ARCTIC WOLF

AUTHORIZED PARTNER | INFO ADVANTAGE

BRIEF

Checklist for Outsourcing Your SOC

A Dedicated Security Team

- 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

Small to midsize enterprises face what's best described as the trifecta of cybersecurity adversity:

- Ransomware attacks, such as **WannaCry** and **Petya**, are more widespread and sophisticated than ever.
- The security expertise shortage is getting worse, with as many as **3.5 million cybersecurity vacancies** by 2021.
- According to Verizon's Data Breach Investigations Report, hackers are increasingly targeting businesses **with 1,000 or fewer** workers.

As a result, small to midsize enterprises (SMEs) are doing what they can to deal with these challenges, and increasingly outsource their security operations to managed security service providers (MSSPs). While a step in the right direction, working with a vendor that lacks the amenities needed for a truly effective security operations center (SOC) with threat detection and response capabilities leaves holes in SMEs' security postures.

To help organizations make smart security decisions, we've created the following checklist to guide the search for a managed SOC:

Real-Time Threat Monitoring

This means having 24x7 continuous monitoring with a focus on threat detection services and forensics for all security incidents. Security information and event management (SIEM) tools are incredibly noisy, making it difficult for a sparsely staffed security team to filter out false alarms and perform adequate forensics on real security alerts that matter.

Make sure your SOC provider is capable of detecting threats at all hours of the day, so that you have ongoing peace of mind.

Complexity

Gartner recently identified a burgeoning cybersecurity market known as managed detection and response (MDR). The "detection" element, as covered above, is critical to identifying threats, but to be prescriptive a SOC must also supply incident response (IR).

Your organization needs a partner that can help facilitate swift, decisive, accurate, and effective IR, whether you're dealing with a false alarm, DDoS, ransomware, or a data breach. If it does not supply 24x7 IR, then it's not a SOC.

Proactive Threat Hunting

Cutting-edge, criminal hacking tactics are increasingly difficult to detect, which means that network configurations need to be continually adjusted based on the newest and wiliest cyberthreats.

The onus is therefore on security operators to learn the unique network topology of their clients, and hunt for threats that are most likely to evade detection through traditional methods. This means utilizing relevant, threat-intelligence sources, applying machine learning and user behavior analytics, and leaving no stone unturned in the search for real security incidents that impact customers.

Strategic Consulting

As they monitor the network and hunt for new threats, dedicated security engineers will acquire a deep understanding of your organization's network topology and location of critical assets, which need to be protected with a defense-in-depth security strategy. No less would be expected of an in-house SOC, so why not demand this of an outsourced SOC?

In addition to the cloud-based scalable technology and well-defined incident response processes, the expertise of experienced security engineers enable clients to gain insights into their overall security posture. Long term, this helps an organization manage business risk more effectively.

Compliance Management

A SOC must be expected to operate with the utmost regard for compliance, whether that's HIPAA, HITECH, PCI DSS, FFIEC, GLBA, or any other standards to which highly-regulated industries must conform. This means providing templates for required and recommended security controls, and basing vulnerability assessments on how well these organizations abide by their respective regulatory standards.

Hackers aren't the only threats to your wallet. Costly penalties for noncompliance can quickly add up, so make sure all risk is managed by your SOC provider.

Predictable Pricing

Last but not least, pricing for this service should not fluctuate based on the number of devices being monitored or amount of log data being ingested one week to the next. A SOC provider should offer a fixed pricing model based on the number of users and sensors rather than volume of log data and endpoints/servers being monitored. This predictable pricing model is especially important for SMEs that may struggle in dealing with turbulent managed service costs.

To learn more about a the Arctic Wolf SOC-as-a-service that is as effective as it is affordable, contact Arctic Wolf today.

ARCTIC WOLF

AUTHORIZED PARTNER | INFO ADVANTAGE

Name: Chris Chan
Email: cchan@info-adv.com
Phone: (585) 331-8706
Website: www.info-adv.com