BRIEF

Why Choose MDR over MSSP or SIEM?

How Managed Detection and Response Solutions Provide Affordable Cyber Protection Against Today's Threats–and Tomorrow's

Although SIEM provides comprehensive security visibility and MSSPs offer quick and affordable solutions, only MDR providers succeed in bringing a cost-effective security operations solution for threat detection and response.

Security information and event management (SIEM) technology is generally the go-to solution for large enterprises that need comprehensive visibility into cyberthreats across distributed IT infrastructure. But SIEM solutions are capital intensive, complex, and cumbersome. That's why many firms now gravitate towards managed security service providers (MSSPs), which offer quick deployment and affordability through subscription models.

While MSSPs provide remote device management–configuring firewalls, intrusion detection and prevention systems, etc.–they come up short in areas of continuous threat detection and response, leaving organizations at risk.

To fully secure their organizations, companies need a cost-effective managed security operations center (SOC) that providers of managed detection and response (MDR) solutions now bring to enterprises of every size. MDR providers transcend the traditional MSSP cybersecurity model by providing a greater focus on the threat detection and response capabilities that leading firms require to effectively secure their businesses from cyberattacks.

SIEM: Powerful Technology That's Hard to Manage

SIEM is a software solution that collects log records of every endpoint and network activity, correlates these logs to identify indicators of compromise, and alerts security analysts when attacks are detected.

Pros:	Cons:
▶ Customers maintain complete control ▶ SLAs depend on in-house capacity to deliver ▶ Strong user and entity behavior analytics	▶ High upfront costs and complexity ▶ Up to 6 months to deploy and see value ▶ Requires 24x7 oversight by skilled security engineers

MSSP: Outsourced Security Management That Lacks in Key Areas of Cybersecurity

Managed Security Service Providers (MSSPs) focus on remote device management, vulnerability management, security event monitoring, and alerting.

Pros:	Cons:
▶ Proficiency in remote device management ▶ Provide basic monitoring and alerts that do not require deep security expertise ▶ Managed endpoint protection via antivirus	▶ Limited knowledge of their customers' IT environments ▶ Limited security skills (if any) for threat triaging and analysis ▶ Limited network monitoring capabilities

MDR: Outsourced Threat Detection and Response Expertise

MDR providers target two primary groups of buyers for their managed detection and response services:
1) Small and midsize businesses with limited investments in security resources (tools/staff).
2) Midsize enterprises that already invest in security resources but seek partners to augment in-house capabilities.

Pros: MDR solutions provide the following capabilities to end-user customers:
▶ Proprietary technology stack for SIEM included in service price ▶ 24x7 monitoring of events/logs, suspicious activity, and alerts ▶ Continuous network monitoring ▶ Threat detection, triaging, and forensics analysis ▶ Remote incident investigation and response recommendations ▶ Vulnerability assessments ▶ Regulatory compliance reporting ▶ Security advisors who act as extensions of end customers' IT and security teams

MDR providers invest heavily in advanced analytics that leverage commodity big-data platforms like Hadoop, invest in elastic computing like Amazon Web Services, and subscribe to multiple third-party threat intelligence sources that track the latest attack vectors.

Managed Security Operations: The Solution Small-to-Midsize Enterprises Need

A managed security operations solution offers MDR capabilities and more. It uses a cloud-based SIEM platform to collect and correlate log data and network flows from network sensors deployed on customer premises. It includes experienced security engineers who focus on threat detection, forensics analysis, and prioritizing incidents for customers. Vulnerability assessment and compliance reporting is also part of the comprehensive solution.

Arctic Wolf® is the market leader in security operations.

Arctic Wolf delivers the following capabilities above and beyond MDR:

- Named Concierge Security® Team (CST) for each customer account whose engineers act as trusted security advisors and extensions to customers' IT-staff
- Hybrid AI (human-augmented machine learning), which provides 10X better threat detection with 5X fewer false positives
- Security optimized data architecture that dynamically scales and ingests, parses, and analyzes unlimited amounts of log data
- Customizable rules engine that enables Concierge Security Engineers to tailor services to specific customer needs
- Cloud monitoring of 1) infrastructure-as-a-service (IaaS) environments like AWS; 2) software-as-a-service (SaaS) environments like Microsoft 365; 3) security-as-a-service (SecaaS) environments like Okta
- Predictable pricing based on a company's number of employees, servers, and deployed network sensors

The advantages of MDR over MSSP or SIEM are discussed in more detail in this white paper on the same topic.

ARCTIC WOLF

Contact Name
Email Address
Phone
Web Addresss