10 Capabilities to Look For in an MDR Solution

Multiple point products and defense-in-depth strategies are no longer sufficient to protect companies that operate in today's cyberspace.

IT organizations require cutting-edge detection and response solutions to stop advanced persistent threats that bypass preventive controls. That means either an in-house, fully equipped security operations center (SOC) staffed with security experts, or an outsourced managed detection and response (MDR) service. The latter is a more feasible option for organizations with limited IT resources.

Named Security Engineer

Relying on an MDR solution to detect threats to your systems requires a security engineer who serves as your single point of contact. That way, whenever an issue arises, you can turn to the same familiar person who understands your organization's operations and its business needs. Such a named engineer is highly trained and experienced, and backed with the full support of a robust engineering team focused on optimizing your security outcomes.

One of the many benefits of working with a dedicated security engineer is their understanding of your network infrastructure and business risks. This means the security engineer is uniquely positioned to make informed recommendations specifically tailored to your environment, and seamlessly becomes an extension of your internal team and a trusted advisor.

A named security engineer:

- Conducts daily triage and forensics
- Customizes services to your needs
- Reports on the effectiveness of your security posture
- Provides actionable remediation recommendations for your environment

Continuous Network Monitoring

Continuous network monitoring is a prerequisite for detecting malicious activity on the network. Simply watching the network during business hours will not allow you to recognize abnormal activity and reliably detect threats to which your systems are exposed around the clock.

Customizable Security Rules

Next-generation MDR providers use a customizable rules engine to define security policies for each customer. This engine allows the provider's security engineers to apply your exact security and operational policies and update them to align with changing business needs. For example, customized rules can selectively filter out noisy events that represent no real security risk, or they can help detect known and unknown threats. In this way, a customizable rules engine helps the SOCaaS provider improve efficiency and accuracy when identifying threats in your environment.

Human-Augmented Machine Learning

It's humanly impossible to analyze the massive amounts of log data coming from even the most modest IT environments. The only way to efficiently and effectively analyze high volumes of log data is through machine learning.

Machine learning works great for identifying known threats, but properly categorizing new threat data often requires human expertise. A next-generation MDR provider leverages human expertise to filter out false positives and fine-tune algorithms as new threats are detected.

Cloud Monitoring

Whether you've fully embraced cloud services already or not, modern IT environments demand an MDR solution with integrated cloud monitoring. That way you ensure that your entire environment is covered, with no blind spots.

Look for a service provider that can monitor your IaaS, SaaS applications, and security-as-a-service solutions. Virtual sensors should use APIs to provide near-real-time monitoring of cloud resources and user behavior to ensure they comply with your security policies and are free from threats.

Compliance Reporting

Good regulatory compliance is typically the result of good security practices. Your MDR provider should help you meet compliance obligations and demonstrate that you have done so.

Vulnerability Scanning

Regular vulnerability scans identify assets at risk and help enhance your security posture. MDR providers should analyze scan results and combine the latest threat intelligence with a deep understanding of your critical assets to develop an accurate, prioritized list of your current vulnerabilities. They can then provide risk-based remediation advice and recommendations to limit your exposure to both known and unknown threats.

Workflow Integration

Workflow integration is critical for ensuring that alerts are prioritized and properly escalated for timely remediation. MDR providers should have onsite workflow integration tools to optimize operational efficiencies related to trouble ticketing. Workflow integration that includes your IT staff helps ensure that remediation items are passed on seamlessly from one entity to the other.

Log Data Collection/Correlation

Look for an MDR solution that provides comprehensive log management and includes the automatic collection, aggregation and retention of log data. MDR engineers can perform queries against this data set to extract useful information for customers.

Scalable Data Architecture

It's important to find an MDR provider that leverages a security-optimized data architecture to unify the ingestion, parsing and analysis of log data, and can dynamically scale compute and storage resources on demand. When instrumented for cybersecurity data science, such architectures serve as the foundation for the analytics used by security analysts to achieve deep visibility into advanced threats. In addition, scalable data architecture provides on-demand access to relevant data for incident investigation, and is immediately operational with no setup time.

ARCTIC WOLF

©2018 Arctic Wolf Networks, Inc. All rights reserved. Arctic Wolf Networks, AWN and the Arctic Wolf Networks logo are trademarks of Arctic Wolf Networks, Inc. in the United States and/or other jurisdictions. Other names used in this document are for identification purposes only and may be trademarks of their respective owners.

AICPA SOC

SOC2 Type II Certified

Contact us
arcticwolf.com
1.888.272.8429
ask@arcticwolf.com