PROFICIO™

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.

1 ADVANCED THREAT DETECTION

Industry leading MSSPs use a combination of people and technology to accurately detect and prioritize indicators of attack or compromise. Components of advanced threat detection include 24/7 investigations by security analysts, customized SIEM use cases, business context modeling, threat intelligence profiling, and AI-based threat hunting models.

How does your MSSP provide advanced threat detection?

□

2 MANAGED DETECTION AND RESPONSE

Next-generation MSSPs can enhance your security with managed detection and response (MDR) services. MDRs will assist your team by managing technologies at the perimeter, core and endpoint to detect and contain threats in both on-premise and cloud-based environments. MDRs also offer vulnerability management and extensive incident response services.

Does your MSSP provide MDR services?

□

3 SECURITY ORCHESTRATION AND AUTOMATED RESPONSE (SOAR)

Automation or semi-automation is required to quickly contain high-fidelity security events and allow time for incident responders to investigate and remediate threats before they cause damage. Leading MSSPs offer robust services for SOAR that support industry leading security technologies.

Does your MSSP automate response actions?

□

4 RISK SCORING

Advanced MSSPs provide their clients with security dashboards and data that shows each client's risk compared to their peer group. MSSPs also provide their clients visibility into their security posture to help identify blind spots in their security controls.

Does your MSSP provide you a risk comparison with your peers?

□

5 FULL LIFECYLE MANAGEMENT

Many organizations lack the internal resources to manage their security products and keep them running to vendor recommended standards. MSSPs with the capability to manage or co-manage these devices help off-load IT teams to do more important tasks while maximizing the value of next-generations tools..

Can your MSSP manage next-generation security products?

□

6 DEDICATED CLIENT SUCCESS TEAM

In addition to the support of a 24/7 security team, MSSPs should assign their clients with a Client Success Team that assist with account management and strategic security advisory functions. This team is tasked with understanding and supporting the business and technical needs of each client over the duration of the relationship to ensure their requirements are being met or exceeded.
Will your MSSP assign you a dedicated Customer Success team?

□

7 FLEXIBILITY AND CUSTOMIZATION

Every client is unique, yet not every MSSP has the ability to customizes their services to the needs of each client. Flexibility spans customizing use cases, reports, dashboards, escalation rules, incident response actions, and more – all required to meet each clients requirements, whether they are self-made or compliance-based. Mapping the managed security service to each organizations' needs improves the quality of cyber defense and minimizes operational disruption.
Is your MSSP highly flexible and able to customize their services?

□

8 POWERFUL CASE MANAGEMENT

MSSPs should use industry leading tools for case management and workflow automation. Providing clients with case management from ITSM tools allow for better client visibility into the MSSP's actions and tighter integration between the client and MSSPs security team.
Does your MSSP provide you access to an enterprise-class ITSM tool?

□

9 GLOBAL SOC OPERATIONS

Global MSSPs have unrivaled visibility into advanced threats and continuity of operations that regional providers cannot offer. Due to volume and breadth of their client base and 24/7 operations, global MSSPs see more advanced threats on a recurring basis and are in a stronger position to respond quickly.
Does your MSSP have global operations and threat visibility?

□

10 SOC 2 TYPE 2 COMPLIANCE

An MSSP should complete an annual audit to demonstrate that it follows strict information security policies and procedures, encompassing the security, availability, and confidentiality of customer data.
Is your MSSP SOC 2 Type 2 compliant?

□

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
MSSP SCORE?