PROFICIO

MDR PROVIDERCHECKLIST

Many managed security service providers claim to enhance your security with managed detection and response (MDR) services. If you currently use, or are investigating using an MDR service provider, you are not alone. Partnering with an MDR service provider is one of the fastest growing trends in enterprise security. Review our MDR Checklist to determine if you are getting the most effective security service.

1 CLOUD-NATIVE PLATFORM WITH OPEN XDR

MDR service providers that leverage cloud-native architectures are better able to deliver flexible and scalable services. These next-generation platforms collect and enrich telemetry from a wide variety of data sources and provide investigators with fast search capabilities. By supporting Open XDR, service providers help clients to leverage advanced security technologies and more effectively detect and respond to threats.

2 CO-MANAGED SIEM

While some organizations prefer to use a cloud-based platform, others want to own and control their SIEM and log retention infrastructure. MDR service providers should support a hybrid model that complements popular SIEMs, like Splunk, with 24/7 security monitoring, advanced threat analytics, and SIEM administration services. Ideally, companies can easily migrate from a fully managed cloud service to a co-managed SIEM model without changing processes or relearning tools and dashboards.

3 24/7 GLOBAL SOC SERVICES

Global MDR service providers often have better visibility into emerging threats due to their diverse client base. SOCs using a Follow-the-Sun model also attract better qualified security analysts due to regional daytime shifts and they offer increased resilience as a natural disaster will not disrupt multiple shifts operating for a single location. Using a provider with a global network of SOCs provides better assurance that they will be able to maintain the staffing levels required to support the volume of investigations generated by their client base.

4 ADVANCED THREAT DETECTION

Industry leading MDR service providers use a combination of people and technology to accurately detect and prioritize indicators of attack or compromise. Components of advanced threat detection should include threat intelligence, use case analytics, business context modeling, MITRE ATT&CK framework, and 24/7 investigations by security experts.

5 THREAT HUNTING POWERED BY AI/MACHINE LEARNING

Threat Hunting is a proactive way to detect targeted attacks. The traditional approach to threat hunting is dependent on experienced cyber professionals building hypotheses that model the attack techniques and tactics used by adversaries. Next-generation MDR providers are improving the effectiveness of threat hunting by adding AI/Machine Learning models to detect anomalies and using internal experts to train and verify these models for increased accuracy.

PROFICIO

MDR PROVIDER CHECKLIST

AUTOMATED RESPONSE AND ORCHESTRATION

Despite their best efforts, internal cybersecurity teams may miss indicators of attack, or due to resource constraints, take too long to respond to threats. MDR service providers should use a client's existing perimeter and endpoint security products to automatically trigger response actions that contain attacks before they cause damage. With the addition of Open XDR, providers can extend the integration of collection, detection, and response functions beyond perimeter and endpoint security to technologies including DNS, Authentication, WAF, and the Cloud.

RISK MANAGEMENT AND SCORING

MDR providers should deliver a risk score that is based on the strength of security controls within a company. This presents continuous visibility into the organization's security posture, helps identify blind spots, and provides peer comparisons. Expect to have an assigned team of security experts customize your service and provide expert advice on strategy and tactics. A Risk-Based Vulnerability Management (RBVM) service provides additional protection by prioritizing patching vulnerabilities to focus on those that are real and exploitable.

MANAGED FIREWALL AND ENDPOINT PROTECTION

For organizations that lack the internal resources to manage their security products, MDR service providers should have the capability to manage next-generation firewalls, endpoint software, and cloud security tools and keep them running to vendor recommended standards. This helps off-load IT teams to focus on other tasks and maximizes the value of investments in technology.

ITSM INTEGRATION AND CASE MANAGEMENT

Having access to industry leading ITSM tools for case management and workflow automation ensures tighter integration between a company's IT team and their MDR service provider's security team. This also enables better visibility into the service provider's actions and SLA metrics.

COMPLIANCE

Many organizations must adhere to compliance mandates and regulations like PCI, HIPAA and GDPR. MDR service providers should have the flexibility to collect and archive log data in their client's preferred location, for a range of retention periods. Service providers should also provide their clients with customizable dashboards and reports that monitor key metrics and possible policy violations that pertain to compliance mandates. SOC 2 Type 2 compliance demonstrates your MDR service provider follows the strict information security policies and procedures required to protect confidential data.

You may not be getting the most out of your security provider.
Contact us to learn about Proficio's solutions.
PROFICIO.COM

HOW DOES YOUR MDR SCORE?