breaches involve human error. Focusing solely on the technology aspect of threats ignores an important part of the threat landscape. A successful security operations provider should include the capability of detecting human-centric threats and include a process to help eliminate human error. This could include an awareness program designed to create a foundational security understanding among employees to prevent many cyberattacks from being successful.

Flexibility

A provider should be flexible in their approach. To achieve value from day one, they should be able to hit the ground running with any security stack. They should also evolve as the customer does and grow to meet the customer's demands.

Bonus: Cultural Fit

DON'T FORGET

Remember, people are a key component of security operations. Just as you vet the provider's technology platform, you should also make sure that you have a rapport with the provider's people, especially your dedicated security team. The security operations provider will see your organization on its best days and its worst days. When you're operating right of boom and stress levels are high, you want to be working with people you can trust and don't mind working with side-by-side for hours at a time.

Discover how security operations can dramatically decrease the likelihood and business impact of an attack while improving your overall security posture.

Despite sizeable budgets and an array of technology solutions at their disposal, most security teams can barely keep up with the barrage of threats targeting enterprise IT environments — and it's only getting worse as attack surfaces grow. It's time for a new approach. This guide provides a pragmatic approach to reducing the risk and impact of an attack and improving security resiliency.

- Understanding cyber risk — learn why companies can spend hundreds of thousands of dollars on security and still succumb to attacks.
- Exploring security operations — examine the tactical and strategic components that comprise security operations.
- Learning how security operations reduce the likelihood of a cyber incident — explore how to lower the risk of becoming an attack target.
- Examining how security operations reduce the impact of a cyberattack — understand how to ensure your business can withstand an attack.
- Achieving world-class security operations — know what it takes to establish effective security operations.

About the Author

A former editor of SearchSecurity.com, Crystal Bedell is a senior marketing consultant specializing in cybersecurity. She's been helping technology providers create engaging content since 2000.

CYBEREDGE PRESS

Not for resale
ISBN 978-1-948939-30-0

9 781948 939300 >