Secureworks®

GUIDE

Defining Security Operation Methodologies for Better Expectation Setting from your Vendors

Defining Security Operation Methodologies for Better Expectation Setting

There are three common methodologies for approaching security operations: fully leverage a third party, hybrid or shared responsibility, and in-house security operations. Each methodology has its own benefits and challenges. Before we deep dive into expectation setting, let us define each methodology.

Fully Leveraged Third Party Security Operations

This model typically combines both managed security service providers (MSSP) and managed service providers (MSP) to help improve security posture. The goal is to control costs and streamline operational security tasks, in order to reduce internal resources requirements. In order to be fully outsourced, your organization will need to lean on an MSSP for visibility through contextualized alerts, as well as an MSP to execute on playbooks, e.g. change management process, based on the alerts generated by an MSSP.

Benefits	Challenges
• Limited resource dependencies • Limited internal systems required • Reduced resource management strain • Reduced need for technology experts • Do not need to develop certain processes, nor buy certain tools	• Limited control over change management • Limited agility • Lack of independence in decision process • Overreliance on third-party skills • Must adopt third-party tools and processes

Hybrid or Shared Security Operations

This is the most common approach to SecOps. For smaller security teams who cannot handle all elements of security operations internally, technology providers, MSSPs, and other partners are used to augment in-house capabilities and offset skills gaps. Hybrid or shared models are good for organizations who may be resource constrained or technology heavy for their staff size. Most operational controls are owned by the organization itself, rather than leveraging third parties.

Benefits	Challenges
• Reduced dependency on third party • Greater control of process management • Ability to set KPIs • Increased capability for decision making	• Conflicting agreements between providers • Challenges swapping out technology • Increased resource dependencies • Skill shortage impacting resources

In-House Security Operations

These lean on extensive internal resources and technologies to deliver security operations. An organization who operates SecOps internally handles all aspects of security, including technology controls, change management, patching, access, authentication, and network segmentation. In order to achieve an effective, fully in-house security operation, there needs to be a synergistic relationship across IT and security. If a threat is detected within the environment, the incident response team can investigate, the network team can setup the appropriate partitions to prevent lateral movement by the threat actor, and the patch management team can prevent reentry.

Benefits	Challenges
• Fully autonomous control • Fully owned processes and SLAs • No third-party control requirements • Full control of change management	• Over-dependency on resources • Complex controls needed • Expertise hard to find and expensive • Often technology dependent

Regardless of the security operations model you choose, there are a few things that you need to consider in order to help set expectations:

Visibility and Network Knowledge

In evaluating whether to operate your Security Operations Center (SOC) internally, leverage a third party to deliver it in its entirety, or a combination of the two, it's important to remember that your knowledge is limited by your visibility. Like we mentioned in Essential Actions for Protecting Business in the Digital Era, if you're only monitoring your front door, you're not going to know if an intruder is trying to breach your windows. Similarly, keeping your most expensive jewelry in the bedroom and only monitoring the garage for intruders is not an effective strategy to improve visibility. Thus, understanding where critical data is located and how it could be accessed and exploited will help determine the level of visibility needed for your organization. This will help you understand whether your own team can handle the level of visibility needed based on the complexity of your environment, or if you need the support of a third party.

Automation

Security operations should be focused on high fidelity and quality of capabilities for both security and infrastructure. Automation is critical in today's digital environment; gone are the days when humans alone could manually triage security alerts. This reality is precipitated by a skills shortage in cybersecurity, as well as an increasing number of available technologies that generate security logs. Automation helps to reduce the amount of noise from your sensors so that limited resources can execute playbooks quickly and effectively.

View Beyond Your Own Horizon

If you don't know what you're looking for, how will you know when you see it? When security operations are in-house with no other data or intelligence sources, chances are your team doesn't have visibility into threat landscape that imposes potential risk to the organization. Threat intelligence based on the latest interactions with cyber adversaries and their tactics is essential for awareness of all potential threats. Because vendors gain intelligence from multiple networks, they likely have more reliable insights; Secureworks calls this the "network effect." Having access to intelligence from thousands of organizations through an MSSP or security vendor gives you a significant edge. Even if you can find and retain a wealth of internal experience, it's difficult to achieve perspective beyond your own network without the assistance of outside organizations and their intelligence.

Know Your Vendor's and Partner's Limitations

No partner can do it all, evidenced by an expression commonly used in cyber security: "The good guys have to be right every time. The bad guys only need to be right once." This applies to your organization, as well as vendors and partners, their services and technologies, and your relationship with them. For example, partnering with an MSSP for security monitoring subjects you to that MSSP's limitations and stipulations with SLAs. It's critical to weigh these limitations and SLAs against the benefits of what an MSSP could bring to your organization. Understanding vendor and partner limitations, as well as the benefits they provide, helps to inform your ultimate decision.

Have a Common Baseline for Service Level Agreement (SLA) Expectations

Regardless of the path you choose for your SecOps model, your internal SLA expectations shouldn't change dramatically. Ultimately, high quality outcomes and responsiveness are nonnegotiable; responsiveness without sacrificing fidelity is the key. Even in a less mature environment, with the right leadership and a third-party partner model, it's possible to meet high expectations for SLAs, quality and quantity of service, and outcomes. The expectations you apply to your model are dependent on the security strategy you develop and the KPIs you are measuring against. Do not sacrifice KPIs too far from your baseline due to third-party limitations. Instead make a fair compromise to your baseline to find a mutually beneficial arrangement.

Understanding Where Risk Lies

You cannot offload risk, and understanding accountability in cybersecurity can be tricky. If a security problem arises you may rely on vendors and partners to identify what went wrong and ways to resolve the issue, but your organization still bears the risk. Risk can be mitigated, but not eliminated or outsourced.

Once you've determined the path forward for security operations, it's important to know how to measure value, whether from an MSSP, MSP, or a technology vendor. There are many ways to discover vulnerabilities or risk on your network, but often, it's the relationship with your vendors and partners that gets you through. The real value of any kind of security service or technology provider is their ability to stay ahead of the game with respect to vulnerabilities or possible incidents, rather than responding reactively to a security event happening in the wild. There are two primary factors to measure:

- **Risk reduction**: Does the addition of this technology or service to your security posture help to reduce risk comparable to the investment? This can be deconstructed in multiple ways, but time to respond, KPIs, and KRIs all come into play in measuring the effectiveness of your vendors and partners in reducing risk.
- **Alignment to and evolution of your security strategy:** You designed your organization's security strategy. Does your vendor or partner help to continuously evolve your security program in a manner that enables your business to keep pace with the changing threat landscape while aligning to your strategy?

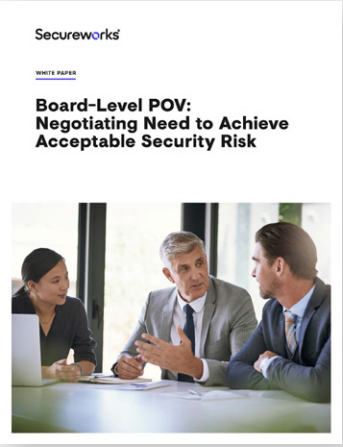
In the digital world, trying to tackle security without good vendor/partner relationships is extremely difficult, even for larger-sized companies. There's simply too much to handle.

The expectations you place on technology, MSSPs and MSPs can be the difference between security success and failure.

"There's so much going on with digital transformation, and it's all about making that leap with new skills and new tools inside the company. That's what digital transformation is... taking all the people you have and retraining them to do the things you need to do to evolve and grow as a company."

Want to learn more?

Click on the assets below to continue learning



Secureworks

Secureworks®

Secureworks® (NASDAQ: SCWX) is a leading global cybersecurity company that protects organizations in the digitally connected world.

We combine visibility from thousands of customers, aggregate and analyze data from any source, anywhere, to prevent security breaches, detect malicious activity in real time, respond rapidly, and predict emerging threats. We offer our customers a cyber-defense that is Collectively Smarter. Exponentially Safer.™

Corporate Headquarters

United States
1 Concourse Pkwy NE #500
Atlanta, GA 30328
+1 877 838 7947
www.secureworks.com

Europe & Middle East

France
8 avenue du Stade de France 93218
Saint Denis Cedex
+33 1 80 60 20 00
www.secureworks.fr

Germany
Main Airport Center,
Unterschweinstiege 10 60549
Frankfurt am Main Germany
069/9792-0
www.dellsecureworks.de

United Kingdom
One Creechurch Place,
1 Creechurch Ln
London EC3A 5AY
United Kingdom
+44(0)207 892 1000
www.secureworks.co.uk

1 Tanfield
Edinburgh EH3 5DA
United Kingdom
+44(0)131 260 3040
www.secureworks.co.uk

United Arab Emirates
Building 15, Dubai Internet City Dubai,
UAE PO Box 500111 00971 4 420
7000

Asia Pacific

Australia
Building 3, 14 Aquatic Drive Frenchs
Forest, Sydney NSW Australia 2086
1800 737 817
www.secureworks.com.au

Japan
Solid Square East Tower 20F
580 Horikawa-cho, Saiwai-ku
Kawasaki, 212-8589
Japan
81-(44)556-4300
www.secureworks.jp