CONNECTWISE

CONNECTWISE EBOOK SERIES

How EDR, SIEM, and SOC Work Together for Ultimate Customer Protection

Build Consistent Cybersecurity Revenue in an Ever-Changing Threat Landscape

Contents

Introduction

Introduction

The lack of information security talent in today's threat landscape has created a challenge for most, if not all, managed service providers (MSPs). You may find it very difficult to hire qualified security technicians and analysts to identify, contain, and mitigate cybersecurity incidents. Additionally, the threat landscape changes daily, so cybersecurity problems keep compounding for you and your customers. On top of all that, your customers may have different threats related to their specific industries, such as financial, retail, manufacturing, and more.

It may feel like a mess, but you can tackle these challenges starting with the resources you have today to build excellent customer protection and consistent cybersecurity revenue. It's vital to offer some form of endpoint detection and response (EDR), security information and event management (SIEM), and a security operations center (SOC) to help protect your customers. These tools can significantly reduce the impact of a cybersecurity incident on your organization and your customers' businesses.

Chapter 1: Use Existing People, Document Processes, and Leverage Technology

You don't have to start from scratch. You already have resources in place today that you can leverage when protecting your business and customers from cybersecurity incidents. Let's step back and take a look.

Your People

Your people are the best line of defense and offense in the battle of cybersecurity. To help them be effective, we must provide them with the "guardrails" or policies and awareness training to perform their duties and spot problems and issues before they turn into full-blown incidents. A properly trained employee is a benefit to your organization and to your customer.

You can say the same for your customers' employees. When you train employees internally and externally, you can identify potential causes for concern earlier simply because more individuals are "looking" for the threat actors. In fact, you might not need to hire more people after adding new cybersecurity policies and awareness training to your process.

Something else to consider: If your people don't have proper guardrails or training, there is a higher level of probability that security incidents will occur and that those incidents will have a high impact on your business.

Your Processes

Documenting and standardizing your processes and procedures is the simplest way to increase security and save money. Why? It creates efficiencies through clear guidelines. When teams and individuals do things their own way instead of using the best practices, it leads to mistakes and shortcuts. These issues are often exploitable and can lead to a cybersecurity compromise, or worse, a full-blown incident.

Yes, it is time-consuming to document processes in the short term, but the benefits far outweigh the time commitment. Documenting process is made manageable when you break it into smaller chunks. First, focus on the most common daily activities, then tackle the one-offs or infrequent tasks. To avoid confusion, give the documented processes to your team when it's completed instead of piece by piece.

Your Technology

Like many things, cybersecurity relies on technology to fill in the gaps and support all the activities necessary to protect an organization. It's not always feasible for a human to perform all the actions required to identify, detect, and contain incidents.

Look to technology to perform specific tasks to reduce processing time and the impact an exploit, compromise, or incident may have on our organization. Traditional antivirus (AV) software is not keeping up with the threat of malware, spyware, and ransomware, to name a few examples. Traditional AV often lacks behavioral analysis such as machine learning or AI that detects what normal and abnormal processing looks like on a system or device. It can continuously monitor and quickly determine if someone or a foreign process has taken over the device.

Chapter 2: How EDR, SIEM, and SOC to Protect Your Customers

Three solutions are vital to protecting yourself and your customers in the current threat landscape—endpoint detection and response (EDR), security information and event management (SIEM), and a security operations center (SOC). Let's go over each one in turn.

EDR

EDR applications provide you and your customer with enhanced behavioral analytics and signatures to spot pesky malware and viruses and stop them in their tracks. In some cases, EDR solutions also use the MITRE ATT&CK® framework to detect and analyze the behavior of the offending code and prevent it from causing harm to the system.

EDR can restore the system to pre-event status if the payload impacts a system. This is unlike traditional antivirus, which can only quarantine and attempt clean up. This often leads to components of the payload remaining on the system, requiring further analysis and remediation by a technician.

There are also a few more versions of EDR that you may have heard of recently. The first is "managed detection and response" (MDR). Typically, this is an EDR with included managed services. The second is "extended detection and response" (XDR), which often includes NOC or SOC services or other enforcement mechanisms using automation.

In all cases, when talent is hard to come by or cost-prohibitive, leveraging existing staff and implementing the right tools gives you the ability to do more with less. Adding EDR, along with other captured events, makes it nearly impossible for a threat actor to find a misconfiguration or another potential vector for exploit or compromise inside your organization.

SIEM

An EDR-type solution is only part of the equation service providers need in their technology stack. Security information and event management (SEIM) is a very complementary application with EDR.

SIEM helps take the guesswork out of every event coming into many consoles every minute of every day. This is important because your staff is busy taking care of other issues and does not have the time to correlate all incoming events to look for the proverbial needle in the haystack. A SIEM is designed to bubble the important events to alert your team as quickly as possible (mean time to detection-MTTD), so they can focus on containment and stop the threat from encrypting, exfiltrating, exploiting, or compromising your business or your clients.

Remember, a SIEM can also process other data types, not just log information. The more information like users, assets, threats, and vulnerabilities ingested into the application, the better the analysis of what is happening in your environment. The more information a SIEM can bring together, the more accurate the analysis, including a faster mean time for detection leading to containment and lower risk for the organization. This is where a really good SIEM can shine if you're struggling to find resources with cybersecurity experience. After all, your customers are looking to you for the best protection you can provide against threats to their organization.

SIEM applications vary, so it's wise to evaluate all the products in this space to ensure they meet your organization's needs. First, depending upon the number of events and the period of time you need to keep them

in storage, consider the amount of disk space you need locally or in the cloud and ensure this storage is scalable without manual intervention. Second, if you are considering the cloud for this storage, look at the cost associated with the amount of data inbound to the cloud network since most cloud providers charge for this. Last, ensure the SIEM solution you pick for your business has the performance and redundancy to keep up with growth as you add more customers and their devices into the event capture. Choosing the right solution with a forward-thinking mindset will save you time, energy, and a massive headache.

SOC

Even when EDR and SIEM are in place, people must still be part of the equation. That's where onboarding an outside SOC comes into play. Most MSPs believe they can build a SOC, which they probably can, but it's not always the right answer. In reality, the cybersecurity talent gap presents two challenges that make building your own SOC impractical and costly.

First, the cost of hiring a single SOC analyst, even a junior one, is often cost-prohibitive for the average MSP owner. On average, a junior analyst commands a salary of $60-80K per year. You may be saying to yourself, "No way! I don't believe it. I can find someone cheaper." And maybe you can. But with a quick check on Glassdoor, most junior analysts make $59–87K per year. Some even reported a cash bonus ranging from $400 per year to $10K per year. Pause for a second. Those numbers are for one junior analyst. The reality is you likely need senior staff that can provide more in-depth analysis too. A senior analyst's pay range is $75-151K per year, not including bonuses or benefits packages. Additionally, single staff members, junior or senior, cannot provide cybersecurity support 24/7 or even 8/5. Depending on how much SOC coverage will best serve your customers, you might need to hire a large, expensive staff, which can make the cost of a SOC cost-prohibitive to your customers as well.

This cost analysis doesn't even consider the platform or application licensing expenses or the required infrastructure and automation needed to run your SOC operations effectively and efficiently. You will also need to invest in productivity and automation tools to assist the staff in weeding through all the events from disparate data sources across multiple customers. In addition to the tools, you will need storage and lots of it, enough to handle a minimum of six months' worth of events, if not a year. A bad actor can sit inside an environment and go undetected for long periods, just like the incident at SolarWinds.

Simply put, when you bring on an outside team, you can have a 24/7 SOC with plenty of qualified, experienced staff at an affordable price, including white-label capability. A SOC team can also act when you cannot; it's a huge benefit most MSPs do not think about. Imagine telling a customer or a prospect that you have the capability not only to detect that something is going on, but you can also detect it and stop the threat when no one is in the office.

There are plenty of SOC services to choose from, so it's essential to do your research, including asking your peers who they use. Here's a list of questions you can ask your peers:

- Are you happy with your vendor partner, or are you running into challenges?
- Can your SOC service ingest all the events from the different systems and devices, including the internet of things (IoT) and operational technologies (OT)?
- Are they SOC2 and ISO compliant, or have other compliances?
- If they are also providing your SIEM solution, does it offer the redundancy and performance necessary to meet or exceed your requirements?

Conclusion

At the end of the day, your customers are looking for your help to keep their businesses as safe as protected as possible so they can sleep at night. Helping them move beyond a firewall and traditional antivirus to a managed EDR solution for enhanced behavior analytics, SIEM to correlate and detect exploits and compromises or malicious activities, and SOC to help you analyze all those events and take appropriate actions is a sure-fire way to build consistent cybersecurity revenue and help everyone get a good night's sleep.

Dive deeper into the software solutions available at ConnectWise

Cybersecurity SOC, SIEM & SecOps: How they work together

Read the Blog >

Evolving Your Cybersecurity Tech Stack

Watch the Webinar >

ConnectWise Fortify live demo

Watch the Demo >