CONNECTWISE

CONNECTWISE EBOOK SERIES

SIEM vs EDR:

WHY USING BOTH GIVES YOU A MORE COMPLETE PICTURE OF CYBERSECURITY THREATS

CONTENTS

Introduction 3
Chapter 1: What is SIEM technology and how would you use it? 4
Chapter 2: What is EDR technology and how would you use it? 6
Chapter 3: A quick comparison of capabilities: SIEM vs EDR 8
Chapter 4: How SIEM and EDR help TSPs protect clients more effectively 9
Chapter 5: Develop a more complete security picture with SIEM and EDR 10

Introduction

SIEM and EDR are acronyms that get kicked around a lot in discussions about cybersecurity, but what do they really mean? More important, what do these technologies do—and do you need to have both in the security technology stack your organization relies on every day for protection?

You'll get answers to these questions and more in this eBook. It offers a quick primer on SIEM and EDR to help demystify these terms. It also highlights the differences between—and underscores the value of—these different but complementary security controls in the following sections.

Chapter 1: What is SIEM technology and how would you use it?

A security information and event management (SIEM) system collects log and event data that an organization's network devices, systems, and applications and services generate. It then brings all that information together into one platform. A SIEM provides security teams with greater visibility into what's happening with all the elements in the IT ecosystem through a "single pane of glass."

Technicians use automation to run the data in the SIEM against various prebuilt security rules. They can swiftly navigate through all the "white noise" from these various data sources—which include everything from web servers to hypervisors—to identify real and actionable events.

The SIEM serves as a critical layer in an organization's technology stack because it amplifies threat detection. With a SIEM, you can learn very quickly if a malicious actor has breached your traditional perimeter defense, so you can move fast to respond.

SIEM: An old tool made better by the cloud

SIEM technology is by no means new; it's been around since 2000. And over time, it's become a fundamental tool for a Security Operations Center (SOC) to provide 24/7/365 monitoring and logging of security event alerts. SIEM helps security teams focus on identifying, analyzing, and responding to the threats and other alerts that matter most.

Today's next-generation, cloud-based SIEMs make it easier for technology service providers (TSPs) to provide SIEM capabilities—including visibility—to their clients. When you work with a SOC using a modern SIEM solution, you can typically get full access to view your alert data. And your team can work right alongside the technicians in the SOC to identify and address critical issues as quickly as possible.

What are some use cases for SIEM technology?

An organization that wants full visibility into its entire IT infrastructure will adopt a SIEM platform, or it will work with a TSP that provides SIEM capabilities as part of its cybersecurity offerings. With advanced SIEM technology, security teams can:

- **Conduct strategic detection:** Today's SIEM solutions can provide real-time visibility into security threats, like malware or suspicious network traffic, impacting network devices, systems, and applications and services. Security teams can use SIEM technology to stay focused on the organization's most critical IT assets and prioritize the response to any alerts related to them.
- **Analyze event data:** Security teams can use SIEMs to analyze event data in real time; this increases the ability to detect threats early, including advanced threats and targeted attacks. The "single pane of glass" view a SIEM provides also helps teams to hunt proactively for threats across the entire organization and shift away from a reactive approach to cybersecurity
- **Enrich logs:** Event logs from security controls like endpoint solutions, web filters and firewalls, as well as from other devices like routers and from applications, offer a wealth of information about potential threats. But they need to be enriched—that is, given more context—to be understood. An example of this process is enriching a log that contains IP addresses with relevant geolocation data for those addresses. A leading SIEM platform can be integrated with other systems using APIs to collect and correlate event and non-event data for enriching logs.
- **Meet compliance requirements:** Real-time correlation and analysis of data, plus data retention and report automation, make it easier for businesses to stay in compliance with mandates like the Health Insurance Portability and Accountability Act (HIPAA) and Payment Card Industry Data Security Standard (PCI DSS).
- **Accept data from many sources in the network:** Because a SIEM has access to multiple and diverse sources of data in an organization's IT ecosystem, and it offers visibility into event data through a single pane of glass, security teams can gain a much better picture of what their various security tools are "seeing" and reacting to. That gives them more insight into potential threats, including their severity and what they're targeting in the network.

Chapter 2: What is EDR technology and how would you use it?

As its name suggests, endpoint detection and response (EDR) solutions are endpoint-focused security technology. Endpoints essentially served as gateways to a network. They include hardware devices such as desktops, smartphones, Internet of Things (IoT) devices, and servers—and they are all prone to vulnerabilities. Malicious actors target endpoints relentlessly in hopes of infiltrating the network.

Like SIEM technology, EDR technology isn't new—although the term "endpoint detection and response" was only coined in the past decade. EDR technology, also like SIEM, can serve as a critical layer in an organization's security technology stack. But EDR solutions don't look at the entire network like SIEM tools do. An EDR solution monitors and collects data about endpoint activity and analyzes it to determine what activity is normal—or not.

Many EDR tools are agent-based, meaning they require the installation of software or a sensor on an endpoint device to enable monitoring and data gathering. This software is what allows EDR tools to provide advanced and comprehensive threat detection and response.

AI and ML accelerate threat identification and response

Modern EDR solutions are cloud-based and use artificial intelligence (AI) and machine learning (ML) for behavioral analysis and threat detection. They can continuously monitor each running process and map it to malicious behavior and quickly identify the root causes for those behaviors by diagnosing corrupt source processes and system settings. Leading EDR tools can also recognize virus and malware variants.

When an AI-driven EDR platform identifies a threat, it can automatically respond to block, remove, or contain the threat and notify security staff so they can investigate the threat further, if needed. Leading EDR tools also provide forensics and analytics capabilities that allow security teams to research identified threats and even search for suspicious activities through threat hunting.

Today's cloud-based EDR tools are easy to integrate with other systems, manage, and keep up to date. Because endpoints are under constant attack by an ever-changing array of threats with varying degrees of severity, many organizations outsource the work of triaging EDR alerts and remediation to a SOC provider, rather than burdening their IT personnel or hiring more security talent.

What are some use cases for EDR technology?

An organization that wants to detect and assess suspicious activity on the endpoints that can access its networks will implement an EDR solution, or work with a TSP that provides EDR capabilities as part of its cybersecurity offerings. With advanced EDR technology, security teams can:

- **Benefit from vendor-driven analysis:** An EDR platform can collect data from endpoints and transmit it back to the vendor for analysis. If the data is determined to be a threat, the vendor will block the threat and create an alert. Security administrators can typically view these alerts in the dashboard for the EDR solution and decide how to respond. Importantly, vendors can also identify false positives, so security teams don't waste time chasing threats that aren't real.
- **Use rollback capabilities:** A modern EDR tool can provide advanced visibility into devices. And in the event of a threat, they can quickly roll back files to previous safe versions through tracking changes in the devices and restoring them to an acceptable risk state. Rollbacks remediate the damage done to endpoints by attacks from threats like ransomware.
- **Query endpoint data quickly:** Security teams can swiftly search information collected by the EDR platform to understand the risk and scope of threats. And they can search the EDR database for indicators of compromise. They can also directly query endpoints in real time.
- **Contain threats at the endpoint:** EDR tools use event and behavior analysis to detect threats, whether those threats are known or zero-day vulnerabilities. If an event is found to be suspicious—either immediately or at a later time—the EDR platform will stop running processes to contain the threat, block further events, and alert the security team. This quick action at the endpoint level is critical for containing fast-moving threats like ransomware.
- **Control and monitor device use:** Advanced EDR platforms allow organizations to control what the devices connected to their network—including USB and wireless Bluetooth devices—can access while on the network. They can also monitor how those devices are being used while they are active in the IT environment.

Chapter 3: A quick comparison of capabilities: SIEM vs EDR

SIEM

- Sees the "whole picture" of a network
- Detects events based on data input
- Provides some automatic response, depending on integrations
- Offers massive detection capabilities
- Useful for analysis and compliance
- Not typically used for threat prevention

EDR

- Focuses only on endpoints
- Detects events on endpoints (e.g., file written, file executed)
- Responds to threats either automatically or with security team intervention
- Features built-in machine learning and behavioral analysis capabilities
- Allows cybersecurity experts to proactively threat hunt across endpoint devices
- Protects endpoints even if they're not on the network

Chapter 4: How SIEM and EDR help TSPs protect clients more effectively

Leading TSPs know that prevention isn't enough to stop all threats. For example, EDR solutions are limited in their ability to detect and deflect highly sophisticated fileless malware. This malware is dangerous, as it exploits vulnerabilities that can give attackers administrative control and the ability to gather data to use in future attacks—like a highly targeted phishing attack.

The fileless malware threat is just one reason more TSPs are starting to use advanced SIEM and EDR platforms together. Adding these layers of advanced defenses to their security technology stack help TSPs develop a more complete picture of the threats targeting their clients—in real time.

With EDR, TSPs can detect, block, contain, and remediate the threats targeting their clients' endpoints faster. They can also analyze and investigate these threats, and if needed, roll back files to "safe" versions. And SIEM technology helps TSPs protect their clients more effectively by providing full visibility into an organization's IT infrastructure and collecting data from multiple sources for analysis. That helps security teams catch events when prevention measures fail.

Also, companies that need to meet compliance and regulatory mandates can benefit from the log capture, retention, and review capabilities in a modern SIEM platform. Clients with highly valuable data, like sensitive financial information and intellectual property, are better protected, too, because SIEM technology can highlight unusual activity related to the systems and devices storing that data.

The value for companies working with a TSP that provides these additional layers of security—aside from being better protected from the latest threats and malicious actors—is the ability to leave this defensive work in the hands of experienced experts who can focus on alerts and threats 24/7/365. They can keep their own security resources focused on high-value work. Also, they don't need to worry about finding, hiring, and retaining more security talent to help them make sense of the constant "white noise" coming from SIEM and EDR tools.

Chapter 5: Develop a more complete security picture with SIEM and EDR

SIEM and EDR are two technologies that, when used together, can help organizations gain a more complete picture on the state of their security. One technology is not a substitute for the other; think of SIEM and EDR as complementary controls.

They are also an important part of an organization's overall security strategy, which includes employing an array of other security controls (technological, physical and logical), adopting best practices and leading frameworks, implementing and enforcing effective policies, creating and testing business continuity management plans, providing relevant end user training, and much more.

Even though a SIEM solution can cover for instances when threat prevention fails, a well-designed EDR platform should still outperform a SIEM tool in prevention. EDR technology should also make it simpler for security teams to react to events.

Likewise, a well-designed SIEM platform should outperform an EDR tool in detection. And it should make it easier for security teams to sift through multiple data sources. Additionally, it should support log enrichment and provide more context about potential threats.

A case for complementary tools

So, what can happen when you don't have EDR and SIEM tools in your technology stack, working together? Consider the following real-world example of a missed opportunity to contain a threat fast:

> An organization's web servers were hit with web shells—malware that enables remote access and control—leading to defacements.
>
> The organization had an EDR platform. But because that tool can only detect when something happens on the endpoint, like the execution of a file, it only detected the threat and triggered an alert *after* the attacker tried to escape the website.
>
> If the organization had an advanced SIEM platform in place, its security team could have detected the malicious traffic as soon as the initial exploit occurred and moved quickly to reduce its impact.