Next page

MSSP Buyer’s Guide: Grow your managed SOC business with IBM Security

IBM **Security**

Table of Contents

It’s no secret that the threat landscape is continuously evolving and attackers are becoming more and more sophisticated. At the same time, new regulations are emerging annually in an attempt to mandate stronger security controls. To stay ahead of threats and keep up with compliance mandates, organizations of all sizes must take a more a proactive approach to security monitoring, threat detection and response. Yet, with an estimated 3.5 million unfilled cyber security jobs by 2021, many organizations simply can’t keep up on their own.

As an MSSP, this opportunity is yours to capitalize on. But much like your customers, you can’t do it alone either. You need security partners who offer differentiated, best-of-breed capabilities and act as true partners to help you effectively grow your business. This eBook will outline IBM Security’s MSSP Partner Program and explain how our best-of-breed threat detection and response solutions can help you capitalize on this unique market opportunity to scale your growth and increase your revenue potential.

Partner with us to boost your revenue

As an MSSP, you'll be facing increasing market demand over the next few years, and you need to be prepared. To win and retain business, you'll need to demonstrate the ability to deliver security services more competently and less expensively than clients can achieve on their own.

Rather than deploying yet another point solution, you need an integrated platform that can provide advanced security intelligence with rapid time to value—while also providing the scalability and functionality needed to quickly and easily meet new requirements from old and new customers alike.

By selecting the right vendor partner with the right partner program, you can stay ahead of the technology curve, provide differentiated, value-adding services and boost your revenue potential. When selecting a security vendor partner, you should look for someone who can help you to:

- Easily deploy and implement effective security solutions
- Enable your internal security team on best practices
- Jointly collaborate on sales engagements, through training and field support
- Expand your business by providing marketing collateral and support
- Achieve recurring services revenue
- Manage enterprise products across multiple customers
- Protect your customers' data and assets

IBM Security's MSSP Partner program empowers partners by providing access to best-of-breed security technologies with flexible business models that enable you to effectively and profitably meet your customers' needs. To help you better acquire and serve your customers, IBM Security has enhanced it's MSSP Partner Program with numerous investments including:

- Marketing growth funds to help drive your managed security business and win new clients
- No-cost training options for technical and sales staff
- IBM Seller compensation to drive alignment between ours and your sales organizations
- Technical and transformational consulting options built for MSSPs
- Opportunities to leverage IBM's Managed Security offerings
- Flexible licensing options (Perpetual, Term, Monthly and SaaS)

As a member of the program, you can take advantage of the entire IBM Security ecosystem and optionally leverage IBM's Consulting or Product Professional Services teams to help you build out your suite of offerings.

> *"With other security intelligence systems, it can take months or require more money to realize benefits. With QRadar, we can deliver value to a new client within four weeks, which is quite unusual in our market. We are growing rapidly because we can provide value rapidly."*

– Christophe Bianco, Managing Partner and Chief Technology Officer, Excellium Services

ibm.com/case-studies/excellium-services

To learn more about IBM Security's MSSP program visit:

Learn more

Offer tiered services to capitalize on different customer maturity levels

We understand that one size does not fit all when it comes to your customers. While some organizations are just getting started with enterprise security monitoring, others are ready for a fully managed, 24/7 Security Operations Center (SOC). IBM Security's threat detection and response solutions are fully integrated so you can offer detection and response services either standalone or as a comprehensive solution, based on your customers' unique needs.

Visibility and threat detection

Effective threat detection requires comprehensive visibility into enterprise-wide activity coupled with intelligent, automated analytics to identify both known and unknown threats. The IBM QRadar Security Intelligence Platform enables your team to collect, correlate, and analyze information across data silos—including the cloud—and applies a series of pre-built analytics to automatically detect and prioritize threats. With over 450 out-of-the-box integrations, you can get new customers up and running faster and help existing customers expand their coverage with less operational effort by your team.

The solution includes SIEM at its core, but also offers optional components including user behavior analytics, vulnerability management and network packet inspection. Smaller customers can get started with basic compliance and threat detection use cases, and you can help them mature their capabilities over time—providing even greater customer value while growing your business.

A popular option to get started is QRadar on Cloud, which provides you with an industry-leading SIEM solution with fewer up-front costs and faster set up. Security teams can access QRadar capabilities from a web browser, just as they would if the solution were deployed on-premises.

With QRadar on Cloud, you can gain access to:

- A single architecture for multiple tiers of managed services, including SIEM, user behavior analytics threat intelligence, and network packet inspection for deeper threat insights
- Over 450 out-of-the-box integrations and 160 pre-built apps, to help you on-board and expand customers with much less effort than competitive offerings
- Intelligent security analytics to automatically detect and prioritize threats
- Comprehensive visibility into network, asset, application and user activity to enable faster, more accurate responses
- Streamlined regulatory compliance with out-of-the-box collection, correlation, and reporting capabilities
- The IBM Security App Exchange, which includes pre-built, easily downloadable integrations, use cases, dashboards and reports
- Ingest and analyze vulnerabilities to highlight the riskiest assets within your environment

Learn more

Accurate investigations augmented with artificial intelligence

Whether you have a security team of 10 or 100, your goal is to ensure that your customers’ businesses thrive. That means protecting your customers’ systems and data to stop threats, stay ahead of cybercrime and maintain compliance. However, the pressures plaguing the modern SOC today can make it difficult for you to achieve your goals. With an increase in unaddressed threats, overload of insights, lack of cybersecurity talent, and longer dwell times, the stakes are at an all-time high.

As an integrated component of the QRadar Security Intelligence Platform, QRadar Advisor with Watson empowers you to drive consistent investigations and make quicker, more decisive incident escalations.

As a result, you can help reduce dwell times in your customers’ environments and increase analyst efficiency, ultimately driving greater customer satisfaction, reduced overhead and increased margins for your business.

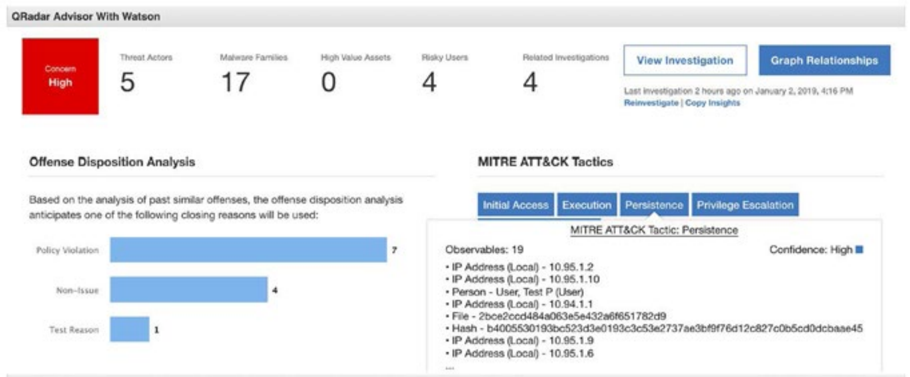
With QRadar Advisor, you can:

- Automate incident analysis and force multiply your team’s efforts
- Drive consistent and deeper investigations
- Reduce dwell times to better protect customers’ environments

Learn more

> *“IBM QRadar Advisor with Watson is a real breakthrough for us and for our clients. Using Watson, our analysts are able to do things 50 percent faster than those without the Watson solution.”*

– Vincent Laurens, Vice President and Cybersecurity Practice Executive, Sogeti Luxembourg



QRadar Advisor With Watson

Concern	Threat Actors	Malware Families	High Value Assets	Risky Users	Related Investigations
High	5	17	0	4	4

Last investigation 2 hours ago on January 2, 2019, 4:16 PM

Offense Disposition Analysis

Based on the analysis of past similar offenses, the offense disposition analysis anticipates one of the following closing reasons will be used:

MITRE ATT&CK Tactics

MITRE ATT&CK Tactic: Persistence

Observables: 19

Confidence: High

- IP Address (Local) - 10.95.1.2
- IP Address (Local) - 10.95.1.10
- Person - User, Test P (User)
- IP Address (Local) - 10.94.1.1
- File - 2bce2ccd484a063e5e432a6f651782d9
- Hash - b4005530193bc523d3e0193c3c53e2737ae3bf9f76d12c827c0b5cd0dcbaae45
- IP Address (Local) - 10.95.1.9
- IP Address (Local) - 10.95.1.6

...

Orchestrate and automate incident response

Statistics say that it is not a matter of "if" but "when" an organization will be compromised. When an incident occurs, it can take hours—if not days—to respond to complex, sophisticated cyberattacks and sort through the multitude of constantly shifting global regulatory obligations. The Resilient Security Orchestration, Automation, and Response (SOAR) Platform is a key part of a managed response strategy. By integrating QRadar and Resilient, you can accelerate your incident response processes while reducing operational overhead.

The Resilient platform offers a unique combination of dynamic case management, orchestration and automation, and machine learning. By deploying Resilient, MSSPs can ensure that analysts are focused on investigating and remediating the most critical security incidents that could impact their customers. Leveraging the IBM Security App Exchange, the Resilient platform provides simple integrations with a variety of security tools and a range of reports and dashboards. This out-of-the-box solution can help you more easily demonstrate the value of the services we provide.

With IBM Resilient, you can empower security analysts to:

- Gain insight from information spanning your customer footprint
- Streamline incident response and scale your managed service operations
- Drive consistency in your service delivery

Learn more

Back to Table of Contents

About the IBM MSSP Partner Program

If you want to continue to grow your business as an MSSP, you need to partner with a trusted security vendor. The good news? The MSSP program that IBM Security offers will help you to provide customers with a set of best-of-breed detection, investigation and SOAR solutions that are easy to scale and deploy. IBM Security has a rich ecosystem of integrations and apps and provides extensive out-of-the-box content in the IBM Security App Exchange. The QRadar Security Intelligence Platform and Resilient Platform are flexible solutions designed to help organizations effectively and efficiently detect, investigate and respond to the most advanced threats. By leveraging automation, these solutions help alleviate the cybersecurity skills gap and provide the operational efficiency needed to become more proactive.

For more information

To learn more about IBM Security's MSSP program, please visit:

ibm.com/security/services/managed-security-services/mssp-program

© Copyright IBM Corporation 2020
IBM Corporation
New Orchard Road
Armonk, NY 10504
Produced in the UK

October 2020

References in this publication to IBM products or services do not imply that IBM intends to make them available in all countries in which IBM operates.