LevelBlue

WHITEPAPER

MSSP Checklist: Increase Sales with the Right People, Processes, and Tools

LevelBlue PARTNER PROGRAM

LevelBlue

People: The Essence of the Relationship Comes Down to Who Represents Your Business

Effectively Assess Capabilities and Associated Roles

One problem many struggling MSSPs share is not taking the time required to clarify who does what. Some companies call them swim lanes, while others use a more formal RACI. Either way, successful MSSPs optimize their team's skills, expertise, and experience without overpromising the services and products they can provide. Roles should be documented and clearly defined for all team members.

Make Training a Regular Practice

Organizations worldwide face challenges in recruiting and retaining strong security talent, and MSSPs are no different. For this reason, MSSPs should prioritize internal cybersecurity training to keep employees up to date on the latest technologies. Topics should be relatable to your business and targeted to the right people within the company. MSSPs with solid training programs tend to attract and retain cybersecurity talent because you're investing in their future. Much like how the enterprise should approach cybersecurity awareness training, you should make your training engaging, unique to the business, interactive, and frequent.

Designate Technical and Management Points of Contact

Accountability is vital for customers. They trust you with their business, so being proactive about where "the buck stops" is critical to your relationship. Before onboarding, customers should clearly understand who, how, and when to contact them. Assign a designated contact who understands the customers' business and technical requirements. Determining how and when customers prefer to be contacted for alerts or other critical issues is also essential.

LevelBlue

Processes: The Strength of the Relationship Comes from a Clear Understanding of How Things Work, Especially When There's an Emergency

Define Your Geographical Target

Establishing geographical boundaries will help to avoid issues down the road. Very few companies have the significant resources to build and run a full-time global security operations center (SOC). If you don't have those global customers, creating your MSSP practice with defined geographical coverage is better. For example, you may choose to serve geographies with compliance requirements and regulations you can uniquely address.

Identify Your Ideal Customers

The more you build an ideal customer profile (or persona), the better understanding you'll gain of where to focus your security service delivery efforts. Once you define your ideal customer, the lead strategy process should be much easier to streamline. But don't forget there are different personas within one organization. Not everyone wants technical information. Often, the person approving the PO needs a business case to take to the Board of Directors. Make sure you understand who is influencing and who is deciding.

Develop a Plan for Generating Leads

Bringing in customers is a top business priority for growing your managed security service. While generating leads is not that different from a typical business, for MSSPs, understanding your customers and strategically prospecting is critical. When prospecting, refine messages to address the small and medium-sized business (SMB) mindset toward security. Research shows more customers rely on outside experts to solve their cybersecurity problems. Remember: Selling cybersecurity is no different than selling anything else — you're asking the prospect to trust you. What you do to convey trustworthiness depends on who you're talking to: **economic buyers** care about business benefits, while **technical buyers** want product details. Your ability to adapt to different business issues is critical.

Address Customer Budget Constraints

Given today's economy, current budgets for potential customers are constantly in flux. MSSPs face a complex landscape where drilling down on the actual business drivers will help identify and justify your proposed solution. Our research shows budgets are likely to shift based on those business drivers. By understanding their motivation and concerns, you'll have more success in establishing a budget that will grow with the business.

Develop a Well-Defined Client Onboarding Process

Effective customer onboarding is the first line of defense against potential threats. A robust onboarding process ensures that customers understand security protocols and best practices, reducing the risk of human error and vulnerabilities. Additionally, it lets you gather critical data about their customers, aiding in creating tailored security solutions. Moreover, a positive onboarding experience fosters trust and collaboration, encouraging customers to actively participate in safeguarding their digital assets. Good onboarding is not just a welcoming gesture; it's a strategic investment in fortifying cyber defense.

Implement an Incident Response Workflow

An incident response workflow is structured to identify and respond to a security incident. Especially for MSSPs, a robust incident response plan is critical to minimize the damage caused by security incidents. The incident response team is vital in this workflow, and each team member should clearly understand their roles and responsibilities.

Create a Process for Addressing and Documenting Internal Informational Risk

Building trust with a customer begins with demonstrating expertise and maturity within cybersecurity. Many widely accepted and highly respected third-party frameworks exist (for example, ISO 27001 and the NIST Cybersecurity Framework) that can be used as a common language to illustrate that an MSSP has internally mastered the processes and technology needed to calculate and mitigate risk methodically.

Establish a Process for Quarterly Business Reviews

Quarterly business reviews (QBRs) are crucial for establishing your business value as an MSSP. A QBR creates a two-way dialogue that can go a long way in building customer loyalty. Do not skip these critical reviews with your key clients to establish clear wins and understand where to improve.

Tools: Smart Businesses Use Tools to Automate, Regulate, and Improve Customer Satisfaction

Calculate the Total Cost of Ownership for Cloud Adoption

Calculating an organization's Total Cost of Ownership (TCO) begins with comparing on-premises costs to those of the cloud. Be sure to include both direct and indirect costs associated with running and maintaining current systems. Estimate existing workloads — including storage, servers, databases, and network bandwidth. Keep in mind that cloud ROI often exceeds cloud TCO.

Address Compliance and Regulatory Requirements

All MSSPs need a solid understanding of today's regulatory landscape in the IT services industry. It's essential to have working knowledge of data laws, privacy standards, security requirements, and breach notification protocols — even when providing basic managed security services.

As a starting point, make sure you have the necessary documentation, compliance examples, certifications, and a clearly defined data retention policy.

Determine Which Clouds and Services to Monitor

Leveraging cloud-based services is essential to stay ahead of changing requirements. Your job is to understand cloud solutions and define each service's benefits and challenges. For high-end service delivery, your SOC should be ready to respond to threats quickly, no matter what cloud solution is deployed. You can boost your profit margins from day one with the LevelBlue Partner Program, which offers MSSP pricing and flexible deployment options. LevelBlue technology and services availble for MSSPs include: LevelBlue Unified Security Management (USM) open Extended Detection and Response (XDR) platform; LevelBlue Managed Threat Detection and Response; LevelBlue Managed Vulnerability Scanning; LevelBlue Penetration Testing Service; LevelBlue Incident Response Retainer; Email Security Powered by Check Point; and Endpoint Security Powered by SentinelOne. With this comprehensive suite of services, MSSPs can accelerate revenue and maintain a competitive edge.

Stay Current with Technologies, Tools, and Trends

The cybersecurity threat landscape is constantly evolving and growing more complex. As cybersecurity experts, MSSPs must maintain strong knowledge of current products, emerging threats, and effective remediation strategies. Many MSSPs often gain entry by offering security assessments — and then expand the relationship by selling monitoring services.

Clearly Define Areas of Responsibility

Customers need to clearly understand who is responsible for responding when an incident or actionable alert is triggered. Some incidents may require shared responsibility, while others should be fully managed by the MSSP. It's also important to define whether the customer will have direct access to the security monitoring console or if they will receive reports only.

Know Which Tools Facilitate Response and Reduce Time to Respond

An XDR approach provides MSSPs with centralized visibility to detect, investigate, and respond to attacks across their customers' IT environments. The USM Anywhere open XDR platform combines advanced analytics with integrated Blue Labs threat intelligence, machine learning, and user and entity behavior analytics (UEBA). It also includes security orchestration, automation, and response (SOAR) capabilities, along with robust third-party integrations — helping you quickly and effectively detect and respond to threats on behalf of your customers.

We're Here to Help

As a LevelBlue Partner Program member, we want you to know we're invested in your success. Your account manager is here to collaborate with you and share best practices. Don't forget to explore the resources in our exclusive Partner Portal* — it's packed with presentation content, marketing materials, and product updates to help you become a well-informed, trusted advisor to your customers.

Interested in becoming a partner?
Let us know, and a member of our team will reach out to you.

LevelBlue

About LevelBlue

At LevelBlue, we simplify cybersecurity through award-winning managed services, experienced strategic consulting, threat intelligence and renowned research. Our team is a seamless extension of yours, providing transparency and visibility into security posture and continuously working to strengthen it.
We harness security data from numerous sources and enrich it with artificial intelligence to deliver real-time threat intelligence, which enables more accurate and precise decision making. With a large, always-on global presence, LevelBlue sets the standard for cybersecurity today and tomorrow. We easily and effectively manage risk, so you can focus on your business.

Cybersecurity. Simplified.

Contact us to learn more, or speak with your LevelBlue sales representative.

LevelBlue
PARTNER PROGRAM