Secureworks®

WHITE PAPER

When to Partner with a Managed Security Services Provider

The information technology landscape is ever changing, which makes securing and monitoring IT networks more challenging.

Today's threat actors are more organized and extremely well funded. They have the time and the resources to study their targets and plan their attacks. It's no longer a matter of "if" but "when" an attack will occur.

From a security perspective, most large and small organizations struggle to fully understand their cyber vulnerability footprint in relation to their network infrastructure, and many lack the ability to find, train, and maintain a staff with the expertise to rapidly detect an intrusion or thwart a sophisticated cyber-attack. Decision makers have reached a crossroads: should they follow the conventional wisdom that certain security information management (SIM) functions should continue to be managed internally, or entrust an experienced third-party vendor to focus on protecting their networks and data assets 24/7/365?

This paper identifies when conditions are ripe for using a Managed Security Services Provider (MSSP), as well as the advantages of partnering with an MSSP in figuring out your organization's security posture and minimizing your risk exposure.

From a security perspective, most large and small organizations struggle to fully understand their cyber vulnerability footprint in relation to their network infrastructure, and many lack the ability to find, train, and maintain a staff with the expertise to rapidly detect an intrusion or thwart a sophisticated cyber-attack.

Assessing Your Unique Security Challenges

The decision to partner with an MSSP hinges on the internal and organic personnel capabilities within the organization and the capabilities and processes in place to respond to a threat or attack. Some tough questions need to be asked when evaluating the level of expertise of your in-house IT team – see graphic below.

Organizations can invest hundreds of thousands or even millions of dollars on SIM tools only to realize that their internal personnel don't have the expertise to deploy and use these tools. Just "checking the boxes" isn't going to work, and training can be a costly and lengthy process. Finding, hiring, training, and retaining the right personnel with the right skill sets (full packet capture intrusion analysis, network forensic analysis, and objective certification – i.e., SANS GIAC) and experience can also be time consuming and expensive.

Assessing Your Organization's Internal Level of Expertise

Does your team have the knowledge to install, configure, and manage SIM tools?

Would they know what to do when an alarm goes off?

Is your team capable of doing packet capture analysis of your event data?

Would they have the forensic data to pinpoint the problem and enumerate the extent of the damage?

Are those tools enough to detect an attack and/or thwart an attack?

What compliance processes are in place? Are they easy to follow? Do they simply cover the basics, or do they go above and beyond to add another level of security?

When to Partner with an MSSP

Luckily, this is not an all-or-nothing situation. MSSPs offer several levels of service to fit various IT department needs and budgets. The three most common are:

Partnering with an MSSP isn't just a way to solve an internal resource problem, it's a way to lower your overall risk exposure.

- **Complete security outsourcing solution.** This involves having one or more staff members of the MSSP embedded in the organization's team, also called residency. These residents serve as experts who understand both the client's infrastructure and processes, and those of the MSSP. If a breach occurs, the residents have access to the MSSP's tools and information in order to expedite the remediation effort.
- **Hybrid solution.** An organization chooses to use a combination of internal staff during regular hours, and MSSP professionals to monitor the network on nights, weekends, and holidays.
- **End-to-end solution.** Some IT departments are small and need to focus on supporting the business lines. They don't have the time or investment dollars to manage internal cybersecurity technology, processes, and programs. An MSSP can manage an organization's security devices 24/7 and, if a breach does occur, can provide forensic capabilities and remediation instructions for the client to execute.

MSSPs focus on articulating the threat landscape. They look for threat actors and study their tactics, techniques, and procedures across all markets. This is an important distinction — not all hackers or attacks are alike. A proactive approach to assessing the threat landscape involves knowing not only who the actors are — hacktivists, nation-states, criminals — but also their individual motives. They each act in distinctive ways, and although their techniques may overlap, their objectives and motivations are different. The key is pattern recognition, which comes from security analysts gathering threat intelligence from a variety of reputable sources across multiple industries and developing new signatures.

The Advantages of Partnering with an MSSP

An MSSP uses the latest technology, techniques, and tactics to help assess an organization's security vulnerabilities and help manage the risks to an organization's assets. Their sole focus is to help clients develop the appropriate security posture for their networks. Outsourcing your IT security to an experienced provider has additional advantages:

- Improved visibility into emerging threats. Top MSSPs monitor thousands of customer networks and leverage applied research to ensure they are always ahead of the latest threats and threat actor tactics.
- Increased efficiency. MSSP analyst teams use the latest technology and tools to detect security gaps and malicious activity in real time.
- Constant vigilance. A team of certified security analysts with deep event analysis and incident response experience monitors alerts 24/7/365 to detect intrusions.
- Focused resources. Using an MSSP focused solely on security information management allows organizations to concentrate on their core business operations and new opportunities.
- Agile processes. Many MSSP delivery options are flexible and do not require substantial investments in additional infrastructure. As an organization's needs change, the MSSP solution can change with minimal disruption.

Conclusion

Network security breaches are becoming more frequent and pervasive. No company or industry is immune to these ever increasing threats. Organizations need to take steps now to ensure that their data assets and intellectual property are not only protected, but also that there is a plan in place to quickly respond to a security incident.

Engaging a managed security service provider can help organizations assess network vulnerabilities and develop an appropriate security posture. Top MSSPs have the expertise and technological resources to help their clients with a myriad of capabilities, including architecture design implementation, network device and traffic monitoring, threat intelligence gathering and analytics, and incident response and forensics. Partnering with an MSSP isn't just a way to solve your internal resource problem, it's a way to lower your overall risk exposure.

Secureworks®

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

We combine visibility from thousands of clients, 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 clients 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
UK House, 180 Oxford St
London W1D 1NN
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