AVERTIUM

WHITE PAPER

Managed Security Services Provider or In-house Solution

AVERTIUM. SHOW NO WEAKNESS™

Introduction

No company can ignore threats to its corporate network. Nor can they take the "it won't happen to us" stance about network security any more. Cybercrime has become the greatest threat to every company in the world. In fact, according to the Official 2017-2018 Cybercrime Report, published by Cybersecurity Ventures, cybercrime will cost the world $6 trillion annually by 2021. This is up from $3 trillion in 2015 and represents the greatest transfer of economic wealth in history. At this rate, cybercrime will be more profitable than the global trade of all major illegal drugs combined.

Every corporate network, no matter the size, has value to someone. From credit card numbers and health records, intellectual property, and client data, to just plain boasting about hacking into a network; there are malicious intentions across our Internet-connected world.

No matter the criminal motivation, information technology (IT) professionals are now forced to approach security from multiple angles to thwart the malicious intent that threatens their organizations' systems daily.

To deal with the ever-changing threat landscape, many IT departments have found outsourcing specific portions of their duties to capable third parties helpful in reducing work load and expenses. But how does this apply to in-house versus outsourced 24x7 managed security?

This paper provides a comparison of security network monitoring for both an internal and external model.

The Value of Network Monitoring

Most companies today, from small to large, have determined they must perform some type of active monitoring on their data network. Large companies are already in the crosshairs of various bad actors for a variety of reasons.

Just ask some big-name retailers who have recently had data breaches that involved millions of records of customer data being stolen. It's not a short list of companies, and the ramifications have reached (and will continue to mount) into the billions of dollars in outright costs for repairs, lost sales, and customer loyalty. These factors ultimately affect the bottom line revenue for each of these companies. For instance, one of these retailers had a staggering 46 percent drop in profits compared with the same quarter the year before.

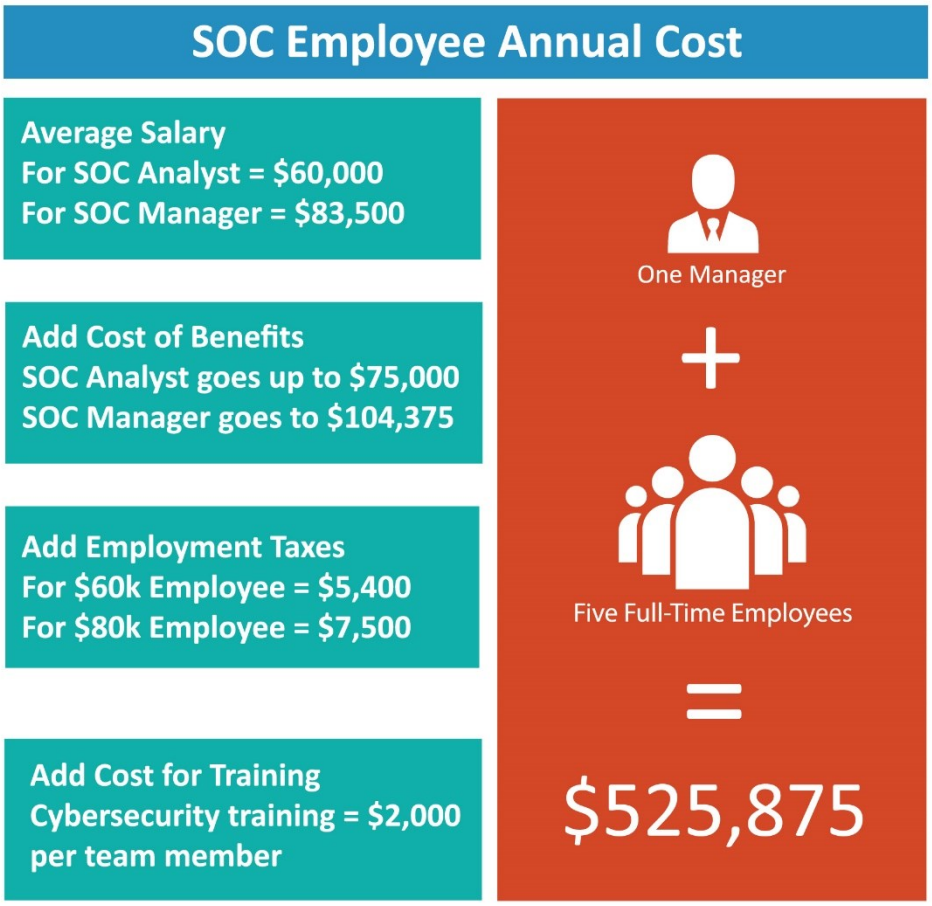
IT security is extremely sophisticated and is eternally changing. It's a sure bet that most corporate networks will or have already been attacked. Effective information security is about intelligence and having insight into who is interacting with your data and how they are doing this.

For such an important decision, it is worth exploring all the engagement possibilities available to find the right way specific to your business to protect your systems, fit your budget and time frame, all while tending to your IT team's needs.

Cost of a SOC

The first question most companies ask when comparing an MSSP versus an in-house solution is, “What will it cost?”.

The average SOC requires at least one manager and five to seven full-time SOC analysts to allow for employee outages such as sick time, vacation, and an on-call rotation. Let’s look at the costs associated with staffing a full-time security operations center:



NOTE: Calculations are based on conservative annual salary, benefits, and tax estimates and minimum number of employees. Actual costs may be higher.

This high-level look at costs is based on the following:

- Glassdoor.com reports that the national average salary is $60,000 for a SOC analyst and $83,500 for a SOC manager. Depending on cost-of-living for your region of the country, these amounts may differ. For this publication, we felt this was a good baseline to use.

- Add to that the cost of benefits. According to MIT.edu, adding health coverage, life insurance, dental plans, and other benefits typically costs the employer in the 1.25 to 1.4 times base salary range. This means on the low end of this range (1.25) the $60k salary employee would cost $75,000 annually and the $83,500 manager would cost $104,375 annually.

- Now consider that employment taxes including Social Security Tax, Medicare and other employer taxes add an average of 9% to the base salary. This adds $5,400 a year for the $60,000 employee, and about $7,500 for the $83,500 employee.

- Then add training. Technical training comes at a premium. Avertium's training experts estimate an average cost for training a SOC employee to be $2,000 per month.

- By this formula, the $60k employee actual cost is $82,400 and the $80k employee is $113,875. If you have five FTEs (remember, this is the low end of what a full-time SOC requires) and one manager, this equals more than $525,875 annually in employee costs alone.

This is (a conservative) estimated employee cost alone and does not take into account the high cost of employee turnover. Additional costs for items such as office space, equipment, hosted cloud services, and technology must also be considered. **This can add up to $100,000 a year or more.**

Compare these costs to a typical MSSP monthly operational cost of $5,000 to $12,000.

Components of 24x7 Protection

To be able to compare apples to apples, we must establish the components needed to make up a capable managed security solution. No matter the mode by which this service is delivered, the solution must include the proper people, processes, and technologies to provide a valuable service.

Security Operations Center

A security operations center (SOC) is a centralized command center that maintains visibility of the security posture of the network. A SOC is not only a physical area complete with the servers, devices, and tools you need to handle the load of data; but must also be the finely tuned "machine" made up of people and processes carefully planned to come together into a cohesive unit that effectively and efficiently watches for, recognizes, and handles any threats that may come your way.

SIEM Management

A key factor in preventing data breaches is the ability to actively monitor the Internet connection(s) and review log files from perimeter devices, such as firewalls and intrusion detection systems.

In addition, an often-overlooked and underestimated aspect of cybersecurity is insider threats which are becoming more common and costly. Whether they are malicious or un-intentional in nature, the most effective security approach for cyber insider threats is to incorporate risk management that includes continuous monitoring and evaluating people, processes, and technologies.

Real-time monitoring is a herculean task because of the immense amount of data and logs generated by the network and computing systems. Security analysts spend a great deal of their time daily reviewing

these logs to find dangerous activity and to identify targeted hosts and exploits that may be happening on the network.

It is much easier to review logs when they are stored on a device designed to capture and process them. Security Information and Event Management (SIEM) is a specialized security tool with software that gathers real-time network and log data for the analysis of security alerts. Typically placed just after the firewall, the device collects or captures threats and provides correlated data intelligence.

As the SIEM is capturing data, security analysts review and report key findings and potential threats and make necessary modifications to systems and network devices to thwart any malicious activity.

A SIEM solution is a faster, cost-effective way for an organization to have complete visibility into the security of their environment. But, it is important to note that the number one requirement, and the most often overlooked in SIEM technology, is constant real-time monitoring and review by capable security analysts.

Advanced Perimeter Defense and Deception Technology

The unprecedented volume of traffic hitting networks and increasing sophistication of threats leaves organizations vulnerable, unaware, and unable to rapidly respond to this new landscape. Today's information security climate demands a proactive approach to stop unwanted, illegitimate and distracting traffic from entering your network environment by reducing traffic and deceiving and catching attackers.

Advanced perimeter defense stops unwanted, illegitimate and distracting traffic from entering your network environment, and deception technology deceives and catches attackers during the discovery phase of an attack when they are most vulnerable.

Managed Detection and Response

Managed detection and response (MDR) services provide customers with a fully-managed and monitored security solution. MDR utilizes software-based endpoint technology to provide prevention, detection, response, and threat hunting for malicious activity in the customer's environment. If a breach has occurred, MDR helps the user to gain control and to better understand the threat. Once the threat is eliminated, the technology provides an ongoing mechanism to prevent attacks and provide insight into future malicious activity.

Technologies to Run the SOC

In addition to the above, a SOC must come complete with technologies that help to run day-to-day activities. This includes systems for ticketing, authentication, documentation, inventory and others; as well as networking devices.

Security Experts

It is of the utmost importance to have qualified, trustworthy and reliable security analysts monitoring and reporting on the safety of your environment. These specially-trained individuals determine which threats captured by the SIEM are real and respond quickly and appropriately.

Security analysts are a specialized IT resource and thus cost more to hire than typical IT support personnel. They also require periodic specialized training. The more coverage required, and the size of the network determines how many team members are needed to staff the SOC.

It should be noted that malicious intent happens 24 hours a day, 365 days a year and, to be completely protected, the SOC should be staffed appropriately to cover this timeframe.

Internal Resources

There are advantages to creating an in-house security operations center. These include knowing your environment intimately, having the freedom to choose the software and tools employed, and hiring and getting to know the security analysts personally.

However, not all companies have the ability and resources to staff the 24x7 coverage needed for security.

The challenges of staffing a SOC are compounded by a major shortage of experienced cybersecurity talent. Consider that Cybersecurity Ventures predicts there will be 3.5 million unfilled cybersecurity positions globally by 2021.

According to a 451 Research study, based on responses from more than 1,000 IT professionals, primarily in North America and EMEA, security managers reported significant obstacles in implementing desired security projects due to lack of staff expertise (34.5%) and inadequate staffing (26.4%). Given this challenge, only 24% of enterprises have 24×7 monitoring in place using internal resources.

Another factor to consider is the time required to build an internal SOC. A typical business environment can take between 18 and 24 months to fully build-out a functioning security operations center.

Outside Resources

An alternative to hiring in-house security personnel is to partner with a managed security service provider (MSSP). There are many mid-size companies who use this approach as it's easy, doesn't require in-house expertise, and allows the company to concentrate on what it does best – its core business. MSSPs or virtual SOC's, as they are sometimes called, can provide the same monitoring and event management services without the need to hire in-house staff or secure space.

Technology

MSSPs use an assortment of security tools in addition to a SIEM device to help detect, thwart and gather information on security attacks. The MSSP is also responsible for providing timely notification of events through the monitoring of network and security log events, identification and remediation of today's modern threats are the primary function of a virtual SOC.

Utilizing an MSSP will almost certainly reduce overhead and is normally expense driven. Consider that the Managed Security Service Provider typically provides all the tools and services needed to monitor the network as part of its monthly pricing structure. In addition, since the MSSP is providing services to many clients, economies of scale are shared with all their clients.

Aggregate Experience

MSSPs attain knowledge from a range of experiences across their client base in order to document and process lessons learned, then apply them systematically to all their clients. Since no two networks are configured or set up in the same manner, each customer's environment provides a learning experience. SOC team members applying their knowledge gained from serving many clients helps reduce the time to remediate issues or problems as they arise.

Consistency of Service

Another advantage of using an outsourced MSSP is the consistency it provides. Hiring, training and retaining qualified staff is costly. Then, what happens if they leave the company? An MSSP maintains a team of analysts to serve you, with practices in place to provide continuity and consistency.

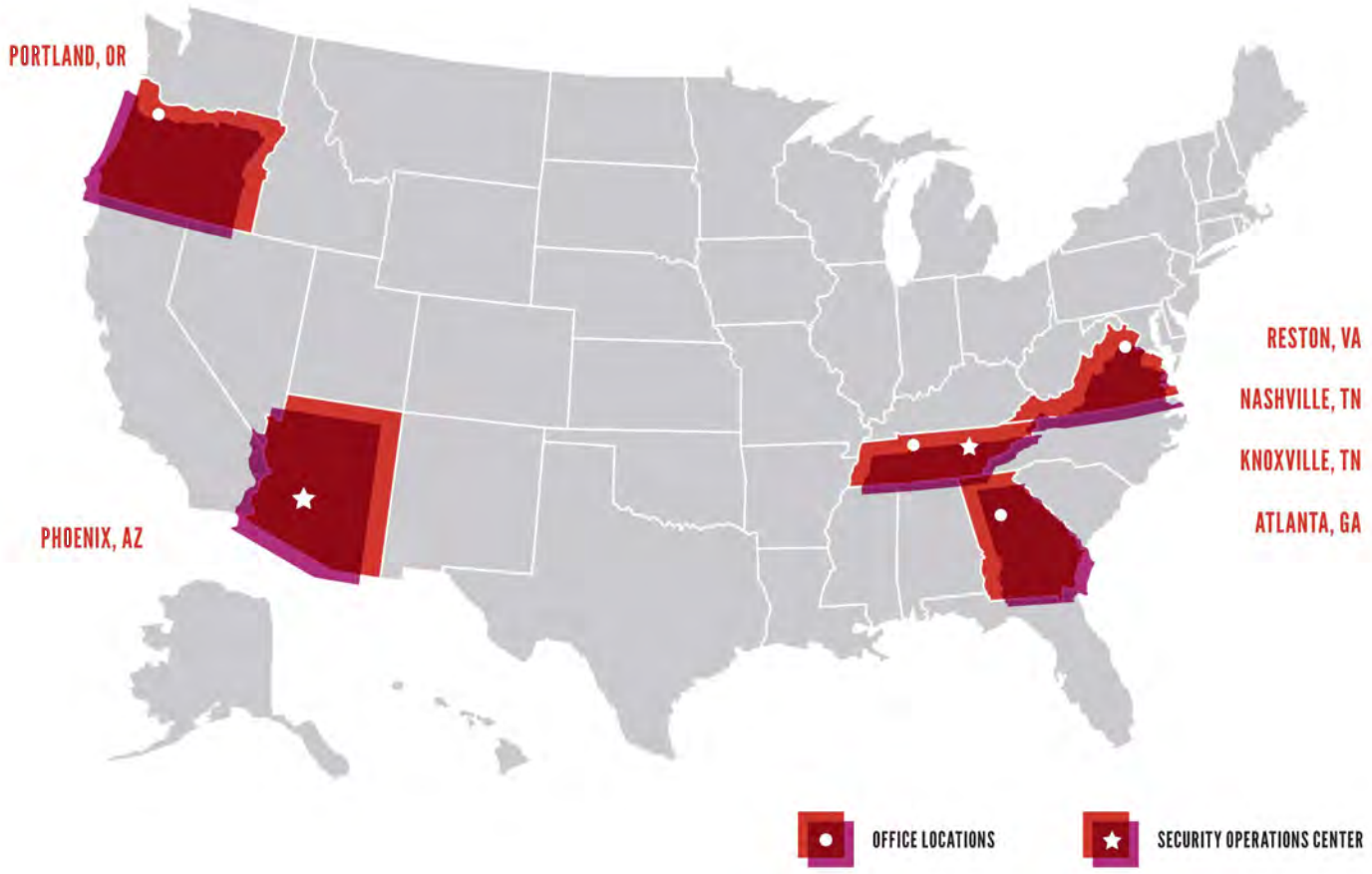
Alternative Approach

An alternative is a hybrid approach in which companies spend cap-ex dollars to purchase the tools (SIEM) and then hire an MSSP to set up, configure, monitor, report and manage the system. This scenario can also be utilized for training of internal analysts for clients who want to eventually take over a SOC operation of their own.

Summary

The best way to prevent damage to any business is to detect and remediate attacks before or as they happen. There is no one simple answer when making a choice on how to manage a SOC. Each organization must carefully consider how each factor impacts their specific needs, and which method best fits the way they do business.

NATIONWIDE COVERAGE
LOCAL DELIVERY



ABOUT AVERTIUM

Avertium, one of the largest cybersecurity services providers to the mid-to-enterprise market, is redefining the landscape with its distinctive show-no-weakness approach. Forged out of three award-winning cybersecurity services companies, each with a unique perspective on the security landscape, Avertium brings enterprise-level security to the many mid-sized and larger organizations that don't have access to comprehensive, specialized protection. More than 1,200 organizations in industries ranging from financial services and manufacturing, to technology and healthcare benefit from Avertium's managed security, consulting and compliance services delivered with more rigor, more relevance, and more responsiveness. The company's dual security operations centers are located in Arizona and Tennessee.

Avertium. Show No Weakness.™

AVERTIUM

+1 (877)-707-7997
hello@avertium.com
www.avertium.com