Managed Detection and Response

There is no magic bullet when it comes to cybersecurity. Every vendor promotes their solution as being the key to vigilant security while playing to the fears about evolving security threats. What companies really need, however, is not yet another product but a focus on detection and incident response. Industry experts point to the fact that there is no such thing as perfect security, and what is critical is the capability to identify and remediate targeted attacks that have bypassed traditional perimeter defenses. Gartner has identified an emerging category of service providers who offer managed detection and response (MDR) to fulfill this growing need.

What is managed detection and response (MDR)?

MDR is different from traditional managed security services (MSS) because they focus on threat detection and remediation versus device management and basic alerting. These services remove the burden from customers of figuring out what the best method or device to use for security monitoring and response capability. MDR services essentially provide security operations center (SOC)-as-a-service and include security event management and analysis, often including the incorporation of threat intelligence feeds. Security engineers front and any triage, forensics and alerting for MDR services versus basic alerting and relying on the customer to do the remediation.

Who needs MDR services?

Every company can benefit from MDR services. Enterprises have the luxury of large budgets and teams of people. Today, 24x7 SOCs with sophisticated tools and processes are the standard for enterprise security. Smaller, mid-market companies have all the same security needs as large enterprise but only a fraction of the budget. They do not have the luxury of having teams of security experts but rely on IT people who wear multiple hats. As a result, mid-market companies stand to benefit the most from MDR services.

Why can’t an MSSP deliver MDR?

Managed security service providers (MSSP) and MDR service providers employ different foundational technologies. MDR service providers leverage cloud technologies, machine learning and big data to provide a stack of network and host-based tools that are positioned at Internet gateways and also collect internal logs, network flows and traffic. MSSPs typically do not have the technology capabilities to ingest and analyze the high volume and variety of log sources required to detect threats well. As a result, even when they are able to detect threats, they lack the detail and context required for the customer to analyze and take proper action.

Is MDR or SIEM better for me?

For mid-sized companies, MDR services are always a better option over a SIEM. Gartner estimates that a SIEM typically takes six to 12 months to deploy for a limited set of threat detection use cases. In addition, they also estimate that a minimum of eight to ten people are required for 24x7 coverage. An MDR service can be installed in 15 minutes, and customers do not have to deal with software licensing, staffing or the cost of third party tools or threat feeds. Companies with deep pockets may not face these issues. Arctic Wolf's MDR service includes a proprietary SIEM and is the fastest, most cost effective way to implement advanced SOC capabilities.

Why is AWN CyberSOC the best choice for MDR?

AWN CyberSOC is the industry's easiest to install MDR service. The service is a combination of world-class cyber-warriors, advanced machine learning and comprehensive, up to the minute threat intelligence. It is anchored by a dedicated security engineer who acts as an extension of your internal IT team and conducts both routine and non-routine tasks to protect you against known and unknown threats. AWN CyberSOC is offered as an affordable monthly subscription and addresses the complete security value chain of threat detection and response.

ARCTIC WOLF Layer 7 Data Solutions

Contact us
arcticwolf.com
1.888.272.8429
ask@arcticwolf.com