Understanding the Differences Between SIEM, SOAR, Managed SOC, MDR, EDR, NDR and XDR

With SIEM & MDR: What You Need to Know

Mar, 2024

Gain Insight Into Which Technology is Right for You

---

https://www.idagent.com/blog/understanding-the-differences-between-siem-soar-managed-soc-mdr-edr-ndr-and-xdr/

https://www.criticalstart.com/siem-mdr-what-you-need-to-know/

Collected by: Mohammad Alkhudari

LinkedIN: https://www.linkedin.com/in/alkhudary/

Cybersecurity is one of the fastest-growing entities in today's digital-first business landscape owing to the sharp uptick in the number of cyberattacks over the past few years. IT professionals know all too well just how relentless and sophisticated cyberattacks have become, especially with the adoption of AI-based tools, like ChatGPT and WormGPT, to launch effective phishing campaigns and create malicious code faster.

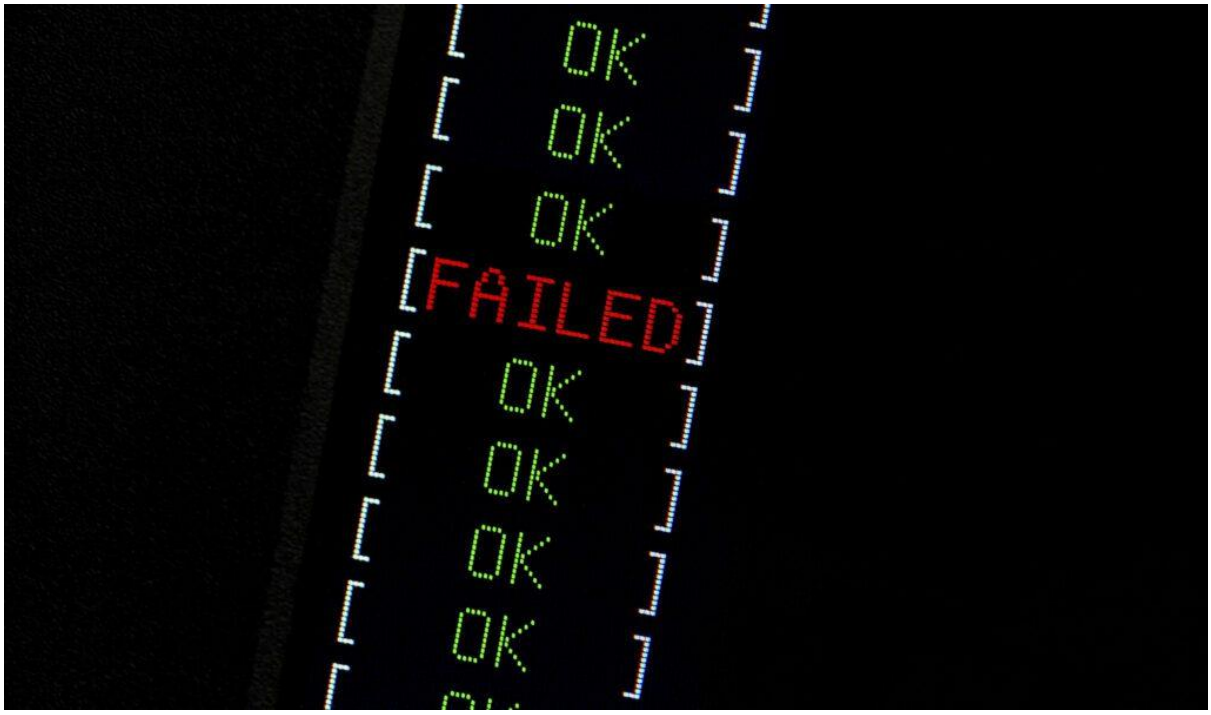
The growing concern for this widespread increase in cyberattacks and their implications has created a need for robust IT solutions to combat cybercrime. While that sounds like a simple enough task, accomplishing it is a whole other ball game. There are literally thousands of security solutions in the market, many utilizing variations of similar technologies. That can make it extremely difficult for an organization's IT decision-makers to make a smart choice. To help you make the best decisions and achieve all your IT security goals hassle-free, this blog will explain everything you need to know about six common security technologies.

Six Powerful Cybersecurity Solutions

Sometimes, distinguishing between the specific roles of solutions like, for example, security orchestration, automation and response (SOAR) and endpoint detection and response (EDR), can throw IT professionals off, which doesn't really bode well for an organization's overall security posture.

Listed below are the six different kinds of security solutions IT pros should be fully familiar with before making any cybersecurity-related decisions.

1. **Security information and event management (SIEM)**
2. **Security orchestration, automation and response (SOAR)**
3. **Managed security operations center (SOC)**
4. **Endpoint detection and response (EDR)**
5. **Network detection and response (NDR)**
6. **Extended detection and response (XDR)**



Understanding SIEM, SOAR, managed SOC and MDR

Let's begin with SIEM, SOAR, managed SOC, EDR and NDR, some of the most often used security technologies available today.

Security information and event management (SIEM): SIEM is a comprehensive solution designed to collect, analyze and interpret log data from various sources across an organization's entire IT infrastructure. It provides real-time insights into security events, aiding in the early detection of potential threats.

Data collection, normalization, parsing, correlation engines and customizable dashboards are the main components of SIEM. These components collectively empower SIEM to excel in threat detection, incident response, compliance management and forensic analysis. It helps IT professionals centralize visibility, detect threats early, carry out efficient incident response and streamline compliance management as well.

Security orchestration, automation and response (SOAR): SOAR integrates various security tools and technologies to quicken and automate incident response processes. It's a multifaceted approach to enhance the efficiency of

security operations by orchestrating workflows and automating repetitive, redundant tasks. SOAR systems bring together threat intelligence, case management and automation to create a cohesive and synchronized response to security incidents

Its three components — orchestration, automation and response — enable the coordination of disparate security tools, reduce manual intervention in routine tasks, and ensure a swift and synchronized reaction to security incidents. SOAR helps increase operational efficiency, accelerate incident response times, reduce workload on security teams and enhance overall cybersecurity resilience.

Managed security operations center (SOC): Also known as a Managed Detection and Response (MDR), a managed SOC is a security service through an external partner, offering 24/7/365 monitoring, threat detection and expert incident response. Managed SOC services provide cost-effectiveness and scalability, making them an ideal choice for organizations managing security for multiple clients like MSPs or IT professionals without deep cybersecurity knowledge. Choosing a managed SOC also frees an MSP or business from the cumbersome process of finding (and paying for) cybersecurity specialists during the ongoing talent shortage. With round-the-clock monitoring by a team of security experts, managed SOC ensures continuous monitoring with the ability to adapt to evolving threats, so as not to bog down an MSP with alerts.

Partnering with a third party requires IT professionals to relinquish a certain amount of control but also streamlines their ability to scale and offer the service immediately to clients without dealing with the many challenges that standing up your own SOC creates.

See the challenges companies face & how they're overcoming them in our Kaseya Security Survey Report 2023 DOWNLOAD IT>>

All about advanced threat detection and response with EDR and NDR

With cybercriminals growing increasingly tenacious in their attempts to disrupt businesses globally, cybersecurity professionals, too, are strongly focusing on strengthening their defenses with these advanced threat detection and response solutions.

Endpoint detection and response (EDR): EDR solutions focus on securing individual devices within an organization's network. They are designed to provide real-time visibility into endpoint activities, enabling organizations to detect, investigate and respond to advanced threats. By monitoring and analyzing activities on computers, servers and other endpoint devices, EDR helps organizations fortify their security posture and swiftly respond to potential security incidents.

EDR solutions include a unique combination of continuous monitoring, behavior analysis, threat detection and automated response. They are built to actively monitor endpoint activities while analyzing patterns and behaviors to identify potential insider threats. They also provide detailed insights into the activities of

individual devices, facilitating rapid detection of malicious behavior. Combining EDR with a managed SOC is a winning move to ensure comprehensive visibility and threat detection.

Network detection and response (NDR): NDR actively analyzes network traffic to detect and mitigate malicious activities. By employing advanced analytics and machine learning, NDR solutions provide organizations with the means to identify and respond to threats that target their network, ensuring comprehensive protection against a wide range of cyberthreats.

NDR comprises packet capture and analysis, anomaly detection, threat intelligence integration and real-time monitoring. These solutions actively inspect network traffic, identifying patterns and anomalies that may indicate malicious behavior and play a pivotal role in detecting network-based attacks, lateral movement and data exfiltration.

Follow the path to see how Managed SOC heroically defends businesses from cyberattacks. GET INFOGRAPHIC>>

A comprehensive security framework: Extended detection and response (XDR)

A newer arrival to the cybersecurity space, XDR solutions are built upon the foundations of EDR, recognizing the limitations of solely focusing on endpoint security. While EDR primarily addresses threats at the endpoint level, XDR takes it a step further by integrating data from diverse sources, including endpoints, networks and cloud environments. This evolution acknowledges the interconnected nature of modern IT environments and the need for correlating information across disparate security layers for a comprehensive and effective threat detection and response strategy.

An XDR approach empowers organizations with enhanced visibility by providing a consolidated view of security events across endpoints, networks and their cloud environments, enabling precise threat detection. Secondly, XDR facilitates a coordinated and effective response to incidents by correlating data and automating response actions. Lastly, XDR supports a proactive security stance, allowing organizations to stay ahead of evolving threats by leveraging advanced analytics and threat intelligence. Choosing XDR can be a strategic move towards a more interconnected and adaptive security framework that may be beneficial to businesses with certain industry requirements.

Explore the nuts and bolts of ransomware and see how a business falls victim to an attack. GET EBOOK>>

5 Things to consider when selecting your ideal security solution

While each of these security solutions — SIEM, SOAR, Managed SOC, EDR, NDR and XDR — offer many benefits in improving cyber resilience, one common downside across many of these solutions is the potential for high implementation and operational costs. Deploying and maintaining these sophisticated security measures often requires a significant investment in terms of both financial resources and skilled personnel.

Small to medium-sized enterprises, in particular, may find the cost of acquiring, implementing and managing many advanced security solutions to be a

substantial barrier. Implementing many of these technologies creates additional burdens like hiring skilled personnel, paying for ongoing training and staying on top of frequent updates to keep pace with evolving threats. In today's challenging economy, IT decision-makers must tread carefully when it comes to adopting any of these advanced technologies.

Here are five important factors to consider before choosing a security solution.

- **Organizational needs and objectives:** Consider your organization's specific cybersecurity needs and objectives. Different solutions address different security concerns, and some solutions may not be ideal for a company's purposes. Make sure the chosen security technology aligns with your organization's strategic IT goals now and ensures that you're future-ready.

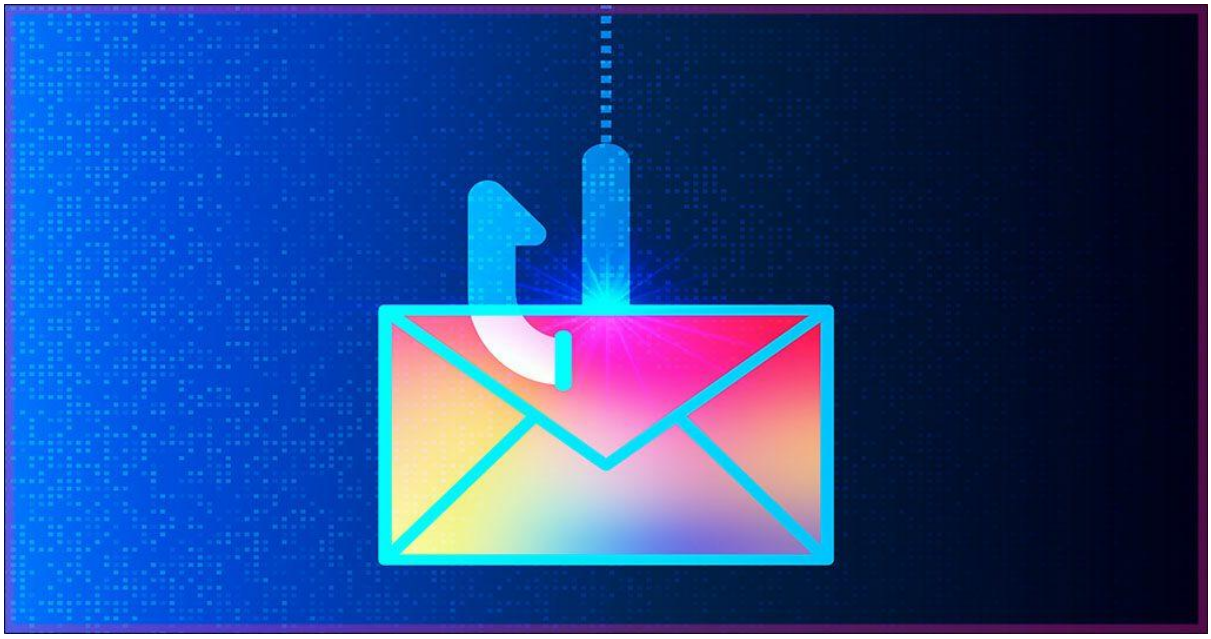
- **Scalability and flexibility:** Assess the scalability and flexibility of the security solution. Ensure that it can adapt to the evolving needs of your organization as it grows as well as the demands that will be placed upon it now and in the future as cyber threats evolve. A scalable solution can accommodate increased data volumes and expanding network infrastructure, while flexibility allows for integration with existing and future technologies.

- **Integration and interoperability:** This is extremely important, especially considering how problematic legacy systems are. The compatibility of the security solution with your existing IT infrastructure and other security tools can ensure seamless integrations and a cohesive security environment, preventing silos of information and enhancing the overall effectiveness of the cybersecurity strategy.

- **Ease of use and management:** An intuitive interface and streamlined management processes contribute to the efficient operation of the solution. If the technology you choose requires specialized security expertise, hiring and training requirements for the security team should also be taken into account. Alternatively, some choices like a smart managed SOC may clear many obstacles from the board at once, making it easy for you to gain major security advantages without a major hit to your budget.

- **Cost-benefit analysis:** Perform a thorough cost-benefit analysis, taking into consideration upfront expenses and ongoing operational costs. Evaluate the total cost of ownership, including licensing fees, hardware,

training and maintenance, and make sure that the solution you choose provides a positive ROI.



What cybercriminal tricks do employees fall for in phishing simulations? Find out in this infographic. GET IT>>

RocketCyber Managed SOC is Your Ideal Cybersecurity Partner

RocketCyber Managed SOC is the most advanced managed SOC on the market, offering compatibility, a combination of advanced threat detection and response and seamless integration with your professional services automation (PSA) system. Gain access to world-class cybersecurity talent without a big upfront investment or added payroll cost.

RocketCyber Managed SOC includes:

- **Continuous monitoring:** Round-the-clock protection with real-time advanced threat detection.
- **Expertise on demand:** Get the cybersecurity expertise you need to keep your organization out of trouble without adding to your headcount.
- **Breach detection:** Thwart sophisticated and advanced threats that bypass traditional AV and perimeter security solutions.
- **Threat hunting:** Focus on other pressing matters while an elite cybersecurity team proactively hunts for malicious activities.

- **Actionable intelligence:** Alerts align with the MITRE ATT&CK framework, bringing clarity that enables a fast response.
- **No hardware requirements:** Patent-pending, cloud-based technology eliminates the need for costly and complex on-premises hardware.

To learn more about cybersecurity solutions and how you can strengthen your cyberdefenses, visit www.rocketcyber.com

SIEM & MDR: What You Need to Know

A defense-in-depth security strategy is built upon the premise that no one tool or process is enough to ensure the protection of an organization's entire technology infrastructure.

But if there is one layer that should be considered foundational to any effective cybersecurity strategy, it is Security Incident and Event Management (SIEM).

What Is SIEM?

SIEM is a cybersecurity software that acts as an aggregator and analyzer of many different sources of data across your organization's entire network.

How Does SIEM Work?

SIEM takes the inputs from Endpoint Detection and Response Tools (EDR) and collates it with network log data. It processes it with additional information from a variety of sources through advanced analytics to provide next-level threat monitoring and response capabilities.

And this enhanced visibility is put to best use through a Managed Detection and Response (MDR) model to ensure SIEM's capabilities are fully maximized.

Benefits of SIEM

The convergence of EDR, SIEM, and MDR enables companies to ingest, analyze and act on the thousands of security alerts that pour in from their environment every day.

It provides the data points to gain visibility and translate it into action, combined with the expertise to understand the nature of the attack and formulate the best strategy to contain it.

What to Consider When Comparing SIEM Solutions

But even when utilized through professional services, an organization must have a clear understanding of what it's hoping to achieve if it plans to get the most out of the SIEM platform that it selects.

As an example, think about planning to purchase a new 4K HDTV. As you evaluate your options, consider the following mindsets:

1. I want to buy a tv with the broadest feature set possible, regardless of cost.
2. I want to buy a "cookie-cutter" TV with standard features and a low cost.
3. I want to understand which features and capabilities are most important to me, and then find the right TV with that feature set to give me the most desirable performance for my investment.

Most would agree that option three is the smart choice. And this type of mindset, a targeted approach that matches capabilities to requirements, can be very useful in the world of information security.

When evaluating SIEM, you can use this mindset to determine what attributes have the most security relevance to your organization.

Understanding what you're looking for can provide a roadmap to your SIEM selection and deployment before you even talk to a vendor.

Questions to Ask When Comparing SIEM Platforms

To develop the right mindset going into this process, it's very helpful to ask yourself the following questions.

What's my budget for this project?

Your budget will dictate the types of data you can send to the SIEM platform, how it will be analyzed and will determine the scope of ongoing monitoring.

If you have a limited budget, you can still get started with SIEM by focusing your efforts on the highest visibility per dollar spent.

What types of log retention compliance standards do I need to meet?

Specific types of regulatory compliance require you to not only store log data but ensure this data is tamper-proof.

There can also be a requirement that determines how long logs need to be kept.

What devices throughout my enterprise contain security-relevant/security actionable log data?

The philosophy on “what’s important” is continuing to change to keep pace with how end users work, and how the threat landscape continues to evolve.

User attribution through Active Directory logs (or however a company chooses to centrally enforce policy), VPN logs, SSO, and wireless authentication are all great starting points to consider.

Network threat detection, web proxies, and traditional firewall logs should be the next step.

The sky is truly the limit, as many SIEM vendors process from as few as one hundred log types, expanding all the way up to thousands.

What do I do with these logs that are coming into my SIEM platform?

Now that you have decided what you want to ingest, you must determine how to take action on the information. Not all logs are created equal.

As an example, one log in an active directory stating, “Login Success” for user John Smith may not be an issue. But several denied logins for that same user may possibly indicate a threat.

Also, consider that if U.S.-based user John Smith is able to successfully log in from overseas during non-business hours it may indicate that further action needs to be taken.

How many people will I dedicate or charter to handle alerts from my SIEM platform?

The number of people you need will depend upon how you answered the previous question and is based in part on the level of risk you’re willing to accept.

How long does it take to implement SIEM as part of my incident response program?

With the support of the right MDR provider, many organizations can often stand up SIEM in 6-8 weeks, while in-house implementations can take up to a year.

Generally, the more users that will be consuming the information provided by the SIEM, the longer it may take to stand up.

Benefits of MDR Services

A managed detection and response service can help you answer these questions and match SIEM capabilities to meet those needs.

Flexibility

Businesses need a feature set that can match their unique use cases, but that usually should not extend into an expensive, time-consuming, fully-customized deployment.

An MDR can ensure a successful implementation by analyzing your current environment, threat matrix, and industry demands and then develop a SIEM strategy that places it at the heart of your security operation.

Adaptability

MDR providers structure the deployment so that SIEM can evolve as your technology and the world around you change.

Critical Start's MDR platform is designed to integrate with several different SIEM providers, including Microsoft Sentinel and Splunk Cloud.

Affordability

MDR integrated with SIEM can be attained by organizations of all sizes without breaking the bank.

An MDR service provider can design a platform designed to work within the demands of your budget that can be delivered in a reasonable amount of time.

Scalability

Most importantly, after implementation, an MDR can process the millions of events coming out of the SIEM.

But here's where it can get tricky: The prevailing wisdom is that with the sheer volume of events coming in, only high-priority alerts should receive attention.

This is a potentially dangerous fallacy, as many ransomware attacks may only trigger a medium or low priority alert.

Resolve Every Alert with a Trusted Behavior Registry

Critical Start's methodology is to treat every alert as equal. This can be accomplished by working with an organization to build out a trusted registry to show what types of activities should be considered normal.

This enables the MDR to focus on all other alerts that fall outside the registry, regardless of their priority status.

Traceability

Where an MDR really performs is if they can use the data provided by a SIEM to track an attack back to its source.

MDR tools can change passwords, isolate endpoints, and effectively lock down a cyber-attack before it can spread to critical components of the network.

MDR & SIEM: Cybersecurity Evolved

That's why an MDR team using SIEM can really outshine the legacy security methods of the past and stand firm against today's broad-spectrum world of security threats.

Still, have questions about how MDR and SIEM can work together to strengthen your organization's security posture? Critical Start's cybersecurity experts are here to help.

LinkedIN: https://www.linkedin.com/in/alkhudary/