CONNECTWISE

CONNECTWISE EBOOK SERIES

Choosing the Right SIEM Solution for Your Cybersecurity Practice

AN MSP'S GUIDE TO SIEM FUNCTIONALITY AND PRACTICE CONSIDERATIONS

CONTENTS

INTRODUCTION

Security information and event management (SIEM) isn't a new technology, but its evolution plays an essential part in protecting against every-changing cyberthreats and attacks. For managed service providers (MSPs), the best change in SIEM is that what used to be an enterprise-level cybersecurity tool is now available and affordable for small- and medium-sized businesses. This means it's easier than ever to go beyond the single layer of firewall and antivirus perimeter to add more layers of cybersecurity to reduce risk for your clients and your business.

This guide will cover what SIEM is, the benefits of the technology for MSPs, and how to choose the right SIEM for your business.

CHAPTER 1: WHAT IS SIEM?

Many feel that SIEM is a complex mystery, but it doesn't have to be. The simplest definition: SIEM combines security information management and security event management (SI + SE = SIEM) to help detect potential vulnerabilities and threats. Whether you call it SIEM, data lake, or log aggregation, adding it to your toolset enhances the transparency of your cybersecurity posture.

The easiest way to think about SIEM is as a "prevent, detect, monitor" tool. For years, firewall and antivirus have been recognized as essential, but prevention alone can't stop all threats. The changing cybersecurity landscape requires preventive security and detective security. That's what SIEM does—it prevents, detects, and monitors to create additional layers of security.

Here's how it works: SIEM collects log and events data from your network devices, systems, applications, and services. It brings all that information into one platform, creating visibility into what's happening with all the elements in your IT ecosystem. Qualified techs or a security operations center (SOC) team then use automation to run the data against prebuilt cybersecurity rules.

This process identifies what is white noise, blocks potential threats that controls can identify, and alerts you to what needs more attention as a potential threat. In other words, it amplifies threat detection so that you can quickly discover a breach and respond when something gets past your traditional perimeter defense.

SIEM has been around since 2000, but its usability and effectiveness became a powerhouse when the technology moved to the cloud. Fortunately, this also made it more accessible to MSPs. The move allowed SOC teams to use SIEM to provide 24/7/365 monitoring and logging of security event alerts. SIEM with a SOC can identify, analyze, and respond more quickly to threats than ever before.

Adopting SIEM may feel more necessary and urgent if you or your clients have compliance and regulatory requirements, you have too many data sources and alerts, or you see the need for added protection.

CONNECTWISE
ManagedServices@dandh.com

CHAPTER 2: WHY SIEM IS IMPORTANT FOR MSPS

The responsibilities of an MSP become more layered and complex as the threat landscape changes. Of course, this means that your cybersecurity practice must become more layered and complex (unfortunately) as well. Additionally, offering deeper cybersecurity services will soon become a "table stakes" for businesses looking for an MSP.

Yes, solid cybersecurity services can help you make more money, but the lack thereof can make you lose money. For example, if you or a client suffers a significant cybersecurity attack, your business and reputation will likely suffer as well. It could even mean a complete loss of a business for you or a client, depending on risk tolerance.

It's not always reasonable or affordable to hire more people to fill in the gaps, especially with the high demand for cybersecurity talent. That's why more cybersecurity automation and the addition of an outside SOC have become an important goal for many MSPs. SIEM with a SOC not only automates a large chunk of threat detection, but it can also prevent, detect, and monitor cyberthreats better and faster than a human-only team.

SIEM can help you:

- Add more layers of protection (security works best in layers) to reduce risk and vulnerability
- Maintain standards to help clients stay compliant to a wide range of regulatory needs across several industries and specialties
- Protect highly valuable data for yourself and all clients, especially those with low-risk tolerance
- Be more insurable when cyber insurance is required for compliance
- Build an additional revenue stream with more robust cybersecurity services

CHAPTER 3: WHAT MSPS SHOULD LOOK FOR IN A SIEM

When you're ready to take advantage of the benefits of SIEM, you must make the most of your time and make the right investment for your business. This checklist will help you know what to look for so you can ask the right questions before committing to a SIEM.

- ☐ Multi-tenancy capabilities for easy visibility across your customer base in one console
- ☐ Easy onboarding and adoption for your team that includes enough support to get you up and running quickly
- ☐ Integration to your existing tools to ensure collection of log and events data from all your network devices, systems, applications, and services
- ☐ SOC support for 24/7/365 cybersecurity monitoring and protection, freeing your team to focus on high-value work
- ☐ Threat detection rules that are updated regularly with the latest threat intelligence
- ☐ An accurate alert system that discards false positives, so you only get alerts that require action from your team
- ☐ Log retention with real-time analysis to create historical analytics required for regulatory compliance
- ☐ Normalization of data and context so raw data is presented in a way that's easier to understand, and the context to understand what's happening in the real world
- ☐ DS sensors to add extra visibility into network traffic for better correlation of events
- ☐ A pricing model with predictable costs so invoices are clear and billing isn't a burden every month

CHAPTER 4: HOW TO PREPARE TO LAUNCH YOUR SIEM OFFERING

One of the main benefits of adding SIEM to your toolset is more customer protection. And adding more tools and benefits for your existing clients is always an opportunity to create a new revenue stream. Having conversations with clients about rising prices for rising values can be difficult but planning and preparing internally beforehand can help smooth the way.

First, use a risk-based approach to think through and understand the different use cases that apply to your client base. Document each use case with speaking points about the risks that lead to your decision to add more layers of cybersecurity, including what the consequences could be without SIEM. This kind of preparation will help you have more meaningful conversations with your clients about cybersecurity and the addition of SIEM and other cybersecurity tools to your services.

Second, build a process for how your team will receive and use the insights generated by SIEM. Creating reports about alerts, threat prevention, and quick response is a tangible way to show your customers the daily, monthly, and yearly value of SIEM protection. You may even be able to show customers any vulnerabilities in their business and recommend paid projects and employee training to make their business safer.

And finally, inventory each customer's systems and services, again use a risk-based approach, to help them decide what is the most vulnerable and what must be monitored to reduce risk.

PREPARE FOR SIEM OFFERING

- Identify customer use cases
- Build a process for using SIEM insights
- Inventory customer systems and services

CONCLUSION

MSPs are the first—and often only—line of defense for every kind of business in every part of the world. A single layer of preventative protection has served MSPs well in the past, but prevention alone can't stop threats in an ever-changing cybersecurity landscape. The addition of a SIEM solution is an addition of multiple layers of traditional preventive security and proactive detective security, which means more protection for you and your clients.

The "prevent, detect, and monitor model" of SIEM:

- Ensures faster threat detection and response
- Creates visibility into what's happening with all the elements of your IT ecosystem
- Adds cybersecurity value that can create a new revenue stream with existing and new customers

The challenges and costs related to recruiting and training cybersecurity talent are very real, but you don't need to add more employees to grow your service offerings and protect your clients. The addition of a SIEM solution can give you the breathing room you need to provide a level of service that helps you retain customers and grow your business.

Why ConnectWise for SEIM

Most SIEM solutions are difficult to manage, expensive to deploy, require in-house cybersecurity expertise, and have pricing models that don't make sense for MSPs. The ConnectWise SIEM solution was built specifically for MSPs as a powerful solution to expand your security perspective to both prevention and detection.

The solution includes comprehensive, flexible SIEM software and a highly trained and certified SOC as an extension of your internal team. This combination streamlines safety and cybersecurity across your network without additional full-time employee costs and complicated implementations.

Our SOC helps you directly handle SIEM results as needed, but they do more to ensure all SIEM users have ongoing updates for known and new threats. The team collects cross-organizational knowledge to see what's happening across the whole SIEM-user partner base and apply results into threat feeds in the software. This can save hours of work for any cybersecurity expert on your team and create a greater peace of mind knowing that your clients have more protection than ever before.

ConnectWise SIEM is also a flexible solution, giving you options to:

- **Use the ConnectWise SOC or your own cybersecurity experts**
- **Choose log retention options at three levels—30, 90, and 360 days**
- **Get service level agreements that make sense for MSPs**
- **Use on- and off-premise deployment options**
- **Employ role-based access control to keep data clean and secure**

Contact us for a live Demo! >>ManagedServices@dandh.com