Netsurion®

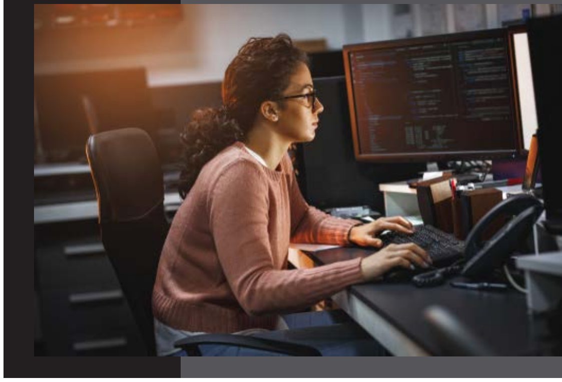
2023 Edition

Managed SIEM

Buyer's Guide

Navigating a complex market and making the smartest investment for your organization.

EXECUTIVE SUMMARY



The modern threat landscape is complex, with an expanding attack surface across on-premises and cloud assets. Aggressive adversaries target today's fluid perimeter, emphasizing the need for greater visibility, rapid detection, effective response, and adaptive security that evolves with the changing threat landscape. And yet advanced threat protection in a world of scarce resources is daunting, with almost 3 million open global IT and security jobs according to (ISC)^2.

The issue: How to reduce cyber risk through continuous monitoring, rapid detection, and effective remediation in a way that is both practical and affordable?

Many organizations are finding cybersecurity success with managed SIEM services that bring together virtually the most crucial technology and expertise for visibility and mitigation.

But the managed cybersecurity market is both complex and ambiguous. These solutions go by many names – Managed SIEM, SOC-as-a-Service, Managed Detection and Response (MDR) for example – and have varying degrees of overlaps and gaps.

As a result, it can be extremely difficult to evaluate which solution will best suit your unique organization's business needs, budget restrictions, and resource requirements.

Our aim in this Managed SIEM Buyer's Guide is to give you clear contextual knowledge and a framework for an efficient buying process that arrives at the best-fit solution for your organization.

KEY TAKEAWAYS

- The security mindset must shift from "incident response" to "continuous response", which assumes you will be compromised. No organization is immune.
- Security Information and Event Management (SIEM) is the engine that drives any substantial cybersecurity solution. But SIEM can be challenging to deploy, tune, and manage on your own – resulting in unused "shelfware" that wastes time and money and creates security awareness gaps.
- SIEM has risen due to its many advantages: it overcomes staffing challenges, provides 24x7 monitoring and alerting, addresses compliance mandates, increases cybersecurity effectiveness, and decreases total cost.
- This buyer's guide assists you in navigating the sea of technology and service provider choices.

CONTENT

EXECUTIVE INVOLVEMENT IN

CYBERSECURITY LEADERSHIP

Organization leaders have many competing initiatives for their time and budgets as they run the business. Cybersecurity is an executive-level issue for several reasons:

- It impacts day-to-day operations, long-term viability, revenue, and reputation
- It is a cross-functional issue in that cybersecurity is everyone's responsibility
- It should be treated as an investment in digital transformation, not a cost center
- Your organization's appropriate cyber risk posture and data governance strategy is crucial

Your organization's leaders must evaluate and weigh many strategic initiatives, as well as determine which to fund or prioritize. It is important to emphasize that the purchase of a managed security solution is one that helps the organization save money and reduce cyber risk at the same time.

Carefully weigh the actual capabilities and timeline of security options like open source tools cobbled together, that might seem less expensive but ultimately take valuable time away from running the business and generating revenue. Include any compliance mandates you must meet and insights regarding critical asset prioritization. Finally, remind your leaders that the security landscape is evolving with new threat vectors like the SolarWinds/Orion data breach in the news headlines. Today's threat mitigation is all about the comprehensive visibility and analytics needed for rapid detection and response to stop cyber criminals.

Cybersecurity involves a balancing act. An organization that is too conservative with an aversion to risk might overlook business advancements and opportunities, while a company that ignores business and technology risk is sure to face the consequences.

ASSESSING YOUR

SIEM OPTIONS

The right SIEM solution varies based on your goals, use cases, budget, compliance requirements, and available staff. SIEM solutions are optimized for different use cases, and one size never fits all. The wrong selection can have a long-lasting impact, be costly to maintain and support, and time consuming to tune, which is why many SIEM deployments end up abandoned.

Understanding the Terminology and Solution Differences

Now that you have some insight into the foundational use cases for SIEM, it's helpful to have a common understanding of the terminology and unique differences between the approaches to security information and event management. Distill down the solutions and tradeoffs as you evaluate the optimal architecture and options for you, as well as your entire team. Advanced threats require more advanced people resources, technology, and incident management than in years past. While definitions vary, and there are always hybrid scenarios, there are four primary options for a managed SIEM solution:

DIY SIEM Software: This do-it-yourself option involves organizations implementing the SIEM technology themselves or leveraging open-source tools in combination to add analytics, compliance, and log storage, for example. Do-it-yourself options typically require a larger team and higher level of expertise to not only implement but also manage, maintain, and tune over time. SIEM is not a "set it and forget it" technology.

SIEM-as-a-Service (SIEMaaS): Also called "cloud SIEM", is basically Software-as-a-Service licensed on a monthly basis and hosted, maintained, tuned, and patched to work optimally so that you don't have to worry about the infrastructure, log storage, or system administration. But you still have the responsibility to drive it to get value out of SIEM-as-a-Service.

SOC-as-a-Service (SOCaaS): In this case, you receive the SOC "function" as a service. Not just the software, but also the people, the processes, and the SIEM platform/tool necessary to perform the network and endpoint threat monitoring, detection, and response for your organization.

Co-Managed SIEM: This is a version of SOC-as-a-Service in which you play a more active role in the shared responsibility of determining and carrying out the security operations strategy. A runbook with incident response (IR) and an operating playbook typically outline the shared responsibility tailored to your organization.

Document your "must-have" criteria from "nice-to-have" considerations so that you don't solve for corner cases that can add complexity and cost. Congratulations if you determine that a DIY approach is optimal for you and your organization. If you quickly realize that you need to augment your skills and staff with a managed SIEM, this guide can help you make sense of the alternatives.

CORE CAPABILITIES OF A

CO-MANAGED SIEM

Squeezed by tight budgets and facing a cybersecurity talent shortage, Small-to-Medium-Sized Businesses (SMBs) are partnering with SIEM providers to leverage expertise without giving up control. SMBs are traditionally priced out of big-ticket information security applications while they are under increased pressure to obtain the sophisticated cybersecurity tools typically found in Fortune 500 firms. But they're faced with tough decisions based on budget constraints and the ultra-tight labor market. That's where a Co-Managed SIEM performs best.

Core SIEM Use Cases

- Real-time alerting and monitoring
- Log correlation and aggregation
- Detect advanced and unknown threats
- Compliance reporting and auditing
- Actionable threat intelligence
- Provide remediation recommendations
- User behavior analysis such as for insider threats
- Long-term event storage
- Conduct threat hunting & forensic investigation
- Integrate with existing tools like ticketing

A Co-Managed SIEM provides 24x7 monitoring, alerting, and threat analysis expertise, as it enables your direct control and daily insights when you need it. An outsourced managed service may provide you with the reports or output, but little or no oversight on the data, process, or analysis that produced the report. A Co-Managed service enables you to view more security context with greater transparency. Your requirements and operational preferences form the foundation of a Co-Managed solution.

The gap seen within SMBs is particularly acute when it comes to the deployment of sophisticated cybersecurity tools such as SIEM software. SIEM requires both a meticulous setup and ongoing monitoring by experts to glean meaningful results from the vast reams of log and event data ingested from every device in your organization.

Advantages of Co-Managed SIEM

Visibility across the network and cloud applications

Assigned customer success team

Threat remediation guidelines

SIEM customization and optimization

Ongoing security and compliance review

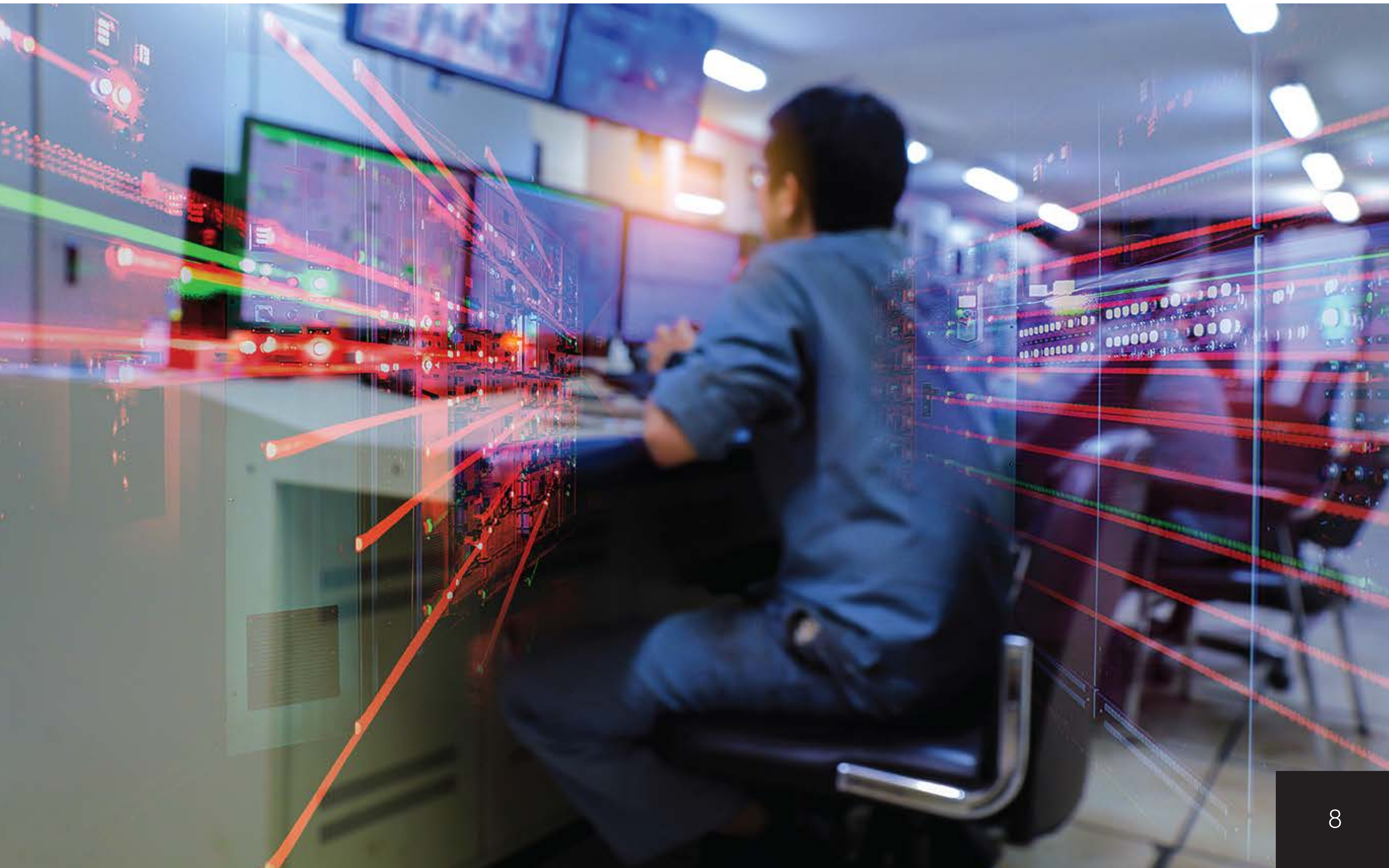
Accelerated time-to-value

Benefits of Co-Managed SIEM include detecting vulnerabilities faster via machine learning and automation, simplified onboarding, and implementation with enhanced time-to-value, while blocking threats with integrated capabilities such as endpoint detection and response. SMBs now have access to the same powerful tools and processes as larger firms, but at a fraction of the cost and much lower total cost of ownership (TCO).

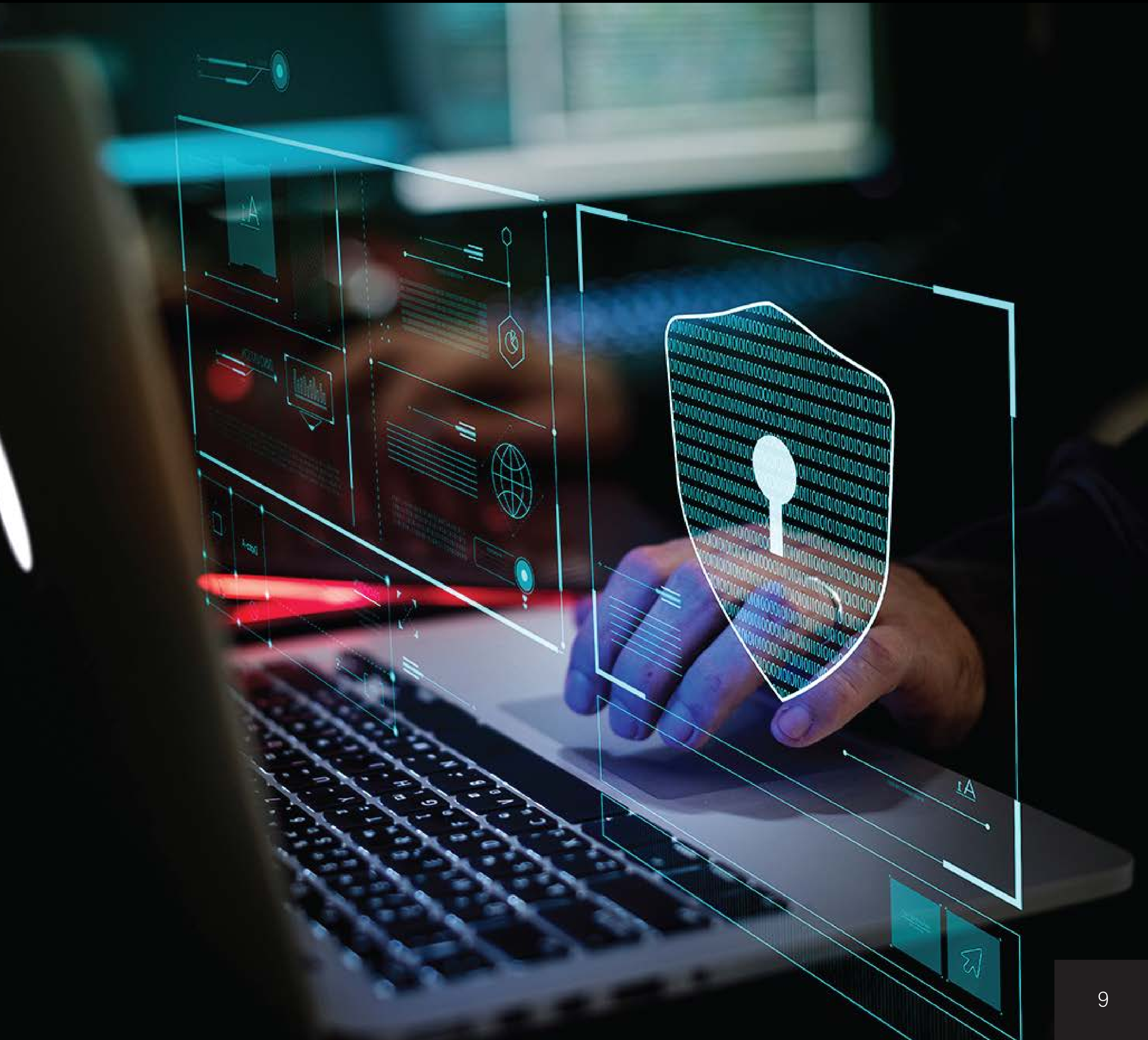
The use cases for Co-Managed SIEM are also as varied as the organizations and industries adopting the security platform. If compliance support is one of your SIEM requirements, be sure to include that in your decision process because some SIEM platforms are optimized more for threat hunting and less for compliance and audit reports. SIEM solutions are not one-size-fits-all and not all are created equal.

> Co-Managed SIEM services enable security and risk management leaders to maximize value from SIEM and enhance security monitoring capabilities, while retaining control and flexibility.
>
> **Gartner, "How and When to Use Co-Managed SIEM," by Kelly Kavanagh.**

The bottom line: a Co-Managed SIEM performs the heavy lifting with a proven track record while you address deeper investigations and remediation activities. You benefit by detecting threats faster, reducing your cybersecurity risk, and optimizing your team to enhance operational efficiency.



OPERATIONALIZING SIEM WITH TECHNOLOGY, PROCESSES, AND PEOPLE

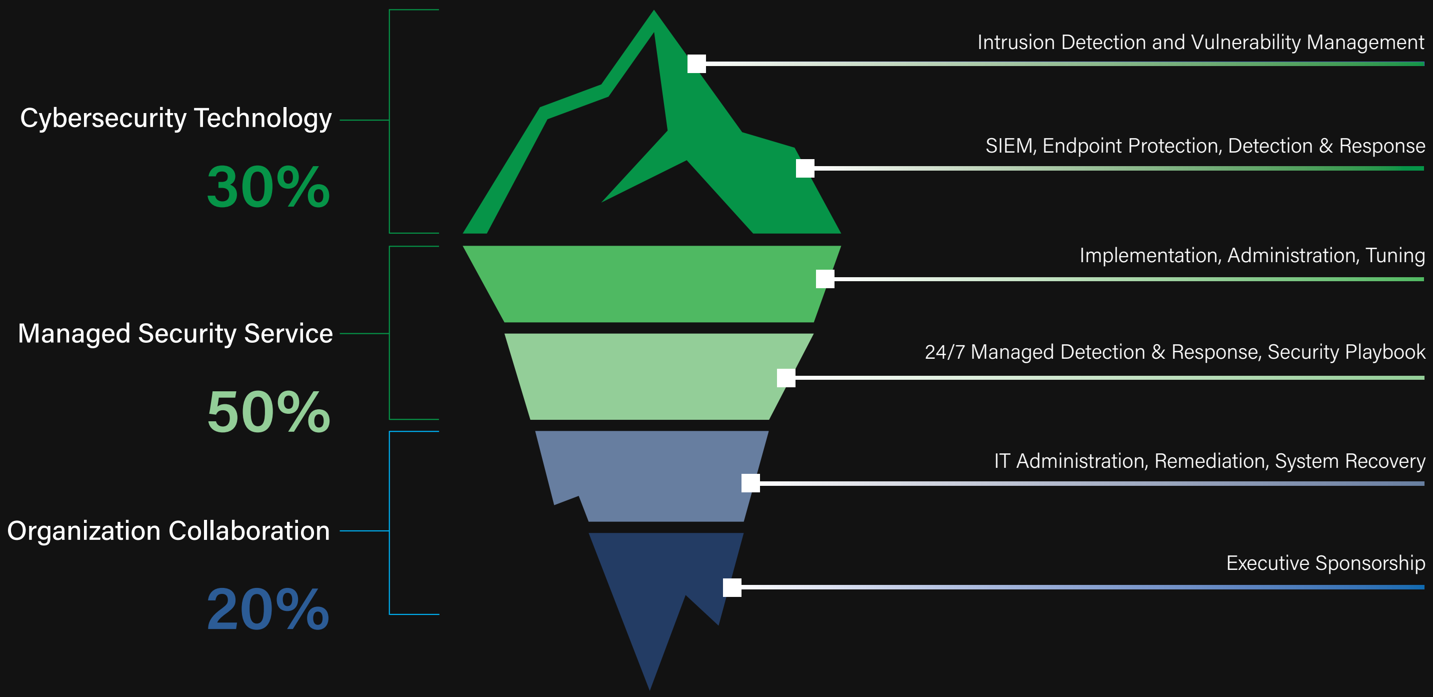


Traditional anti-virus (AV) and anti-malware solutions on the endpoint have long been a staple for enterprise security. However, due to long adoption periods and first-generation technology, they are now being exposed due to advanced cyber attacks. While legacy AV can detect malicious code, threat actors are now able to avoid detection through obfuscation techniques.

When you consider replacing legacy AV, there's a new opportunity - SIEM, Endpoint Protection, a 24x7 SOC visibility and threat hunting, called **extended detection and response (XDR)**. This route offers organizations an ability to consolidate technology and realize improvements in both team efficiency and cybersecurity spend.

Technology is just the tip of the iceberg

Without process discipline and expertise, the promise of SIEM technology cannot be realized



Cybersecurity Technology
30%

Managed Security Service
50%

Organization Collaboration
20%

Intrusion Detection and Vulnerability Management

SIEM, Endpoint Protection, Detection & Response

Implementation, Administration, Tuning

24/7 Managed Detection & Response, Security Playbook

IT Administration, Remediation, System Recovery

Executive Sponsorship

Figure C: Technology, Process, and People Requirements are Not Always Visible

Technology: You need a well-tuned SIEM to provide the foundational visibility for your SOC, along with IDS/IPS, vulnerability assessment tools, advanced analytics and reporting, endpoint detection and response, and more. Automation can also increase efficiencies when applied to the massive amounts of data that must be correlated and filtered for cyber threats. Threat intelligence then provides context and is specific to your organization’s goals and risk posture.

As Figure C shows, technology is just the tip of the iceberg in a SIEM solution. You still require the human experts – the cybersecurity analysts – and process discipline to review the suspicious alerts that need additional evaluation and incident response handling.

Processes: Detailed organization-specific incident response playbooks need to outline specifically what should happen when ransomware, malware infections, distributed denial of service (DDoS) attacks, or other threats are detected:

- These playbooks specify how to respond, investigate, what evidence to gather, and how and when to escalate.
- SOC processes call for continuous monitoring 24x7 since attackers don't take a break during off-hours.

People: Staffing is likely the most expensive and challenging component in developing a DIY SOC. It's difficult to hire a team of Tier 1 security analysts with the bandwidth and expertise to perform 24x7 monitoring, all while we're experiencing a worldwide shortage of cybersecurity talent.

- You need to cover three work shifts, including management and subject matter expertise in your IT technology infrastructure and advanced Tier 2 and 3 resources for threat hunting, research, malware analytics, and more.
- Some organizations erroneously think they can staff a SOC with only three resources total or one analyst per shift. That staffing is insufficient and does not allow for time off, training, or adequate forensic investigation.
- A more realistic SOC approach is to have a minimum of 8 to 10 analysts for around-the-clock coverage. Note that it will also be even harder to retain them in the face of stiff competition for these scarce resources. There is also the related expenses of the physical location and real estate as well as telecommunications costs.

It's easy to see why a managed SIEM solution makes sense from both a time-to-value and cost stance. It is both practical and affordable while addressing today's staffing challenges.

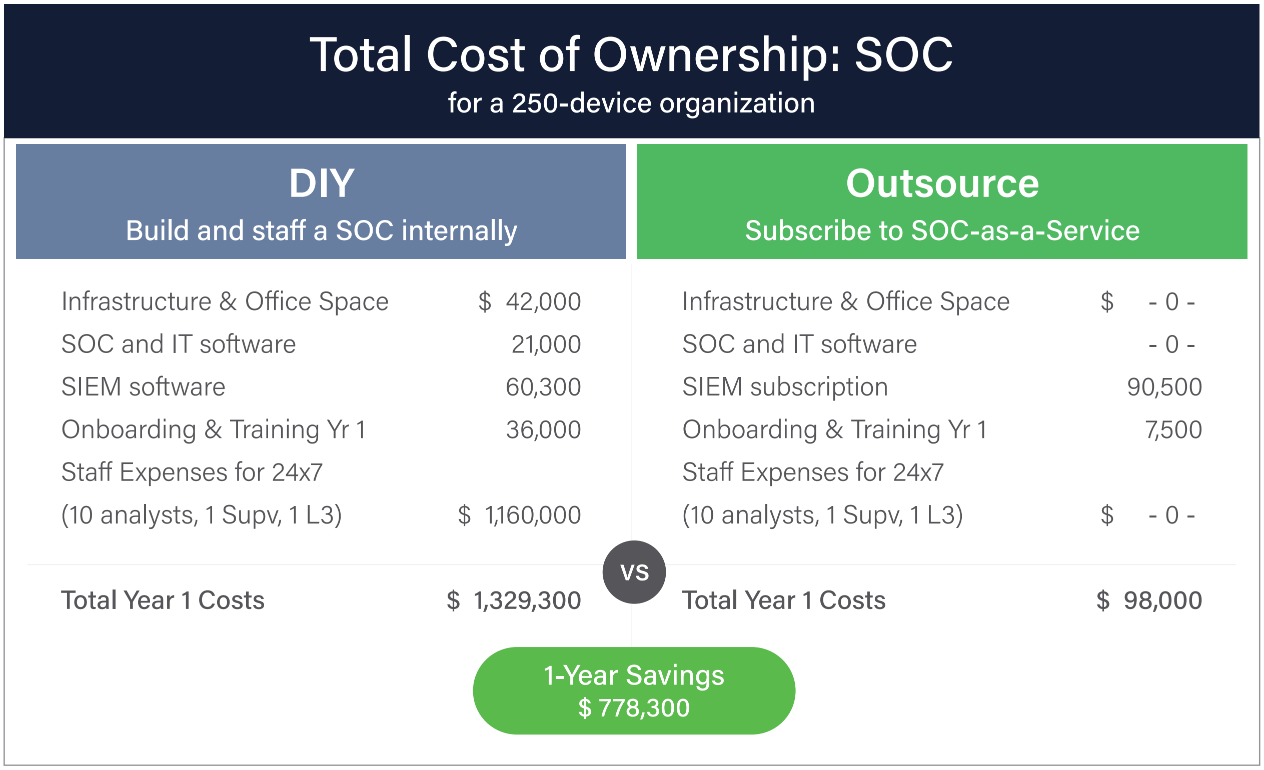
WAYS TO ACHIEVE A 24x7 SOC

POWERED BY SIEM

The SOC is the command center for your cybersecurity operations, with SIEM as the engine providing visibility, correlation, and alerting. It takes a sophisticated combination of people, processes, and technology to run a SOC that operates 24x7. There are two main paths: build your own SOC or take a managed approach with SOC-as-a-Service. Some of the decision criteria regarding these options and tradeoffs include:

- Cost
- Control
- Onboarding and start up
- Flexibility
- Time-to-value

A "Build Your Own" SOC tradeoff includes higher costs, but more control and flexibility. You determine your organization's risk tolerance and you decide which threats fall outside that level. You also implement your own threat investigation and forensics. Building your own SOC also requires operating a SIEM – which is no simple task. A DIY approach may initially seem more affordable, but there are many overlooked or hidden expenses as the Operationalizing SIEM with Technology, Process, and People section outlined. Evaluate the TCO over time, including the implication of rising salaries. On the other hand, SOCaaS generally has a faster time-to-value of 1-2 months versus 12-14 months for DIY because the infrastructure and staff already exist. SOC-as-a-Service avoids reinventing the wheel and offers all the benefits of an in-house SOC with very few disadvantages.



Total Cost of Ownership: SOC

for a 250-device organization

DIY Build and staff a SOC internally		Outsource Subscribe to SOC-as-a-Service	
Infrastructure & Office Space	$ 42,000	Infrastructure & Office Space	$ - 0 -
SOC and IT software	21,000	SOC and IT software	- 0 -
SIEM software	60,300	SIEM subscription	90,500
Onboarding & Training Yr 1	36,000	Onboarding & Training Yr 1	7,500
Staff Expenses for 24x7		Staff Expenses for 24x7	
(10 analysts, 1 Supv, 1 L3)	$ 1,160,000	(10 analysts, 1 Supv, 1 L3)	$ - 0 -
Total Year 1 Costs	**$ 1,329,300**	**Total Year 1 Costs**	**$ 98,000**

VS

1-Year Savings
$ 778,300

Figure D: Significant Cost Savings With an Outsourced vs a Do-it-Yourself Approach

Lower your TCO of Co-Managed SIEM vs DIY SIEM

Netsurion's Co-Managed SIEM maximizes value and enhances security monitoring capabilities with control and flexibilty. Netsurion's SIEM solution maximizes value and enhances security monitoring with control and flexibility.

ACHIEVING

COMPLIANCE IS FUNDAMENTAL

The best SIEM platforms continue to innovate to stay ahead of evolving threat actors and changes in the threat landscape. Compliance mandates such as PCI DSS and HIPAA initially drove SIEM adoption. While compliance and audit reporting remain table stakes, today's SIEM solutions have an increased focus on threat detection and forensics. IT and security budgets once dominated by prevention are seeing a more balanced approach with increased emphasis and spending on detection and response as well. This means the convergence of one-stop-shop capabilities such as user & entity behavior analytics (UEBA) with machine learning (ML), endpoint detection and response (EDR), threat intelligence like MITRE ATT&CK for improved context and correlation, intrusion detection systems (IDS), file integrity monitoring (FIM) and automation and incident response. Whether you call it SIEM 2.0, SIEM+, or Next-Gen SIEM, the benefits of this continued innovation include:

- A holistic approach to cybersecurity and threat detection
- Greater convenience for users and IT decision makers
- Investment protection over the long term
- Fewer point products to purchase, implement, and manage

Over time, SIEM architecture has also evolved. The majority of early SIEM deployments were delivered on-premises, but SIEM-as-a-Service and Co-Managed solutions are gaining wide adoption. You can deploy SIEM with private cloud hosting, provider hosting, and Software-as-a-Service (SaaS) in addition to on-premises formats.

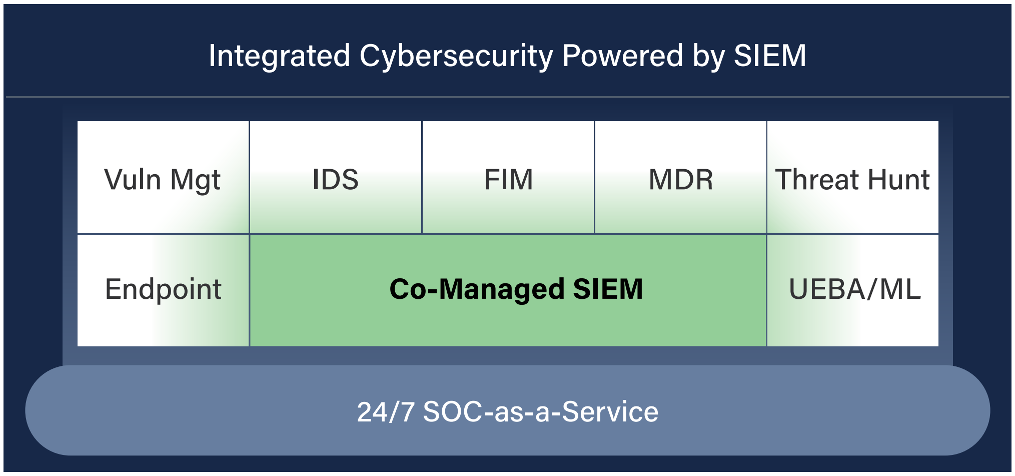


Figure E: Evolution of SIEM Architecture

Integrated solutions built on the foundation of SIEM such as SIEM + Endpoint Protection + SOC eliminates buying and managing multiple point products that add complexity.

SIEM technology needs people and processes to convert vast amounts of raw data into actionable information for cybersecurity decision making. It is a crucial tool used by security analysts in a physical or virtual SOC. However, SIEM tools still require sizing, architecting, onboarding, tuning, and managing – responsibilities that you may not want to own. Managed SIEM services have grown in popularity as the cybersecurity skills shortage has impacted the ability to staff projects and operations.

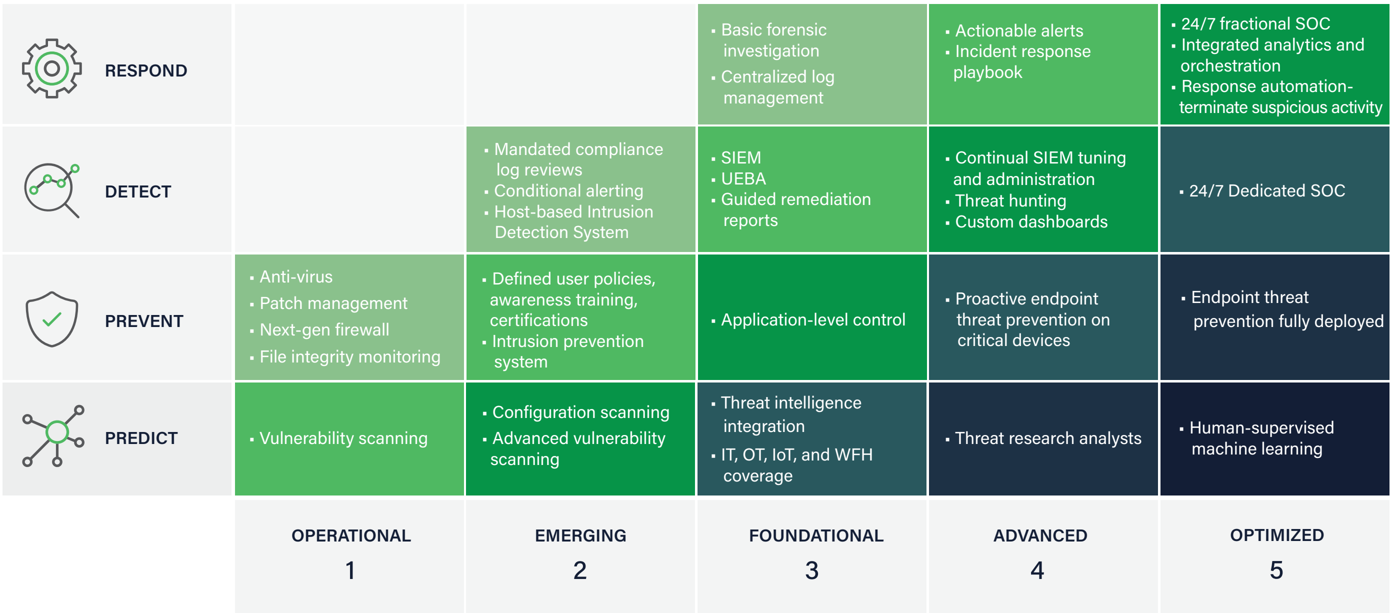
EVALUATE YOUR

CYBERSECURITY MATURITY

Security maturity is about more than purchasing tools or layering on more point products. There is no silver bullet to security maturity and improving your cybersecurity posture. More technology and tools can also contribute to IT sprawl and complexity, create siloed visibility, and add more work for you and your team. These frameworks can be useful to see where you stand relative to your peers or industry best practices. Models can also serve as a type of roadmap on your cybersecurity improvement journey.

Shown below in Figure F is a straightforward Cybersecurity Operations Maturity Model from Netsurion. Move from left to right to assess your current risk mitigation stance from reactive to proactive. Netsurion's model outlines some of the optimal technology, processes, and people you need for security effectiveness, such as a 24x7 SOC and a multi-layered approach. Proactively making changes in your security approach is critical, before facing marketplace pressures or regulatory fines.

Assess realistically where you stand and what levels can best accelerate your progress. The best solution may be a hybrid approach, managing some aspects internally and leveraging a managed service provider for others. Capabilities like SOCaaS provide increased security coverage and expertise..



RESPOND			• Basic forensic investigation • Centralized log management	• Actionable alerts • Incident response playbook	• 24/7 fractional SOC • Integrated analytics and orchestration • Response automation-terminate suspicious activity
DETECT		• Mandated compliance log reviews • Conditional alerting • Host-based Intrusion Detection System	• SIEM • UEBA • Guided remediation reports	• Continual SIEM tuning and administration • Threat hunting • Custom dashboards	• 24/7 Dedicated SOC
PREVENT	• Anti-virus • Patch management • Next-gen firewall • File integrity monitoring	• Defined user policies, awareness training, certifications • Intrusion prevention system	• Application-level control	• Proactive endpoint threat prevention on critical devices	• Endpoint threat prevention fully deployed
PREDICT	• Vulnerability scanning	• Configuration scanning • Advanced vulnerability scanning	• Threat intelligence integration • IT, OT, IoT, and WFH coverage	• Threat research analysts	• Human-supervised machine learning
	OPERATIONAL 1	EMERGING 2	FOUNDATIONAL 3	ADVANCED 4	OPTIMIZED 5

Figure F: Optimizing Your Cybersecurity Maturity Over Time

The objective of the model is to help you understand your current state of cybersecurity maturity in order to create a holistic strategy for enhancing your security posture over time. Improve your cyber resilience and reduce breach response times by implementing processes that are industry best practices, repeatable, and leverage external resources as needed.

Using the Cybersecurity Maturity Model

- Which stage best reflects your organization today?
- Which stage best reflects the capabilities your organization should have?
- Are you capable of deploying that stage across your entire organization?

CO-MANAGED SIEM

ADVANTAGES

Netsurion delivers SOCaaS based on our award-winning SIEM platform and specializes in Co-Managed SIEM to collaborate with your IT team in delivering the best-fit security solution.

We are renowned for our Managed Security Services as well as our SIEM technology and MDR service:

Managed Detection and Response

Next Gen MDR Service Provider

Hot XDR Company

SIEM

We enable customers to increase their cybersecurity coverage with the integrated services at lower cost.

ADVANTAGES OF CO-MANAGED SIEM FROM NETSURION

- Detect and minimize threats faster
- Simplify security and compliance
- Increase operational efficiency
- Reduce cybersecurity costs and resources
- Integrate the synergies of SIEM + EDR + SOC

Threat Detection and Compliance in Action

An insurance organization with its sensitive financial data and supply chain connections was a high-value target to cyber criminals. The organization processed credit card payments and grew large enough that they faced increased security and compliance mandates for PCI DSS. They quickly realized that their small IT team was stretched too thin with day-to-day operating responsibilities, and their previous ad hoc log monitoring was too inconsistent and might even have created security gaps. After considering several SIEM providers, they selected Netsurion to enable Co-Managed SIEM on a 24x7 basis. The financial services organization is now confident that their proactive security approach augments their three-person IT team to defend their network and protect their sensitive data.

A MANAGED SIEM

BUYER'S TOOLKIT

As you and your IT/security team evaluate how to protect your organization from advanced threats, know that you don't have to go it alone. This guide helps outline your options with a focus on best practices that maximize your cybersecurity investment and finite resources. You can then focus on growing your business and engaging with customers without turning into an IT company.

Assess Your Security Maturity: It's helpful to have a roadmap that highlights the cybersecurity journey ahead so that you know where you stand and what's needed to achieve better security outcomes, and increase safeguards and compliance. Download this Cybersecurity Operations Maturity Model for businesses like yours.

See Our Co-Managed SIEM Up Close: A picture paints a thousand words as they say. Request a one-on-one demo to see for yourself how easy it is to achieve speed-to-value while retaining control and flexibility. We'll show you how Netsurion predicts, prevents, detects, and responds to advanced threats to minimize the impact of any potential data breach.

Eliminate Guesswork With a SIEM Checklist: View the checklist to understand the considerations for selecting a Co-Managed SIEM. We've created a checklist based on hundreds of SIEM decisions and implementations: communicating cyber risk to executives, evaluating options, and understanding people, processes, and technology implications.

To learn how Netsurion can augment your existing staff and reduce cybersecurity risk, email us

CONCLUSION

It is often unrealistic for most small-and-medium-sized businesses to hire, train, and retain in-house SOC staff and implement the state-of-the-art threat intelligence provided by the SIEM and Managed Detection and Response (MDR) solutions necessary to be effective. Attempting to implement DIY cybersecurity can result in underutilized security software that becomes shelfware and leads to gaping vulnerabilities.

Netsurion provides a smarter investment. Our Co-Managed SIEM, SOC-as-a-Service, and MDR delivers the optimal combination of people, processes, and technology. We enable you to predict, prevent, detect, and respond to security incidents when every minute matters in reducing attacker dwell times.

ABOUT NETSURION

Netsurion® delivers an adaptive managed security solution that integrates our Open XDR platform with your existing security investments and technology stack, easily scaling to fit your business needs. Netsurion's 24x7 SOC operates as your trusted cybersecurity partner, working closely with your IT team to strengthen your cybersecurity posture. Our solution delivers managed threat protection so you can confidently focus on your core business.

Headquartered in Ft. Lauderdale, FL with a global team of security analysts and engineers, Netsurion is a leader in Managed Extended Detection and Response (MXDR). Learn more at www.netsurion.com.

SOURCES

- ISC(2), "2021 (ISC)2 Cybersecurity Workforce Study, October 26, 2021," https://www.isc2.org/News-and-Events/Press-Room/Posts/2021/10/26/ISC2-Cybersecurity-Workforce-Study-Sheds-New-Light-on-Global-Talent-Demand
- Gartner Press Release, "Gartner Says Data and Cyber-Related Risks Remain Top Worries for Audit Executives," November 7, 2019. https://www.gartner.com/en/newsroom/press-releases/2019-11-7-gartner-says-data-and-cyber-related-risks-remain-top-worries-for-audit-executives
- https://www.netsurion.com/case-studies/co-managed-insurance-company
- Gartner, "Critical Capabilities for Security Information and Event Management," Toby Bussa and Kelly Kavanagh, December 03, 2018. https://www.gartner.com/en/documents/3834694/critical-capabilities-for-security-information-and-event

Netsurion®