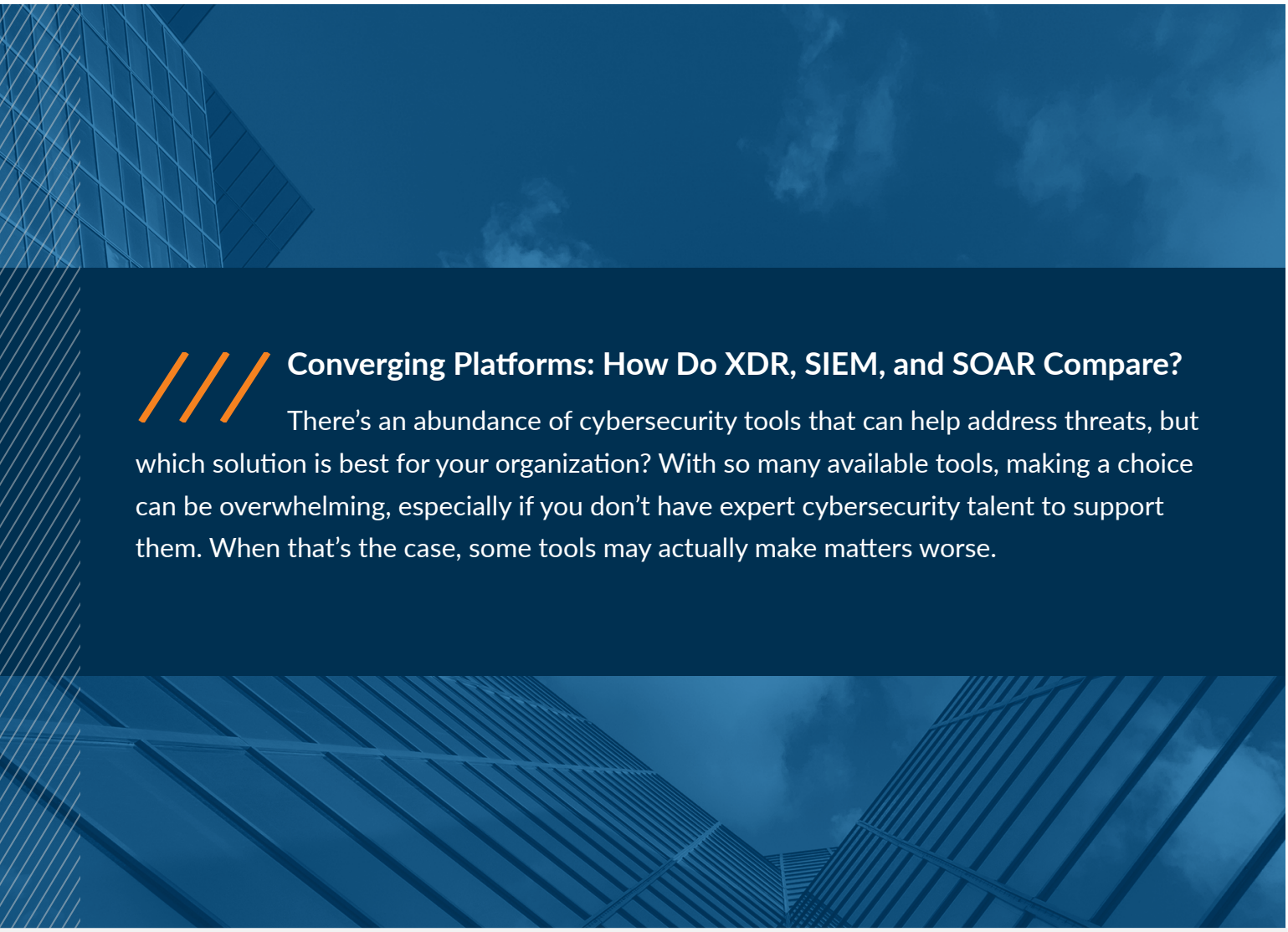
ARCTIC WOLF

END CYBER RISK

WHITE PAPER

Converging Platforms: How Do XDR, SIEM, and SOAR Compare?



Converging Platforms: How Do XDR, SIEM, and SOAR Compare?

There's an abundance of cybersecurity tools that can help address threats, but which solution is best for your organization? With so many available tools, making a choice can be overwhelming, especially if you don't have expert cybersecurity talent to support them. When that's the case, some tools may actually make matters worse.

A strong cybersecurity program combines the best and most appropriate technologies with a team of dedicated security professionals that have the expertise and experience to wield them effectively.

This guide discusses the emergence of extended detection and response (XDR), and how it compares to security information and event management (SIEM) and security orchestration, automation, and response (SOAR) toolsets.

We also take a close look at the critical role played by security analysts and discuss why the success of any tool depends heavily on these analyst's skills and effectiveness.

The Need for Converging Technology

Almost every form of security technology aims to address a specific pathway exploited by attackers. For example, the goal of antivirus software is to detect and prevent the introduction of viruses onto a user's device. In a similar vein, endpoint detection and response (EDR) solutions focus on the device as a common attack vector, while network traffic analysis (NTA) tools scrutinize a company's network traffic for signs of malicious activity.

As each form of technology appeared, it solved a discrete problem. Antivirus solutions are not superior to EDR or NTA, nor are they inferior. These solutions complement each other. They address different threat vectors, and all are necessary components of an effective security program.

Because each tool addresses a specific need, supporting these disparate tools requires different expertise provided by separate analysts. The more tools a company adopts, the greater the burden on its security operations to manage, maintain, and optimize their performance.

Siloed technology can force analysts to further specialize and dedicate large portions of their time to overseeing relatively few security tools. Yet, when new security solutions become available, analysts are often expected to manage these new tools too and be able to manually assimilate and interpret ingested data.

The conflict between the need to specialize and the broadening scope of solutions often results in an overinvestment in tools and a lack of the expertise to fully support them.

To address the issue of too many separate tools, cybersecurity technologies were developed to connect them in a comprehensive solution. These "next-generation" solutions combine telemetry and tools into single consoles or "panes of glass" for the security team to view all activity in its IT environment.

Combining relevant data into single consoles minimizes the time analysts spend moving between platforms. It also makes it easier to correlate the data and develop subsequent steps appropriately.

LET'S LOOK AT XDR, THE MOST RECENT SINGLE CONSOLE TO ARRIVE IN THE MARKETPLACE—AND LET'S SEE HOW IT'S DIFFERENT FROM SIEM AND SOAR.

What Is XDR?

Extended detection and response is a relatively new concept in the security world, so there are several definitions of XDR floating around. Currently, Gartner defines XDR as *"a security threat detection and incident response tool that natively integrates multiple security products into a cohesive security operations system that unifies all licensed security components."*

Gartner's definition indicates how XDR solves challenges many organizations face. Whereas individual solutions lack integration, XDR is attractive to businesses because of the integration of multiple security products, resulting in a more cohesive approach to security operations.

Instead of providing analysts with multiple solutions, each with its own unique view of the organization's data, XDR provides a single, comprehensive view that captures multiple solutions all at once. As XDR becomes commonplace and evolves, its approach may vary widely between security providers.

Regardless of how a provider structures an offering, XDR should provide:

- Endpoint visibility and response actions
- A view into all networks across the organization
- Support for log ingestion, leveraging existing tools and technology
- Insight into cloud-based data
- An overview of discrete solutions, such as authentication applications
- An ability to correlate data to detect suspicious activity appearing in one or more data feeds
- An open-ended platform that allows for the integration of future technologies

Because the detection and response actions take place in a single console, analysts can make faster and more informed decisions. Unlike having to rely on the limited activity that takes place on an endpoint, XDR brings in telemetry that also allows analysts to see and make connections on the activity that takes place between endpoints.

While technology forms the basis for XDR, as with any tool it is only effective when overseen by qualified security operations experts who can extract the greatest intelligence and value from the solution.

How XDR Stacks up Against SIEM

XDR and SIEM share several similarities. Both approaches aim to collect data from across the enterprise to enable real-time event analysis.

However, critics of SIEM view this approach as being overly focused on gathering and correlating data, and triggering alerts. This makes SIEM inherently noisy, which can easily inundate and overwhelm security teams that are oftentimes already stretched thin. And by requiring analysts to make the connections buried within the data, there's an increased risk of costly errors and choke points, both of which can lengthen an organization's response time.

Frequently, legacy SIEM solutions lack necessary built-in response capabilities.

In contrast, XDR centralizes incident response and can control individual security products when needed. Threat detection takes a different path, too. Analysts using SIEM solutions typically create alerts and hunt for and ingest relevant threat intelligence data feeds, whereas with XDR, the solution analyzes data to identify incidents.

Many organizations also find SIEMs difficult to install and tune, which leads some to engage professional service firms to optimize the platform. It can require one or more dedicated analysts to run the technology platform. Because XDR is typically delivered via SaaS, deployment takes less time and is more flexible.

A critical weakness of SIEMs is that their performance depends on the quality and integrity of the data it receives.

If a company cannot create, maintain, and ingest high-quality logs, the SIEM cannot rectify the shortcomings in the data. To address this weakness, a security team provider can help organizations review existing logs and identify which data points will provide the most value.

Because XDR is a new technology that is not yet standardized, log usage varies quite a bit. Before selecting an XDR solution, security departments should understand how the security provider views the use of logs. A centralized, searchable repository of logs can provide a security team with visibility over its IT environment, which helps to streamline the process to uncover and respond to cyberthreats.

A key strength of XDR is how it enables a deep analysis of several high-quality data sources to deliver more accurate detection with less noise, resulting in a faster, more effective response to security threats.

How XDR Compares to SOAR

SOAR is another technology designed to combat the problems with multiple, disjointed security solutions. Like SIEM, SOAR ingests and analyzes data and incorporates telemetry from disparate tools in a single location.

Companies can rely on discrete threat detection technologies, or chain them together to improve—and potentially automate—the organization's response.

However, automation requires integration. Analysts must also correlate data and ensure the automated responses are appropriate.

Like SIEM, certain SOAR solutions can result in alert fatigue.

Since XDR collects and correlates data from multiple security solutions, security teams receive fewer alerts, and those they do receive are generally of higher quality.

While automation can provide numerous benefits, it requires some degree of oversight to perfect the approach and ensure it functions as designed over the long term.

It can also create a false sense of security, particularly when organizations embrace automation to such an extent they become disconnected from the activity that takes place in their environment.

Since XDR typically includes artificial intelligence and machine learning technologies, automation can prove efficient and effective, especially when augmented by humans.

XDR Considerations

Before embracing XDR, organizations should realize that extended detection and response is still evolving and that no two solutions are the same. In addition, it's important to consider the merits of this relatively new approach compared to SIEM and SOAR solutions.

Given that XDR relies on a single platform, incorporates telemetry from across the enterprise, correlates data quickly to deliver high-quality alerts, and leverages machine learning and artificial intelligence, it solves many of the shortcomings of legacy solutions.

However, like its predecessors, XDR does not function without skilled security analysts, who can make the difference between a solution serving its purpose to protect the organization or providing false hope while keeping the business remains exposed to unmitigated risk.

Regardless of the approach your organization pursues, remember that an effective cybersecurity program requires skilled and experienced people. Technology alone is never enough.

How Arctic Wolf Can Help

As anyone with knowledge of the cybersecurity sector knows, there's no shortage of tools for companies to embrace. However, there's undoubtedly a shortage of cybersecurity professionals who possess sufficient talent and training to ensure those tools deliver on vendors' promises.

The most technologically adept and advanced tools will not solve the perplexing cybersecurity problems facing organizations today if there aren't skilled and experienced analysts to support them.

Arctic Wolf's approach does not rely on a single technology. Instead, our platform integrates with an organization's existing cybersecurity tools. The Concierge Security® Team assigned to your account features high-performing security operations professionals who can help catapult your organization's security posture to a new and sustainable level of effectiveness and performance.

Learn more about our security operations approach.

About Arctic Wolf

Arctic Wolf® is the market leader in security operations. Using the cloud-native Arctic Wolf® Platform, we help organizations end cyber risk by providing security operations as a concierge service. Highly trained Concierge Security® experts work as an extension of your team to provide 24x7 monitoring, detection, and response, as well as ongoing risk management to proactively protect systems and data while continually strengthening your security posture. And we now provide managed security awareness training to better inform and prepare your employees about security best practices and how to effectively respond against social engineering attacks.

For more information about Arctic Wolf, visit arcticwolf.com

Contact Us

arcticwolf.com
1.888.272.8429
ask@arcticwolf.com