Engaging with the Right MSSP Partner

Choosing the right Managed Security Services Partner can be complicated.
The odds are that you’re either using, looking for, or recently fired a Managed Security Services Provider. Either way, it’s important to pick an MSSP that’s right for you. The right MSSP will work together with you to provide the best cyber defense against the exponential rise of cyber threats facing the infosec industry and of course, your business!

Engaging with an MSSP is highly critical for businesses who:
√ Need 24x7x365 management of technology & infrastructure
√ Lack internal expert resources
√ Are having difficulty scaling their in-house security practice
√ Need improved data enrichment with cross client correlation, and evolving threat modeling
√ Are challenged to keep up with emerging technologies, new threats and security trends

In This Guide
• Why Pick an MSSP
• MSSP Focus Areas

Focus Area #1: Technical Capabilities
An MSSP needs to have a perspective on your logs - what should be collected initially vs what can be collected in time. For example, Herjavec Group always recommends capturing firewall, active directory, IPS, critical servers, and anti-virus logs at the onset of an onboarding experience.

An MSSP needs to be able to explain how they leverage Big Data Analytics, Anomaly Detection and Threat Analysis to support your environment.

√ Big Data Analytics improves the efficacy of security alerts by actively investigating anomalies and providing the context around each incident detection. It examines the environment for log relationships to seek out anomalies by tracking unusual activity and working backwards to find the context.

√ Anomaly Detection proactively detects the unknown through machine-based learning to identify data pattern changes.

√ Threat Analytics further dives into the data collected and analyzes it for threats using functions such as IP reputation look-up, protocol parsing, deduplication, and more.

Ask yourself: How is this information going to be depicted for you in a way that’s easy to understand and consume?
Focus Area #2: Operational Readiness & Onboarding

During the onboarding process, it’s important that your MSSP takes the time to properly set up your contact points within their company, understand what your needs are, and explain what processes they have in place in case of an alert. A good onboarding uses systematic processes with detailed operational readiness checklists.

<table>
<thead>
<tr>
<th>Is Your House in Order?</th>
<th>Onboarding Best Practices</th>
</tr>
</thead>
<tbody>
<tr>
<td>✓ CSIRT Ready – Is Incident Response defined, documented, practiced?</td>
<td>✓ Define “notable event” vs “incident” based on triple Ds (disruption, degradation, nuisance)</td>
</tr>
<tr>
<td>✓ Asset Classification and Owners – Is this defined and regularly updated?</td>
<td>✓ Build work products such as asset lists, critical applications, SEV priority, etc.</td>
</tr>
<tr>
<td>✓ Ticket Pile-Up – How reactive are IT and Product teams to ticket findings?</td>
<td>✓ Vulnerability scoring definition</td>
</tr>
<tr>
<td>✓ War Games – When was the last table-top incident response exercise?</td>
<td>✓ Defined ownership of process and escalation</td>
</tr>
<tr>
<td>✓ Response Procedures – What will we actually do when attacked?</td>
<td>✓ Poor man’s owner lists: use top users, empty directory, last logon, etc.</td>
</tr>
<tr>
<td></td>
<td>✓ Agreed upon operational readiness checklist</td>
</tr>
</tbody>
</table>

“Within 72 hours of signing a contract we had our solution up and running, grabbing analytics, fine-tuning and we were able to get through a PCI audit in record time.”

- Ed Fox, VP Network Services at MetTel

“The biggest reason we see for the need to engage an MSSP is people. The people factor is drastic. You need to hire at least 7-8 people to maintain a fully compliant, 24x7x365 SOC and a lot of businesses struggle to find the necessary talent.”

-- Atif Ghauri, VP at Herjavec Group
How to Find the Right MSSP

Focus Area #3: Alerts, Investigation, Response
You want to ensure your MSSP has a disciplined approach to use case development and is consistently evolving the alerts triggering in your environment through tuning and new use case development.

It’s All About the Use Cases!
Don’t just start with onboarding data sources - start with use cases.

- Identify and analyze MVAs (most valuable assets) and HBI (high business impact) devices
- Model use-cases around your MVA and HBI devices
- Use cases will tell you what logs you need (not the opposite)
- Then pick the technology to implement these use cases

Use Case Development Best Practices

√ First Things First - Ensure critical conditions produce notification
√ Environment Centric - Build alert rules specific to your environment and requirements
√ Fluid Thresholds - Ensure appropriate thresholds are applied to reduce false alarms
√ What and Why - Know what event sources are logging to the SIEM and why
√ What’s Most Important - Categorize alerts according to severity levels
√ Track Them All - Ensure non-critical events are excluded from notification, but reviewed

“Herjavec Group has become an extension of our Information Security team. Our Account Manager and Technical Account Manager are trusted resources to our organization. We rely on them for guidance and support on an ongoing basis. We have truly become one team.”

- VP IT, Automobile Service Provider

Focus Area #4: SLAs and Contracts
While SLAs and contracts can be time-consuming, they are essential to a healthy Client-MSSP relationship! There are some key DOs and DON’Ts that we recommend for a successful client/provider relationship.

DON’T:
- Have a 5-minute SLA
- Default on a one-year contract
- Do a POC of MSSP - this takes a lot of time for the client and the MSSP so instead, it may be better to do log due diligence

DO:
- Unannounced VA scans and penetration testing
- Provision enforceable SLA penalties
- Define success with simple KPIs

Use Case References

- Popular SIEM Starter Use Cases
- SANS Critical Security Controls ***
- NIST 800-53 ***
How to Find the Right MSSP

How Herjavec Group Can Help

At Herjavec Group, Information Security is What We Do.

Dynamic IT entrepreneur, Robert Herjavec, founded Herjavec Group in 2003 to provide cybersecurity products and services to enterprises globally. We have been recognized as one of the world’s most innovative cybersecurity players, and excel in complex, multi-technology environments. Herjavec Group delivers SOC 2 Type 2 certified managed security services supported by state-of-the-art, PCI compliant, Security Operations Centers, operated 24x7x365 by certified security professionals.

We take on the day to day defense of your infrastructure by monitoring your network, systems and data 24x7x365. We add value by providing context and enriching the data you receive, helping to optimize your organization’s IT security monitoring, incident detection and incident response times.

Our expertise includes:
- Consulting and Compliance
- Product and Service Delivery
- Managed Security Services
- Incident Response
- Identity and Access Management

Herjavec Group has offices globally including across the United States, United Kingdom and Canada.

For more information, visit www.herjavecgroup.com.

Follow Us

LinkedIn: Herjavec Group
Twitter: @HerjavecGroup