MSSP Checklist

If you currently use, or are investigating using a Managed Security Service Provider (MSSP), you are not alone. Outsourcing 24x7 security event monitoring, analysis and alerting is one of the fastest growing trends in the enterprise security. Review our MSSP Checklist to help determine if you are getting the most effective security service.

Actionable Alerts

- □ Does your MSSP send you accurate alerts with very few false positives?
- □ Is the volume and priority of alerts you receive tailored to your threat landscape and unique business context?
- □ Does your MSSP send you notifications that clearly describe why an alert is important and how to respond?

Advanced Threat Detection

- □ Does your MSSP frequently surprise you by detecting critical security threats that you had no idea existed?
- □ Has your MSSP modeled the kill chain used in APTs and other targeted attacks to better detect Indicators of Attack and Compromise?
- □ Does your MSSP integrate global threat intelligence for advanced correlation and threat discovery?
- □ Does your provider use powerful tools like commercial Next-Generation SIEM, advanced use cases, business context modeling, behavior analysis and machine learning pattern discovery to detect and prioritize threats?

High-Touch SOC Services

- □ Are your MSSP's Security Analysts responsive and available 24x7?
- □ Does your provider's Security Operations Center (SOC) team proactively investigate suspicious events and not overly rely on system-generated alerts?
- □ Does your MSSP's SOC team really understand your environment and act as an extension of your security team?
- □ Does your MSSP regularly consult with you on alert trends, threat trends, and how to improve your security posture?

Fine-Grained Customization

- □ Does your MSSP maintain a Runbook customized to your unique environment, processes, and escalation rules?
- □ Does your MSSP create custom SIEM use cases and content to reflect your specific technologies, applications, and policies?
- □ Does your provider create dashboards and reports customized for the needs of different types of users?

Automated Response

- □ Does your MSSP provide the option of automating the response to high-risk events for breach prevention to ensure threats are contained in real-time, 24x7?

Visibility and SIEM Access

- □ Do you have full access to your security events and the ability to drill down and investigate each event?
- □ Does your MSSP alert you when one of your log sources stops sending logs to the MSSP's log aggregators?
- □ Does your MSSP provide easy-to-use dashboards, log search, and reports to visualize your security posture?

Hybrid Deployment

- □ Does your MSSP offer the choice of a cloud-based SIEM, managed on-premise SIEM, or hybrid deployment models?

How does your MSSP score?

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

www.Proficio.com

PROFICIO