Secureworks®

WHITE PAPER

Comparing Managed Security Services Versus In-house Security Information Management (SIM)

How to stand back and evaluate your organization's cybersecurity options

Proactively managing information security is a critical component to mitigating the risks to your information assets and to your business. Intellectual property, financial information, and employee and customer data are just some of the private information stored in an organization's network. Maintaining the confidentiality, integrity and availability of these assets should be of the utmost importance to every organization.

Leveraging a security services provider such as Secureworks® for global Managed Security Services will help manage the risks to your IT assets in an efficient, cost-effective fashion aligned with industry best practices. There are significant advantages to this approach:

- **Improved visibility into emerging threats.** Secureworks monitors thousands of client networks and leverages applied research to ensure that we are always ahead of the latest tactics, techniques, and procedures of modern threat actors.
- **Increased efficiency.** No additional operational overhead to invest in SIM and manage an expert team of analysts.
- **Constant vigilance.** A 24x7x365 team of certified Senior Intrusion Analysts with deep event analysis and incident response experience monitor alerts to detect intrusions.
- **Purpose-built technology and architecture.** Built-in redundant architecture delivered through seven integrated Security Operations Centers (SOCs) provides a scalable solution.
- **Focused resources.** Your security team can spend their time on system maintenance and security culture within your business.
- **Agile processes.** Flexible delivery options to meet the individual security needs of each organization.

An organization's data is part of its portfolio of assets, and protecting those assets is a necessity. Executives must decide the best approach for their organization, weighing the quality of protection, risk tolerance and the associated costs to define their security program.

Comparison of initial and ongoing costs

The Secureworks Counter Threat Platform™ (CTP) is fully managed and maintained by Secureworks professionals. All components of our Platform are located at our global SOCs where they are managed 24x7x365 by our team of experts.

Comparable to any large-scale enterprise software deployment, SIM technologies can take a long time to deliver ROI and bring measurable benefits to an organization. Secureworks services empower you to be a "user" of SIM technology without having to bear the costs of managing a complex and burdensome on-site solution.

The following pages compare the differing cost structures and security scenarios typically encountered by organizations deploying information security processes in-house to those who choose to partner with Secureworks as a Managed Security Services Provider (MSSP).

Managing information security in-house

Because the confidentiality of corporate data is so vital to an organization, it's understandable that some executives are reluctant to outsource what feels like the integrity of their business. It seems counterintuitive that — when all aspects of information security are handled by an internal team — the costs can be higher and the risks to the business greater. But by managing information security internally, organizations face unforeseeable costs from staffing and hardware to licensing and maintenance.

Staffing and training

Staffing a true 24x7x365 Security Operations Center requires a minimum of seven full-time employees. While IT departments, network groups or even security teams may have the talent and expertise, they rarely have the current and well-practiced skill set that is required to execute real-time or even batched security event analysis. There are millions of events generated every day within an environment, and an analyst must rapidly filter to isolate the one or two true security incidents. To provide the necessary skill sets, analysts must receive periodic training from technical-oriented organizations such as SANS. This training adds thousands of dollars per employee in annual investments.

Of course, nothing can compensate for experience, and finding employees that have this experience can be time-consuming and costly. You must also consider the costs of turnover should personnel critical to the daily operation of the SIM technology depart. SIM technology cannot run itself – if the SIM Manager or other critical staff member leaves, there will be a significant performance lapse even if you have fully trained replacements available.

Having the proper security personnel puts tremendous pressure on IT departments to recruit, train, compensate and retain a 24x7 security staff. The cost of training or enhancing a security professional's skills for an in-house network can be prohibitive. Tools, such as SIM products, are not easy to understand out of the box and by no means easy to use. Learning how they work takes weeks, if not months, of training depending on the specific SIM technology and your personnel's background.

Hardware, software and licensing

The bulk of the disclosed up-front SIM costs stem from licensing. The initial licensing costs of most enterprise-class SIM software technologies go well into six figures and annual license fees are typically between 10 and 25 percent. Additionally, with most SIM software solutions, agents must be purchased for all technologies to be monitored with the SIM system. After the initial purchase, the cost of agents must also be considered each time your infrastructure changes.

To be effective, in-house SIM software solutions need dedicated databases and high-end servers for agent systems and management systems. You will need at least one database administrator who knows the underlying database system (Oracle, MySQL, etc.) in and out. In addition to initial hardware capital expenditures, there is often ongoing maintenance of the backend systems which must be kept running optimally for the SIM solution to function properly.

Any company managing SIM in-house should have a mirrored test environment for creating and testing correlation rules. Turning a rule on in production can easily have unexpected, adverse effects such as flooding or slowing the application. A test environment is a must if you intend to effectively manage the in-house SIM system without causing problems throughout the enterprise. This can easily double the anticipated hardware costs.

Implementation

Deploying SIM software in enterprise environments is a complex and expensive process that can last anywhere from 6 to 18 months depending on the customization required and the amount of resources you can throw at it. Installation is not intuitive and you will need consulting services to successfully deploy an on-site SIM system.

Management

Due to their complexity, SIM solutions are nontrivial to manage and maintain. Resources will need to be spent on full-time SIM managers and database administrators in order to keep the SIM technology up and running. Both managers and analysts will need to be familiar with all types of systems in your environment and how they interact, to manage filters and correlation rules. In addition, agents will need to be upgraded when new versions of the underlying monitored devices change and any customization to the agent will need to be repeated in most instances when deploying the upgraded agent.

Comparison of Secureworks security services

Development of Secureworks Counter Threat Platform began in 1998 and has been continuously improved during the past 20 years. The experience and expertise gained through the monitoring of thousands of global client networks provides this purpose-built security technology with unmatched visibility across the threat landscape. The CTP supports our team of SANS, GIAC, and GCIA certified Senior Intrusion Analysts who are solely focused on analyzing security events on a 24x7x365 basis.

We deliver real-time monitoring, correlation and expert analysis of security activity across your enterprise, and we lead the industry in client satisfaction. We have the mature technology, robust processes and experienced security experts needed to effectively detect and respond to both known and emerging threats in real time.

All of our Managed Security Services are provided in an unlimited and unmetered fashion with no hidden or additional costs. Regardless of the number of incidents escalated, calls to the SOCs, events analyzed, etc., the monthly subscription fee will remain constant per monitored/managed device. In order to form a true security partnership, we believe that we cannot place limits on the number of calls to the SOCs, escalated incidents or the time our Senior Intrusion Analysts spend working with each of our clients to secure their critical assets. Nor do we believe in a tiered staffing model where clients are forced to interact with junior-level personnel before speaking with experts. Instead, every call is handled by one of our certified, experienced security professionals. Because of this, we have one standard SLA for each of our Managed Security Services and impose no limits on the level of support we provide for our clients.

Finding the real security incidents

Secureworks monitors billions of events each day and already has in place the people, processes and technology needed to filter the overall haystack of events to the few truly important security events of interest. We are able to accomplish this by continuously tuning our platform to identify new threats when we see them, as well as eliminating non-security events when we identify such activity to be normal business traffic. This enables our solution to scale indefinitely while constantly adapting to new threat environments.

This, in particular, is a difficulty we have seen with enterprises which have deployed in-house SIM technologies. Performing this task in-house requires extensive initial and ongoing tuning of the SIM technology simply to cut through the millions of events such as logins, downloads, or software updates a typical company sees every day. Failure to manage the technology in a way that does not flood the in-house staff is symptomatic of many failed SIM deployments.

Experience and visibility

We see malicious activity occurring across all of our clients, giving us global visibility into the overall threat landscape as well as threats specific to major industries, including financial services, healthcare, retail and utilities. Our platform leverages the information we gain by applying security findings analyzed from a single client across our entire client base. As a result, we can detect and respond to a much greater breadth of attacks with more speed and accuracy than an in-house solution.

Faster response to and resolution of security incidents

Our experienced analysts know exactly what to do when an anomalous event does occur. This allows us to identify and respond to the "needles in the haystack" faster and with more accuracy than is possible with an in-house solution. Once an incident is identified, we work directly with the appropriate client staff to mitigate the threat and minimize its impact.

Total solution redundancy

All aspects of Secureworks Managed Security Services, from the people to the technology, ensure uninterrupted security monitoring and response. Secureworks operates seven integrated Security Operations Centers with hundreds of expert Security Intrusion Analysts (SIAs). All Secureworks SOCs are staffed 24x7x365 and all SIAs are required to hold the SANS, GIAC, and GCIA certification.

Additionally, all members of our SOC team are trained cross-functionally in multiple roles to ensure that all critical responsibilities are covered and service is not impacted should anything change in terms of personnel.

Secureworks SOCs operate as a single entity, with the systems mirrored in real time using integrated video and voice technologies. They each undergo annual SSAE 16 audits and periodic FFIEC examinations. All SOCs are equipped with redundant high speed Internet connections, fiber optic loops and back-up power generators.

In-house solutions expose you to risks associated with infrastructure and staff availability which are not factors with Secureworks services. Should an in-house SIM manager or other critical staff member leave, your organization's security posture will invariably suffer while provisions are made to re-staff the position. Complete fault tolerance requires building out at least two 24x7x365 SOCs, each with a minimum of seven full-time employees and all corresponding hardware/software necessary to conduct security event analysis. This can be extremely cost-prohibitive.

Focusing your efforts

Secureworks allows your security team to spend their time focusing on strategic efforts to improve your security, instead of having to spend their time and energy to keep a complex SIM technology up and running, performing event analysis and managing security technology. We find the security incidents that need your attention and help you to work through them so that your team makes the most out of their day-to-day security efforts. Our SOC team strives to be an extension of your own security team, filling in competency gaps and providing unlimited support for any security issue. As a result, your security program is more efficient, runs smoother and provides greater protection for your enterprise.

Objective security analysis

Secureworks experts provide objective, in-depth analysis of security activity. Their effectiveness is not affected or impacted by any internal influences that can be common in some enterprises, such as political maneuvering or pressure from other groups within the company. As a result, the information provided by our analysts will be consistent and measurable, ensuring that your metrics are accurate and not influenced by factors not related to the security of your organization.

Flexibility

Secureworks solutions are delivered as a managed service and, because it does not require substantial investments in additional infrastructure, you are not locked into our solution. If your needs change, you have the freedom to pick a solution that is best for your organization. With an in-house solution, your flexibility is compromised by the large capital investment in a solution that may not meet your security needs in the future. With Secureworks, you are subscribing to our service, security expertise and Threat Intelligence visibility – not investing in our technology.

Technology solutions can easily become outdated or obsolete in two to three years. Our services ensure that you will always have an agile monitoring solution that protects your assets.

Secureworks Counter Threat Platform can monitor virtually any security technology without the use of agents. Our CTP’s filtering system is operationally updated to accommodate new technologies and technology upgrades without additional development, as is required for agent based technologies. This provides you with the flexibility to utilize the security technologies which best fit your needs.

Compliance and reporting

Secureworks provides unmatched visibility into your organization's security and compliance posture. The Secureworks Client Portal provides access to hundreds of pre-built and easily customizable reports to ensure that stakeholders at all levels can easily understand relevant security information. Granular reports allow IT staff to drill down into specific events and logs, while dashboards, charts and tables allow executives to gain insight into the higher-level security trends. All actions taken against a specific event by both Secureworks and the client's internal security team are tracked to ensure all issues are handled in a timely fashion and that SLAs are being met.

Reporting has also been specifically designed to help clients demonstrate adherence to regulatory requirements and can significantly ease the burden of security compliance reporting for many organizations. Whether your organization is governed by PCI, SOX, HIPAA, FISMA, NERC CIP, FFIEC or GLBA, you can rest assured that the Secureworks Client Portal can easily demonstrate compliance to auditors. Secureworks undergoes annual SSAE 16 certifications and adheres to industry best practices while safeguarding client information assets.

Secureworks is ranked by Forrester as a leading innovator and enduring institution in cybersecurity In a comprehensive study of security solutions providers, Forrester concluded that, "Secureworks continues to blend exceptional threat research and incident response. Many providers use machine learning to produce security rules, which they then test and deploy for customers; Secureworks is one of the first to apply machine learning in real time, enhancing protection and minimizing false positives. The company has also unified the Counter Threat Unit research team and Security Operations team into a single organizational chart with defined processes for information sharing and escalations. Client events and incidents are worked by SOC analysts and CTU team members in tandem when necessary, resulting in a differentiated experience for their customers."[1]

Counter Threat Unit™ (CTU™) Research Team

In addition to hundreds of certified Security Analysts, Secureworks is home to the Counter Threat Unit™ (CTU™) research group, an elite team of security researchers dedicated to staying abreast of the latest threats and trends in cybercrime.

Leveraging our global threat visibility, proprietary toolsets and unmatched expertise, the CTU team performs in-depth analysis of emerging threats and Zero-Day vulnerabilities. They are at the forefront of cyber threat research, specializing in malware analysis, reverse engineering, counter intelligence, forensics, cyber-crime monitoring and countermeasure development.

The CTU group has a strong reputation for publishing high-quality research on real threats to businesses and is frequently the first to market with the identification of new exploit techniques and the analysis of emerging threats. Their expertise is often specifically sought by government agencies and large enterprises, as well as many news outlets including The Associated Press, The Wall Street Journal, The Washington Post, USA Today, CNN and The New York Times. The team is deeply involved in many influential threat research circles, including government, academic and industrial research forums.

This team of experts ensures that Secureworks clients are protected from the latest and most sophisticated threats by constantly updating our technology to recognize these attacks. Aggressive SLAs and a commitment to protecting our clients result in faster, more comprehensive protection of their assets.

Sources:

[1] "The Forrester Wave™: Managed Security Services Providers, North America, Q3 2016. The 11 Providers That Matter Most And How They Stack Up" Jeff Pollard. August 30, 2016.

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
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