BitLyft
Cybersecurity

# MDR vs MSSP vs SIEMaaS

COMPARISON GUIDE

## Exploring the differences and what it means for your organization.

# OVERVIEW

With so many terms, acronyms, and trends it can be difficult to understand who is offering what. There are also so many providers and decisions to make that companies can find themselves wondering which choice is the best and who can actually deliver on what they promise.

The goal of this document is to break down the meaning behind common terminology and explain the differences between several of the most prominent security offerings in the market (MDR, MSSP, and SIEMaaS). We've listed the pros and cons of each type of offering along with a set of questions you can ask when talking with a provider to help determine which is the best choice for you and your organization.

## MDR

**Managed Detection & Response**

## SIEMaaS

**Security Incident Event Management as a Service**

## MSSP

**Managed Security Service Provider**

# MDR

MDR is a newer term that has gained traction over the years. Gartner defines MDR providers as "...providing 24/7 threat monitoring, detection and lightweight response services to customers leveraging a combination of technologies deployed at the host and network layers, advanced analytics, threat intelligence, and human expertise in incident investigation and response."

## PROS

- Remediation time can be reduced from days into minutes
- 24/7 monitoring of network logs, activity, and alerts
- Providers can do all of the testing and sandboxing
- Offers some access to security experts instead of a full-time employee
- Stops threats once they are detected and analyzed
- Validates the severity level of a threat before making an alert
- Great visibility into endpoint activity of users

## CONS

- The term MDR can be used as a marketing cover for older model MSSP services
- The R (response) in MDR can sometimes be your responsibility to handle and not the vendors
- Some MDR providers use limited technology (like only EDR) to see only a fraction of network activity leaving you still exposed in critical areas
- Can still be reactive responses to threats without proactive measures to improve your security posture

With so many vendors saying they are MDR, it's important to understand the "real" work that will be done to help your organization see and respond to threats. Some service provider companies have switched out the term MSSP for MDR with no real difference in services, while others make MDR their main focus. Below is a list of questions to ask an MDR provider to better understand what services and technology you're really getting.

## QUESTIONS FOR MDR PROVIDERS

- What technology do you use to collect logs?
- Is SIEM included in your platform?
- Do you support all SaaS applications?
- Are you able to offer immediate user behavior analytic insights?
- Are you utilizing any automation components to reduce dwell time (SOAR)?
- Can you describe some examples of detected threats my organization will need to remediate that you can't handle?
- How long does it take for your system to create alarms and rules?
- Is email being monitored?
- Do you work seamlessly with on-prem or cloud components?
- What kind of reporting and details do I get with your platform?
- How can I access my data for insights?

# SIEMaaS

SIEMaaS is security information and event management technology delivered as a service. There are some powerful SIEM tools on the market, but you may not be able to procure the talent and expertise on staff to get the most value out of these tools. SIEMaaS providers can install, set up, and maintain the tool, but the purchasing organization is typically left to operate and use the technology on a daily basis.

## PROS

- Organizations maintain full control over the SIEM technology and their teams leverage the tool as they see fit
- Software can be on-premise or cloud based SaaS depending on the SIEM
- Internal security teams who understand the operations and architecture of the organization are using the tool
- Organizations set the expectations and deliverables for the internal security team to deliver

## CONS

- Learning how to install, manage, and update a SIEM is a complex process
- It's a time-intensive process to become proficient with any SIEM
- Requires in-depth understanding network architecture to get the best SIEM results
- Improper tuning and parsing of logs can cause false positives and leave network exposed
- SIEMaaS doesn't come with management of tool, leaving your organization to deal with responding to threats and incident response

Don't confuse SIEMaaS with Managed or Co-Managed SIEM. SIEMaaS is just typically the licensing, installation, and some tuning of the tool. Managed SIEM options typically come with all of the SIEMaaS features but with ongoing utilization of the tool for incident response.

## QUESTIONS FOR SIEMaaS PROVIDERS

- How will I know my SIEM is properly tuned?
- Does the SIEM offer real-time user behavior analytics (UBA)?
- Do you response to any alarms or is that fully our responsibility?
- Do you provide any security recommendations and advice based on SIEM activity?
- Does my purchase come with consulting or service support?
- What other services do you provide that I might need to be success that are not provided in the base pricing?
- How often will you be maintaining the SIEM?
- What are your SLAs and standard communication response times?

# MSSP

An MSSP (managed security service provider) is one that is focused on a broad range of security tools and technology services. Some manage SSO, endpoints, SIEM tools, and vulnerability scanning. Others are just MSP's who branched out of IT to offer security services with their existing line of offerings.

## PROS

- Bundled services can provide savings compared to the cost of full-time employees
- Duties of monitoring the company network can be shared between MSSP and the organization
- Companies don't have to worry about internal staff turnover breaking continuity of service
- Providers offer a much wider range of knowledge, products, and services
- MSSPs can offer access to the latest technologies and help you think through implementation

## CONS

- An outsourced MSSP may have challenges in learning your business and organization goals
- Potential limits in communication between the two parties
- The MSSP may not be singularly focused security which may reduce effectiveness in detection and response capabilities
- MSSPs tend to be add-on business units to service providers, potentially reducing their expertise
- Not all MSSPs consistently analyze your security posture to anticipate your needs and recommend changes

Managed security services providers can help organizations who don't have the internal staffing to accomplish security goals without increasing headcount. There are some significant cost savings and improved efficiencies small teams can gain by using an MSSP over doing the work internally. However, it's important to make sure you're hiring experts, not an add-on unit with less skill and focus in the area you need it most.

## QUESTIONS FOR MSSP PROVIDERS

- What sort of ongoing dedicated tuning, maintenance, and support will we get?
- How long have you had this specific business unit as a service offering?
- What percentage of your business is focused on managed security?
- How often do you spend time in our system to provide recommendations on improving our security posture?
- How do you help us detect and remediate threats in our network?
- How do you communicate with our team and how often can we expect to hear from you?
- Why have you chosen any specific brands over others in your offerings?
- How do you combat alarm fatigue?
- Do you use any automation (SOAR) or threat intelligence technology to protect my environment?

# THE BITLYFT APPROACH

Our approach to cybersecurity focus on providing our clients with a comprehensive platform that goes beyond MDR, SIEMaaS, and MSSP models. Our team of security experts coupled with our powerful BitLyft AIR platform illuminates and eliminates cyber threats in seconds before they have time to harm you or your customers.

## AIR PLATFORM

**Visibility**
Security Information and Event Management (SIEM)

**Expert People**
Security Operations Center (SOC)

**Speed & Efficiency**
Security Orchestration Automation and Response (SOAR)

**Intelligence & Accuracy**
Central Threat Intelligence (CTI)

**The BitLyft AIR platform merges the best of people and software to provide you unparalleled protection for your organization.**

**LEARN HOW**

info@bitlyft.com | www.bitlyft.com | 517.220.0990