Trustwave®

An Executive's Guide to Budgeting for Managed Detection and Response

Examination of Managed vs. Self-Managed Models

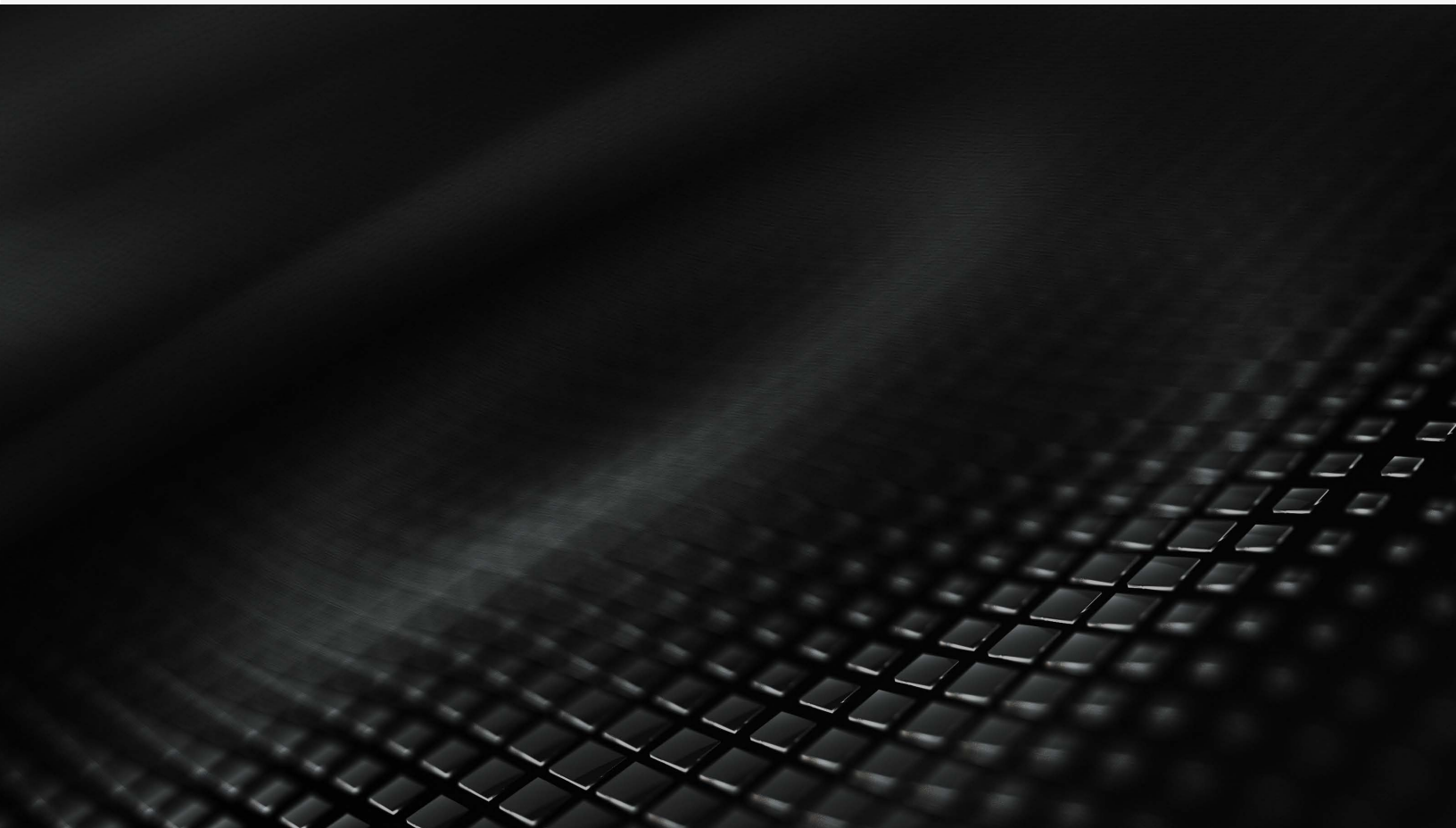


Table of Contents

Executive Summary

Organizations around the globe are under a persistent threat of becoming a target of a cyber-attack or the victim of a cybercrime. To properly identify, contain and eradicate these relentless threats, it is imperative that your security operations include effective platforms, processes and people.

With nearly 70 percent of business leaders reporting that their cybersecurity risks are increasing, and the average cost of a data breach is $3.92M, enterprises are feeling the pressure to implement solutions to help ensure they're protected (Accenture, 2020). Managed detection and response (MDR) providers that can harden security postures and implement operational protocols are becoming highly sought after as a means to guard against a breach as well as to provide immediate cost benefits in both infrastructure and personnel throughout an organization.

Global cybercrime costs are expected to grow by 15 percent per year over the next five years, reaching $10.5 trillion USD annually by 2025, up from $3 trillion USD in 2015. (Cybersecurity Ventures, 2020).

To adapt to these ever-increasing cyber threats, organizations have found it necessary to continually expand the size of their cybersecurity teams to detect, analyze and respond to cybersecurity incidents—and even after these investments, the average time to discover a breach remains 280 days. Some larger enterprises may even establish their own Security Operations Center (SOC) staffed with security analysts and engineers as well as managers who oversee security operations. SOC staff work close with organizational incident response teams to ensure security issues are addressed quickly upon discovery, but these Herculean tasks come with a hefty price tag and can also be outsourced to specialists.

Determining the best combination of people, process and technologies needed to keep their organizations safe from potential threats both now and in the future is a daunting task.

The goal of a threat detection and response team is to protect customer and organizational data and assets from cybercriminals. Whether you have a self-managed cybersecurity team or a managed detection and response provider, the end goal is the same: keeping your organizational network secure. However, having a cybersecurity strategy that is expensive, but ends up being ineffective or incapable of preventing cyberattacks, can not only invite financial disaster but can cause irreparable damage to your organization's reputation, leaving your customers unwilling to trust an organization that can't protect their personal information.

A cost analysis for managed detection and response versus a self-managed cybersecurity program is one of the most responsible first steps you can take to identify which method of defense is the most effective and cost-efficient way to provide the highest level of cybersecurity throughout the organization.

On average, establishing a SOC costs $2.86M or more (Ponemon Institute, 2020). While that is an impressive amount of capital outlay, it is still much less than the $3.86M dollar-average cost of a data breach (CSO Online, 2020). As a result, companies are realizing the benefits to investing in a robust cybersecurity program.

While the case for implementing cybersecurity measures is clear, many leaders responsible for establishing and maintaining their company's security protocols are unsure how to identify if a large investment—like establishing a SOC—is going to protect the business from potential security threats in the most cost-efficient manner. Are more superior and cost-effective alternatives available? The short answer is yes, there are alternatives to an in-house SOC that can improve organizational security, bring down operational costs, and drive a higher return on investment (ROI): Managed Detection and Response.

There is a clear need to protect your business from threat actors who possess the potential to instantly destroy your reputation. Large enterprises may have had a head start in allocating the budgetary investment needed to address this challenge. However, small and mid-sized businesses may not be in the same state of readiness, either because they don't have the budget to allocate, or they think they're immune from an attack due to the size. Unfortunately, nearly half of all cyberattacks are aimed at small businesses (CNBC, 2020), leaving them even more vulnerable than their enterprise counterparts.

Small and mid-sized businesses must utilize all their resources efficiently and intelligently to solve for a challenge that is neither their core business nor their area of expertise. This makes it imperative that all available resources are allocated to the right place, for the right people, with the right systems and tools. Working with a Managed Detection and Response provider can be a cost-effective way for small and mid-sized business to implement robust and thorough protections without the large capital investment and ongoing costs to maintain and staff a SOC.

Cybersecurity should be considered a fundamental requirement for is paramount to every company, regardless of size or industry. The threat of cyber-attacks increases exponentially every day, and the financial costs and long-term impact to an organization can make or break the business. The shortage of cybersecurity personnel continues to make finding staff increasingly difficult—and expensive. Structuring the process, procedures, and team to combat the ever-evolving threat landscape is both costly and time-consuming. Alternatively, the immediate expertise, advanced tools, and field-tested procedures that the right managed detection and response provider brings to bear can deliver the same or often better results at a fraction of the cost over building your own in-house capability.

In this white paper, we will outline the hard and soft costs in building a modern in-house security operations capability. **A more customized cost review can be found online:** ***Self-Managed Detection and Response Cost Analysis Calculator*****.**

Introduction

The cost of an effective cybersecurity strategy continues to increase exponentially. Endpoint management, intrusion detection, malware and ransomware monitoring, and compromised environments make it increasingly difficult for enterprises to maintain a secure perimeter with their limited resources. Organizations are also required to store and manage various types of data, which they are legally and ethically bound to protect from threat actors.

Studies indicate that close to 60% of all businesses that fall victim to cyberattacks end in closure, indicating the gravity of the issue (Inc. com, 2018). Without dedicated security operations personnel and tools, a managed security services provider (MSSP) or a Security Operations Center (SOC) to detect and monitor security incidents across networks, organizations are left completely vulnerable to a host of cyberthreats.

Self-Managed Cybersecurity Program vs Managed Cybersecurity Program: Overview, Challenges, and Solutions

The cybersecurity team or center is your first line of defense against threat actors ready to gain unauthorized access to your organizational network or environment. Due to the very nature of the Internet and electronic communications, it is extremely difficult to continuously develop a strong security posture and maintain the strength of your perimeter to protect your employees, your customers, and your critical and important company data.

Primarily, the SOC is responsible for the detection, containment, and eradication of security threats, so that the ecosystem remains free from vulnerabilities. Although quite a few businesses have an in-house SOC, they continue to remain vulnerable to security threats. This is due to the lack of resources dedicated to security tools and other essentials.

Self-managed cybersecurity programs

A self-managed cybersecurity program is a centralized unit of an organization which closely works with the IT and Development teams and is responsible for an organization's overall cybersecurity. This unit is comprised of advanced security tools and highly specialized cybersecurity experts that work 24 hours a day, 7 days a week, and 365 days per year to keep track of anomalies and to detect security threats in real-time. In this case, the company invests capital towards security tools for monitoring and tracking incidents and dedicates operational budget towards maintaining the tools as well as training and development of specialized staff. According to a survey, over 50 percent of cybersecurity professionals admitted that they had received less than twenty hours of training, which is obviously completely insufficient (Tech Republic, 2019). Therefore, unless an organization is fully capable of investing in cybersecurity architects, engineers, and tiered analysts with enterprise-level tools, it is advisable to avoid setting up an in-house threat detection and response operation.

A managed SOC and managed detection and response service both involve engaging a Managed Security Service Provider (MSSP) who takes care of your cybersecurity needs in exchange for a recurring subscription fee. Depending on your current business processes and your IT infrastructure, you can choose to secure specific endpoints or invest in a comprehensive security plan. In this case, the MSSP uses its own security tools and professionals to identify, report, and manage security incidents, thus ensuring that the business engaging their services has the best and most current protections, without the ongoing capital investment.

Challenges involved in setting up an in-house cybersecurity program

Building and setting up an in-house cybersecurity program with threat detection and response capabilities can mean different things to different businesses. Organizations in different verticals will likely have different priorities in terms of what they're protecting. While a hospital system might place a high priority on protecting patient records, they might pay less attention to email servers, for example. Alternatively, a retailer's main concern may be in maintaining PCI compliance over the credit card information they're collecting and could potentially overlook security in another aspect of their business.

And while the set-up and management costs are typically the main concerns, there are others that are often overlooked. Some of the other core challenges involved in setting up a state-of-the-art self-managed detection and response team include such things such as ongoing staffing and training concerns, and the continuous maintenance for the required hardware, software, and tooling,

Financial and budgetary constraints

According to a survey, close to 2.5 percent of the GDP of all businesses in the world are invested in cybersecurity services. Although this might translate to under 2 percent of a larger company's operational costs, it could encompass up to 4 percent in the cases of small and mid-sized businesses. (InfoSecurity Magazine, 2020).

In fact, due to the steep costs involved in setting up SOCs, a majority of small businesses entirely skip this or set up a namesake self-managed cybersecurity program, which does not exclude them from the predatory eyes of cybercriminals. Almost 44 percent of all security threats are launched against small businesses, out of which at least 14 percent are unprepared to defend against (CNBC, 2020). This could be fatal for a company's existence, even more so now due to the considerably larger attack surface, a result of the increased number of remote workers (and therefore endpoints).

Nearly half of organizations claim that limited budget is one of a handful of barriers they face when it comes to IT security. (Malwarebytes, 2019) This accentuates the fact that many small businesses remain vulnerable to cyberattacks due in large part to budgetary constraints.

Staffing and training cybersecurity SOC

Cybersecurity professionals work around the clock, monitoring technologies that detect and notify them of anomalies or deviations. Therefore, even the smallest cybersecurity entity would need a team of at least twelve cybersecurity professionals to maintain reasonable coverage 24/7/365. Another reason an internal SOC requires a large number of team members is the fact that most cybersecurity professionals are highly specialized in certain areas. Therefore, several different individuals would be needed to handle threats, systems, rules and content as well as the network around the clock. Moreover, cybersecurity professionals are a rare breed, so headhunting is anything but easy; there is a shortage of cybersecurity professionals that consistently leaves more than 13 million positions unfilled, so they can afford to be picky about their jobs and frequently change jobs in pursuit of more money and better benefits; organizations are typically willing to pay a premium for skilled professionals. Additionally, the average annual salary paid to a cybersecurity professional is around just shy of $76,000, and for a fully staffed organization the total salaries of a complete team can exceed a million dollars per annum (PayScale, 2020).

Organizations typically have varying level of experts as part of their cybersecurity team. This includes SOC analysts, security architects, content administrators, and cloud architects and engineers. The minimum salary per year for the lowest level SOC analyst is $75,000 per year and an experienced analyst can earn more than $120,000 per year. More specialized positions are also in the $200,000+ per year salary range. The right staff within a SOC is an inescapable cost that may be overlooked when a company is scoping an internal SOC.

Maintaining the correct hardware, software, and cybersecurity tooling

A SOC is responsible for ensuring that the necessary security measures are implemented, which requires a team to monitor the impact of all the software applications and hardware have on the network's security. They also need to manage hundreds and thousands of notifications indicating security incidents and anomalies; if this is done manually, it may require a significant number of staff hours.

Management of mean time to detect (MTTD) and mean time to respond (MTTR) is at the forefront for all InfoSec professionals. The sheer number of events, incidents, and problems are massive for companies. The larger the company, the more there is to monitor and manage. Systems, software and tooling are other mandatory costs, and if more innovation and advanced MDR capabilities are required, these can exponentially increase costs. According to a study, the average time taken to identify and contain security breaches is 280 days (IBM, n.d.). This can be reduced by using technologies such as artificial intelligence and machine learning; however, deploying these technologies and using them effectively requires specialized professionals who are experienced with these tools.

Endpoint management across the enterprise

In an organization, there may or may not be uniformity in technology, which can create siloes and a number of challenges managing endpoints. Networks are ever-growing, and the addition of bring-your-own-device (BYOD), remote workspaces and employees, and expansive cloud technologies make endpoint management extremely challenging for any enterprise, but even more so for small to mid-sized companies. The diverse technologies used by businesses can make it nearly impossible to avoid the multiplicity of security tools. Building an in-house cybersecurity program requires investing in several network monitoring and detection tools, data collection and data monitoring appliances, and device management solutions which must then be administered by experienced individuals.

Compliance and Governance

Complying with government mandated data security rules and regulations requires businesses to classify their datasets and protect them accordingly. Businesses handle different types of data from customer and organizational data to jointly owned intellectual properties. This data is comprised of financial and health-related information, personally identifiable data, and a variety of other sensitive or proprietary information that could be protected under a specific law or regulation. The various compliance mandates that apply to an organization can vary greatly depending on the nature of your business, its size, and the place of operation. Compliance and governance are essential for curbing insider threats as well, as they affect more than 1 out of every 3 businesses worldwide, every single year (Tech Jury, 2020).

Depending on the scope of your business operations, you might have to comply with regulations such as the General Data Protection Regulation (GDPR) which protects the personal information of the citizens of the European Union. Likewise, the Health Insurance Portability and Accountability Act of 1996 (HIPAA) applies to the private medical data of the US citizens and others. There are also other sector-specific regulations such as the Payment Card Industry Data Security Standard (PCI DSS), which maintains specific security guidelines for businesses accepting online payments.

Hiring professionals who are experienced in ensuring compliance with a diverse set of rules and regulations can be both expensive and difficult. Adding to the enormous cost of a security breach, is the potential for severe fines and penalties, to the tune of hundreds of million dollars in settlements (The National Law Review, 2020). Working with a managed detection and response provider can help you better scale your compliance program by helping you avoid additional staffing costs and legal penalties associated with a protracted data breach.

Advanced Threat Hunting and Eradication

We live in times when cybersecurity risks are at an all-time high, and there is no point waiting for an attacker to come up with a ransom note. Instead, your SOC and cybersecurity teams must be proactive, run open-ended searches, and look for and eliminate vulnerabilities and threats alike. This involves gathering deep insights, such as finding the indicators of compromise, security analytics, adversary threat intelligence, and endpoint security. This again requires a high level of expertise and the use of appropriate resources to identify and eradicate these threats or vulnerabilities in an organization's network.

Components of a Self-Managed Cybersecurity Program: Security Tools

Given the numerous challenges involved in setting up a self-managed cybersecurity program, you might wonder if your business can realistically run an efficient and fully functional SOC. After all, the stakes are high, and the slightest misstep could lead to heavy business losses. Following is a description of the standard SOC toolkit that you will need to invest in to maintain a strong security posture by providing MDR services internally.

Security Information and Event Management (SIEM)

Security Information and Event Management (SIEM) helps businesses gather useful data from the organization's security tools and make sense out of it. SIEM starts with log aggregation, which involves compiling notifications from the various security technologies — firewalls, antivirus console, wireless access points, active directory, and others. SOC service providers can offer additional solutions to solve your cyber challenges when you employ their SIEM solutions.

SIEM solutions can help companies maintain compliance requirements as well as to detect hidden cybersecurity threats through cross-correlation and analysis of all the raw event logs from across the entire network. Also, SIEM records full configurations of applications running across various devices to keep track of unauthorized changes and potentially dangerous events.

Intrusion Detection and Prevention System (IDPS)

Intrusion Detection and Prevention System (IDPS) is a combination of Intrusion Detection Systems (IDS) and Intrusion Prevention Systems (IPS). Primarily, IDS monitors network traffic for indications of an attack, alerting administrators to possible attacks, often caused due to the nefarious activities of malicious threat actors. It also plays a pivotal role in detecting policy violations and malware introduction through external and internal forces.

IPS is a security protocol that denies network traffic based on security profiles. Usually, there are two types of IPS — signature-based and anomalies-based. IDPS then refers to the combined functions of the IDP and IDS. Doing this in a self-managed SOC requires the organization to invest in the technologies as well as professionals who can aggregate the data and interpret it. The cost of deploying IDPS tools begins at $10,000 depending on the size and requirements of an organization. (Planet, 2018)

Endpoint Detection and Response (EDR)

Endpoint threat detection and response can be a powerful defense against attempts made to breach an organization's security. With the ever-growing number of endpoints as the result of smartphones, laptops and the explosion of remote workers, the threat landscape today is bigger than ever before. EDR involves deploying a set of tools specifically designed to detect and investigate endpoints for anomalies and suspicious activities, allowing companies to proactively monitor their security perimeter and respond effectively to threats.

Security Orchestration Automation and Response Tech (SOAR)

SOAR (Security Orchestration, Automation and Response) refers to a stack of software applications that can collect security threats from various sources and automatically respond to low-priority incidents, without human intervention. Such a solution can stop many potential threats in the initial stages and help reduce the burden on cybersecurity professionals, allowing them to focus on more important incidents.

Primarily, SOAR includes three sets of technologies — threat and vulnerability management, security incident

response, and automation of security operations. The threat and vulnerability technologies refer to remediation technologies and how the incidents need to be managed when they occur. The second set of technologies, the security incident response, refers to those that define how the organization intends to respond to the various security incidents. Finally, the security operations automation is responsible for policy execution, incident reporting, and additional actions. MDR service providers have the expertise to combine technologies to safeguard organizations, making the incident detection and response time by professional cybersecurity providers much faster.

Malware and Ransomware Protection

Ransomware attacks continue to haunt the public and private sectors alike. In this type of attack, the threat actor makes use of a file-encrypting software and demands a ransom in exchange for the decryption key. Although this type of attack often makes headlines when deployed on a public sector agency, it has an equal—if not greater—impact on the private sector. A Trustwave survey of 996 IT professionals revealed that over half had experienced ransomware or phishing attacks in the past year. (Trustwave, 2020)

Businesses that experienced a ransomware attack reported sustained damages over $500,000; roughly 40 percent of MSPs and IT professionals believe their organization could not withstand that kind of damage. Many businesses would experience irreparable damage in the event of a successful ransomware attack. (NinjaRMM, 2020)

Managed detection and response providers offer a deep focus on proactively eradicating threats with a combination of human-led, proactive threat hunting, we pursue threats, actively looking for threat actor in your environment. If we see something happening in one customer environment, we will look at your environment to see if it is happening there as well. An experienced managed detection and response provider is an expert in understanding and eradicating threats. Experts use a combination of tools and human-led proactive threat hunting and continuous threat research to stay one step ahead of the attackers.

Threat Intelligence Solutions

Threat Intelligence is the amalgamation of incident tracking and attribution, which helps identify bad actors attempting to stage an attack or breach your environment. These intelligence feeds allow the cyber community to share information about the latest attacks, patterns, behaviors, and signatures used. Information that cybercriminals often leave behind are IP addresses, file hashes, and filenames that can enable a professional to conclude who is responsible for it. This information adds to your program's knowledge and allows your systems to adapt appropriately to the current threat landscape. Monitoring, updating and correlating these insights are labor-intensive tasks that are best performed by a highly skilled expert.

Governance and Compliance Solutions

Enterprises are aware of GDPR, HIPAA, and other compliance requirements that are specific to each industry. You need to have a sound governance and compliance roadmap that guides your employees and contractors about the do's and don'ts from a security perspective. Maintaining compliance in your country, state, or city is important, but also providing your customers and clients with the assurance of a secure environment is of the utmost importance. Organizations typically use a combination of tools to measure compliance.

Cost-Analysis of Self-Managed SOC

As previously mentioned, the potential costs involved with establishing and maintaining an in-house SOC can be prohibitive to most organizations, particularly when compared to leveraging a reputable MDR provider.

No Standard Framework

There is no standard framework for developing a comprehensive cybersecurity or SOC strategy. The NIST framework has become a referenced voluntary standard but has many challenging and costly components. This makes an in-house program even more costly because organizational needs often change from year to year or even month to month. With every new technology adopted and every operational change—in every department— the attack surface changes and therefore can potentially require an entirely new approach. Process, procedures, and training are all pieces of the framework for a successful cybersecurity program and enterprises need a simplistic way to be assured all items are addressed.

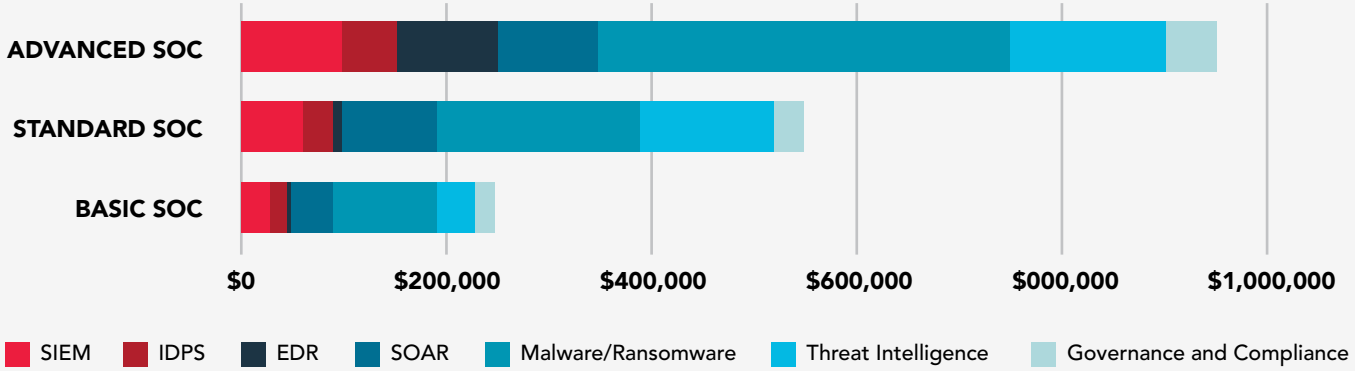
For example, the COVID-19 outbreak compelled businesses to allow employees to work from home, and very few organizations were prepared for it. As a result, an increase in the number of security breaches and policy violations were reported. On the other hand, there were companies that outsourced their security operations to providers that adapted, implemented processes to support the needs of each company individually, enacted repeated penetration tests, and repaired vulnerabilities with the appropriate security patches.

An organization needs to have a cybersecurity strategy that can handle all types of emergencies and changes in standard operating procedures while maintaining a secure environment. Since setting up an in-house SOC is an expensive proposition that can result in high operational costs, it often makes more sense for a company to outsource their cybersecurity needs to a Managed Detection and Response provider with flexible and innovative capabilities.

Budgeting for your Security Tools

Cybersecurity teams require a diverse set of resources for event and incident investigation, threat detection, response, and remediation and leverage several security tools from which meaningful data can be monitored, sourced, aggregated, and analyzed. The following chart provides estimated costs.

Self Managed SOC Tools: Annual Costs



Budgeting for your Security Team

As mentioned earlier, businesses that wish to set up an in-house cybersecurity team incur significant set-up and maintenance costs. Below are cost models for staffing a basic, standard or advanced SOC.

Basic SOC Elements	Annual Expense
6 Technicians ($75,000 salary)	$450,000
6 Mid-Senior Level Employees ($95,000 salary)	$570,000
Expert-level Professionals	---
HR Recruitment Costs* (10% of Salary Costs)	$102,000
Training and Development Costs (20 hours at $200/hour)	$48,000
Subtotal: Staffing	**$1,170,000**
Basic Monitoring, Tracking and Remediation Security Tools (from Chart 1)	$250,000
Total: Staffing + Tools	**$1,420,000**

Standard SOC Elements	Annual Expense
4 Technicians ($75,000 salary)	$300,000
4 Mid-Senior Level Employees ($95,000 salary)	$380,000
4 Expert-level Professionals ($120,000 salary)	$480,000
HR Recruitment Costs* (10% of Salary Costs)	$116,000
Training and Development Costs (20 hours at $300/hour)	$72,000
Subtotal: Staffing	**$1,348,000**
Advanced Monitoring, Tracking and Remediation Security Tools	$550,000
Total: Staffing + Tools	**$1,898,000**

Advanced SOC Elements	Annual Expense
6 Technicians ($75,000 salary)	$450,000
6 Mid-Senior Level Employees ($95,000 salary)	$570,000
6 Expert-level Professionals ($120,000 salary)	$720,000
HR Recruitment Costs* (10% of Salary Costs)	$159,000
Training and Development Costs (20 hours at $500/hour)	$72,000
Subtotal: Staffing	**$1,971,000**
Specialized Monitoring, Tracking, Remediation and Threat Hunting Security Tools	$950,000
Total: Staffing + Tools	**$2,921,000**

* HR recruiting costs are subject to increase depending on the attrition rate.

Training and Certification

Cybersecurity is an ever-evolving discipline, which means there is literally new information that needs to be learned all the time. To keep up with the dynamics of this profession, organizations must provide their cybersecurity team with the required training and certification opportunities. As a matter of fact, over 70 percent of Information Systems Security Association (ISSA) companies have been impacted by the cybersecurity skills shortage and 45 percent believe it has worsened. The top ramifications of this skills shortage include an increasing workload, unfilled open job requisitions, and an inability to learn or use cybersecurity technologies to their full potential. (Information Systems Security Association, 2020).

Cost Analysis of Managed Detection and Response (MDR):

Protecting your enterprise from threats is of the utmost importance. Seventy percent of breaches were from outside bad actors and 86 percent of breaches were financially motivated. Organizations—regardless of size or industry— need solutions to solve their cybersecurity challenges and look to managed detection and response. There are both financial and operational benefits to leveraging an MDR provider to protect your organization.

Removes the Requirement to build an in-house Cybersecurity program

The cost of developing and building an in-house cybersecurity strategy is well-chronicled and expensive. People, process, and tools all represent immediate and ongoing financial costs for enterprises of all sizes.

Reduces maintenance and support costs

Systems, software and tools are essential to every security organization. In addition to the upfront purchase costs, there is ongoing maintenance and support costs, which are typically 15 to 25 percent of the annual cost of the system or software. The need to completely refresh, update or replace hardware or software as organizational improvements are made or processes change. A managed detection and response provider eliminates this cost for your organization, as the contract with an MDR provider allows for agility to scale up or down as organization needs change.

"Trustwave provides Managed Detection and Response for clients of all sizes in a wide variety of industries. A major law firm leveraged them to extend security coverage, quality and reliability at a fraction of the cost of maintaining these capabilities internally. "Trustwave was unique in seeking first to understand our industry and environment, then partnering with us to customize the best possible service plan to achieve our security objectives. It was a true partnership from the beginning and my team can now focus on broader risk management strategies,"

CISO, AMLaw 100 Firm.

Detect and remediate threats by gaining endpoint visibility across your enterprise

Enterprises and networks expand and multiply frequently. The management of these networks is best handled by cybersecurity experts who have the industry-leading tools, systems, and software to manage and view all endpoints. Visibility is a challenge for many companies and this challenge often leads to threats not being detected quickly—or accurately. A managed detection and response provider's sole focus is to detect and remediate threats in conjunction with your team. The visibility, the process, the procedures, and the actions can help save days and hours from the average time to detect threats or breaches to your environment.

Reduces the need for personnel staffing, hiring, and training

SOC personnel requires highly specialized cybersecurity experts at all levels. This includes first and second tier analysts, architects and engineers supporting the network, and the team required to continuously update systems and hunt for threats. By opting for a managed detection and response provider, the challenge of hiring, training and retaining these individuals is removed. An expert MDR provider not only alleviates these costs, they often deliver a high level of customer satisfaction service to their client companies.

Reduces the possibilities of non-compliance, fines, and penalties

Governance, compliance, audits, and the preparation to adhere to these requirements and standards is costly. The fines and associated penalties for not adhering to these requirements even more so. By selecting a managed detection and response solution, organizations reduce their risks liability exponentially, as their provider is likely well-versed in the technical requirements for various regulations and can provide the necessary services as part of their contract.

> "Trustwave helped us secure more than 75,000 endpoints and IoT devices across 400 different sites. They provided proactive monitoring to identify issues on a device level before they impacted the entire network. Automation and clear, centralized policy management helped us rein in costs while improving reliability"
>
> Chief Information Security Officer, major transportation and transit organization.

> "The big concern is not knowing what you don't know, and it's very hard to find in-house people with the necessary expertise. These exercises are always very eye-opening. Trustwave helps us find evolving vulnerabilities and helps us increase awareness among employees about possible threats"
>
> Chief Information Security Officer, major Icelandic bank.

Do-It-Yourself or Partner with a Cybersecurity Expert?

Managed detection and response (MDR) is an ever-evolving process that requires the financial commitment, time and attention of highly specialized professionals, who make use of advanced SOC tools, and most importantly the necessary systems, software, and tools. In the present economic conditions, taking on these expenses to establish and maintain an internal SOC not be feasible for some larger businesses and a majority of small to mid-sized companies. The ability to do more with less and receive a higher ROI from your investment is a critical cost-saving business practice. The ability to leverage an experienced and reputable partner to develop and manage a thorough cybersecurity program could be the difference between the success or the collapse of an organization.

To get the most out of your budget and still receive the highest ROI for your investment, contracting the services of an MDR service provider can do just that. An MDR service provider can all but eliminate the costs associated with establishing and maintaining an internal SOC, by allowing clients to leverage industry experience and expertise, utilize the correct and most current systems and software, and gaining the expertise of a focused and specialized team.

Trustwave Managed Detection and Response Summary

Your job is to keep your business moving. Our job is to stop threats so that your business can keep moving. Period. We embed our elite expertise and proven threat lifecycle capabilities into your security program and environment to help you identify threats, investigate the depth and scope of those threats, and help you respond by taking containment actions. We partner with companies of all sizes and industries to eradicate threats. All day. Every day.

With a customer-centric approach, Trustwave integrates our services with our clients' security environments and programs – not the other way around – to provide complete visibility across endpoint, network and cloud to proactively eradicate threats.

Learn more about Trustwave Managed Detection and Response *here*.

And, complete your research on Managed Detection and Response financials, by visiting our online *Self-Managed Detection and Response Cost Analysis Calculator*.

Bibliography

Accenture. (2020). Retrieved from https://www.accenture.com/_acnmedia/PDF-116/Accenture-Cybersecurity-Report-2020.pdf

Acronis. (2020). *Buy Acronis Cyber Backup.* Retrieved from Acronis: https://www.acronis.com/en-us/business/backup/purchasing/

CDW. (2020). *Symantec Endpoint Protection Endpoint Detection and Response - initial subs.* Retrieved from CDW: https://www.cdw.com/product/symantec-endpoint-protection-endpoint-detection-and-response-initial-subs/5254378

CNBC. (2020, March 9). *SMALL BUSINESS PLAYBOOK.* Retrieved from CNBC: https://www.cnbc.com/2019/10/13/cyberattacks-cost-small-companies-200k-putting-many-out-of-business.html

Computer.org. (2015). *A Framework for Designing a Security Operations Centre (SOC).* Retrieved from Computer.org: https://www.computer.org/csdl/proceedings-article/hicss/2015/7367c253/12OmNAHmOvg

CSO Online. (2020, March 9). *Top cybersecurity facts, figures and statistics for 2020.* Retrieved from CSO Online: https://www.csoonline.com/article/3153707/top-cybersecurity-facts-figures-and-statistics.html

CSO Online. (2020, August 13). *What is the cost of a data breach?* Retrieved from CSO Online: https://www.csoonline.com/article/3434601/what-is-the-cost-of-a-data-breach.html#:~:text=The%20average%20cost%20of%20a,over%20the%20last%20five%20years.

Cybersecurity Ventures. (2020, November 13). *Cybercrime To Cost The World $10.5 Trillion Annually By 2025.* Retrieved from Cybercrime Magazine: https://cybersecurityventures.com/hackerpocalypse-cybercrime-report-2016/

Datacenter Knowledge. (2019, May 14). *SIEM Pricing Models Set for a Shake-Up.* Retrieved from Datacenter Knowledge: https://www.datacenterknowledge.com/security/siem-pricing-models-set-shake

Datto. (2018, December). *https://www.datto.com/resource-downloads/Datto2018_StateOfTheChannel_RansomwareReport.pdf.* Retrieved from Datto's State of the Channel Ransomware Report: https://www.datto.com/resource-downloads/Datto2018_StateOfTheChannel_RansomwareReport.pdf

IBM. (n.d.). Retrieved from https://www.ibm.com/security/data-breach

Inc.com. (2018, May 7). *60 Percent of Small Businesses Fold Within 6 Months of a Cyber Attack. Here's How to Protect Yourself.* Retrieved from Inc.com: https://www.inc.com/joe-galvin/60-percent-of-small-businesses-fold-within-6-months-of-a-cyber-attack-heres-how-to-protect-yourself.html

Information Systems Security Association. (2020, July). *The Life and Times of Cybersecurity Professionals 2020.* Retrieved from Information Systems Security Association: https://2ll3s9303aos3ya6kr1rrsd7-wpengine.netdna-ssl.com/wp-content/uploads/2020/07/ESG-ISSA-Research-Report-Cybersecurity-Professionals-Jul-2020.pdf

InfoSecurity Magazine. (2020). *Is Effective Cybersecurity Expensive?* Retrieved from InfoSecurity Magazine: https://www.infosecurity-magazine.com/blogs/effective-cybersecurity-expensive/

International Federation of Accountants. (2018, June 27). Foundation for Economies Worldwide = Small Business. Retrieved from International Federation of Accountants: https://www.ifac.org/knowledge-gateway/contributing-global-economy/discussion/foundation-economies-worldwide-small-business

Malwarebytes. (2019, October). *SMBs lack resources to defend against cyberattacks, plus pay more in the aftermath.* Retrieved from Malwarebytes: https://blog.malwarebytes.com/business-2/2019/10/smbs-lack-resources-to-defend-against-cyberattacks-plus-pay-more-in-the-aftermath/

Network World. (n.d.). *Building an IDPS without big iron.* Retrieved from Network World: https://www.networkworld.com/article/2185763/building-an-idps-without-big-iron.html#:~:text=Companies%20seeking%20to%20deploy%20intrusion,alternatives%20might%20fit%20the%20bill.

NinjaRMM. (2020, May). *To Pay or Not to Pay: Introducing the 2020 Ransomware Resiliency Report* . Retrieved from NinjaRMM: https://www.ninjarmm.com/blog/2020-ransomware-resiliency-report/

PayScale. (2020, August 29). Retrieved from PayScale: https://www.payscale.com/research/US/Job=Cyber_Security_Engineer/Salary

PayScale. (2020, August 30). *Average Cyber Security Analyst Salary.* Retrieved from PayScale: https://www.payscale.com/research/US/Job=Cyber_Security_Analyst/Salary

Planet, e. (2018, February). *9 Top Intrusion Detection and Prevention Systems: Guide to IDPS.* Retrieved from eSecurity Planet: https://www.esecurityplanet.com/products/top-intrusion-detection-prevention-systems.html

Ponemon Institute. (2020, January 22). *Cost of a Data Breach Report.* Retrieved from IBM: https://www.ibm.com/security/data-breach

Tech Jury. (2020, August 17). *20 Insider Threat Statistics to Look Out For in 2020.* Retrieved from Tech Jury: https://techjury.net/blog/insider-threat-statistics/#gref

Tech Republic. (2019, August 29). *Cybersecurity analysts overworked, undertrained and buckling under volume of alerts.* Retrieved from Tech Republic: https://www.techrepublic.com/article/cybersecurity-analysts-overworked-undertrained-and-buckling-under-volume-of-alerts/

The National Law Review. (2020, August 3). *Court Approves Class Action Settlement in RE: YAHOO! Inc.* . Retrieved from The National Law Review: https://www.natlawreview.com/article/court-approves-class-action-settlement-re-yahoo-inc-customer-data-security-breach

Trust Radius. (2020). *Threat Intelligence Platforms.* Retrieved from Trust Radius: https://www.trustradius.com/threat-intelligence-platforms#:~:text=Threat%20intelligence%20pricing%20is%20often,on%20the%20number%20of%20feeds.

Trustwave. (2020, October). *2020 Trustwave Data Security Index.* Retrieved from Trustwave: https://www.trustwave.com/en-us/resources/library/documents/2020-trustwave-data-security-index/

ZNet. (2019, January 16). *North Korean hackers infiltrate Chile's ATM network after Skype job interview.* Retrieved from ZNet: https://www.zdnet.com/article/north-korean-hackers-infiltrate-chiles-atm-network-after-skype-job-interview/

Trustwave is a leading cybersecurity and managed security services provider focused on threat detection and response. Offering a comprehensive portfolio of managed security services, consulting and professional services, and data protection technology, Trustwave helps businesses embrace digital transformation securely. Trustwave is a Singtel company and the global security arm of Singtel, Optus and NCS, with customers in 96 countries.
For more information about Trustwave, visit *www.trustwave.com.*

Trustwave®