Stratecast | FROST & SULLIVAN

SOC-as-a-Service versus DIY SOC

The Business Case for AWN CyberSOC is Compelling

A Frost & Sullivan Report

Information and Communications Technology

50 Years of Growth, Innovation and Leadership

EXECUTIVE SUMMARY

A daunting facet of a good cybersecurity strategy is balancing the act between effectiveness and cost of cybersecurity controls. How do you determine what is the total cost of ownership (TCO) of people, process and technologies that keep any organization's assets protected from cyber criminals and malicious insiders?

Today, recommendations on 'required' cybersecurity technologies are as abundant as the ever-growing variety of cyber threats. However, purchasing and installing all or even a portion of the recommended technologies and upgrades to next-generation versions would exceed the budget of most organizations. Missing is guidance on operationalizing the technologies, individually and collectively, for maximum return. For that, a competent and process-supported InfoSec team, crossing multiple disciplines, is required. However, more skilled InfoSec staff adds to an organization's recurring costs, and is challenging in today's tight InfoSec labor market. Consequently, organizations often find themselves under-equipped in the InfoSec staff, processes, and technologies needed to combat today's cyber threats and comply with regulations.

Zeroing in on a specific example is threat detection and response. For many organizations, they are inundated with a sea of suspicious events and security alerts. They cannot reliably and at scale sift through this material to identify legitimate threats, assess severity, develop and prioritize responses, and then take action—all before damage is done. They lack repeatable processes and expertise, even if they have deployed an expensive set of threat detection and response technologies. And with circumstances worsening—more logs and alerts and cyber threats intensifying—reliance on buying and managing more cybersecurity technology and increasing in-house expertise is unrealistic. New options are needed.

Fortunately, there is a viable alternative option that includes 24x7 monitoring—a critical need that is often not operationalized due to cost and complexity. In this paper, we investigated SOC-as-a-Service as a highly affordable and effective turnkey outsourcing option for threat detection and response. **In our cost analysis, we determined that organizations with few, if any, dedicated InfoSec personnel may spend up to 8.8 times more over a three-year period building and operating their own Security Operation Center (SOC), a Do-It-Yourself (DIY) approach, versus subscribing to SOC-as-a-Service (SOCaaS)—in this case, Arctic Wolf Networks (AWN) CyberSOC™ service.**

INTRODUCTION

Despite best investments in cyber defenses, cyber adversaries can circumvent preventive measures. Consequently, organizations' cybersecurity strategies must follow the dual path; prevention to reduce the attack surface, and detection and response to counter threats that circumvent prevention. While both prevention and detection/response are essential, organizations struggle with cost and operational barriers. Simply, the cost of building and equipping a DIY SOC is prohibitive, and the expertise out of reach. There is, however, a new approach to accomplishing positive threat detection and response outcomes at a price that is multiples less than a DIY SOC.

In this report we leverage our body of cybersecurity research and recent interviews with AWN CyberSOC customers to accomplish the following:

- Describe the drivers for threat detection and response
- List the essential solution requirements for effective threat detection and response
- Compare the three-year costs of SOCaaS, based on the pricing of the AWN CyberSOC service, with the costs of a DIY SOC
- Compare features of SOCaaS to a DIY SOC

BUSINESS DRIVERS FOR THREAT DETECTION AND RESPONSE

The business drivers for an effective approach to threat detection and response are summarized in three points, which we delve deeper into in the following section:

1. Cyber threats represent a growing business risk as organizations are increasingly digitally dependent.
2. With an overwhelming number of security alerts and system logs, the effort and expertise required to achieve effective threat detection is increasing.
3. Many organizations lack the InfoSec talent and headcount needed to detect and respond to threats before damage occurs.

Heightened Digital Dependency and Business Risk

In our interviews with AWN CyberSOC customers, the interviewees described the implications of cyber compromises and data breaches on their digital-dependent businesses. Avoiding these implications drove their evaluations of outsourced threat detection and response options. The table below highlights the stated implications for each company we interviewed.

BUSINESS	IMPLICATIONS OF CYBER COMPROMISES AND DATA BREACHES
Law Firm	As a recipient, retainer, and user of sensitive client data in the course of standard operations, corruption of that data and data breaches cause the risk of unrepairable damage to the law firm's reputation and client trust.
Plastics Manufacturer	Compromises to the digital supply chain can negatively affect production flow and damage the manufacturer's reputation, impact contractual obligations with suppliers and clients, and disrupt sales momentum. Of note, the manufacturer must bidirectionally guard against third-party risk: both to itself as the unintentional source of cyber threats to suppliers and clients; and vice versa, suppliers and clients as the source of cyber threats to the manufacturer's production and back-office operations.

BUSINESS	IMPLICATIONS OF CYBER COMPROMISES AND DATA BREACHES
Agricultural Products Producer	Operational and cost efficiencies have been won through digitized systems and workflows. Cyber compromises can directly impact production. Additionally, disruptions to environmental systems can impact the health of hens (a critical asset) and jeopardize compliance with food safety regulations. Also, and similar to the law firm and the plastics manufacturer, corruption of financial transaction data, or disruptions in invoicing, contribute to negative financial outcomes.
Regional Credit Union	Regulatory compliance, if not systematized, can become a recurring cause for concern, and force spikes in operational effort by the IT and security teams. In a worst case scenario, non-compliance places the credit union's charter at risk. For credit union members, they have implicit trust that the credit union is following reasonable processes and procedures to ensure their data is protected and their privacy guaranteed. If this bond of trust is tarnished or broken, retention of existing members, and attracting new members, may be impacted.

Through our interviews, common themes emerged. AWN CyberSOC was chosen for two primary reasons:

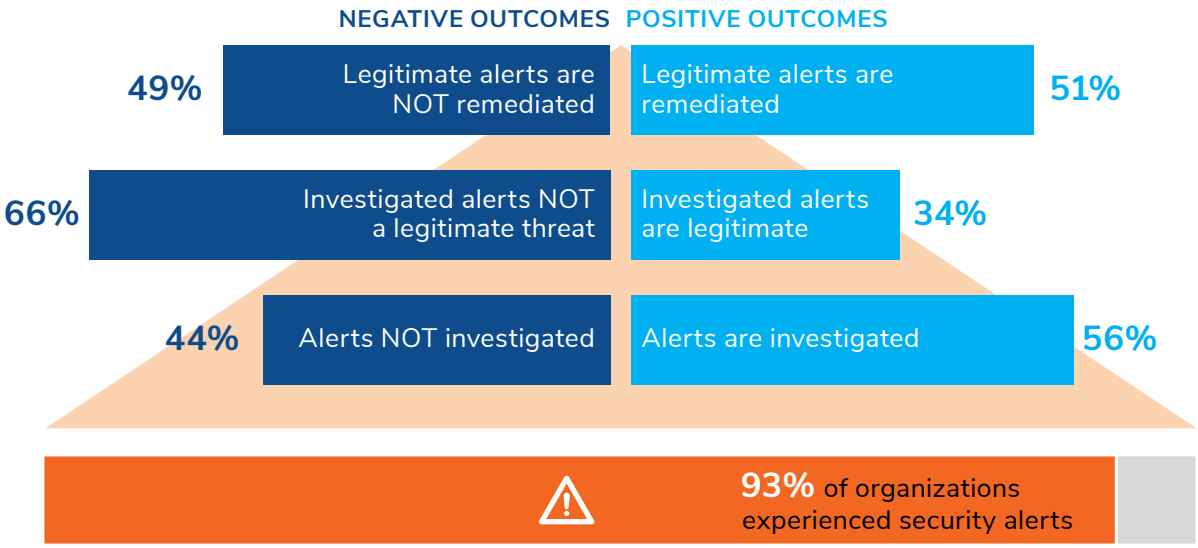
- AWN CyberSOC was overwhelmingly more cost-effective than a DIY SOC—Staffing the SOC was by far the largest cost consideration. Interviewees' perspectives varied on the number of trained personnel needed to operate a SOC, from a minimum of three to more than six; with annual compensation for each SOC staff member ranging between $80,000 and $120,000. Based on our calculations, the annual cost of SOC staffing is, at minimum, four times more than the entire cost of the AWN CyberSOC service. One customer estimated its annual SOC staffing costs would exceed $500,000; nearly 10 times what it currently pays for the AWN CyberSOC service. Adding in technologies and services necessary to equip a SOC—security information and event management (SIEM), vulnerability scanning, and external threat intelligence—the cost efficiency of AWN CyberSOC increased further over a DIY SOC. AWN CyberSOC includes all of these capabilities in its service at no extra cost.
- AWN CyberSOC has been effective—All of the interviewees expressed high levels of satisfaction with AWN CyberSOC in rapidly identifying and assessing threats, pinpointing contributing factors, and recommending prioritized actions. None of the customers have experienced a business-impacting cyber compromise or a data breach since subscribing to the service. Each interviewee also called out the high caliber expertise of the customer-dedicated AWN Concierge Security™ team (CST). Indicative of that expertise and reflective of customer intimacy, false positives have been few in number and explainable (e.g., planned changes in customer's environment or circumstances not communicated in advance to the CST). With three of the interviewed customers having three or more years with AWN, change in CST personnel has occurred. Each of those interviewees confirmed that no lapses in service quality occurred during transition. Replacement CST members came on board well versed on the customer, its environment and circumstances, and its history.

A more detailed cost comparison of SOCaaS with AWN CyberSOC pricing and DIY SOC will follow in the Cost Comparison section.

An Overwhelming Number of Security Alerts and System Logs

Although contributing factors to cyber compromises and data breaches vary, typically, there are indicators of compromise (IoC) present in advance. Unfortunately, those indicators are buried in an avalanche of system logs and security alerts, and too frequently are not understood in time to avoid damage. Illustrating this point is data on the uneven treatment of security alerts, as reported in *Cisco 2018 Annual Cybersecurity Report.*

EXHIBIT 1: **Outcomes**



Source: Cisco 2018 Annual Cybersecurity Report

For the AWN customers interviewed, a principal reason for outsourcing, and ultimately subscribing to the AWN CyberSOC service, was to overcome their deficiency in timely identification and investigation of security alerts and logs for legitimate IOCs. They stated that they lacked the technical means to collect and filter all their logs and alerts; the expertise to investigate and place IoCs into proper context; and the time to take appropriate action. In security parlance, their Mean Time To Detect (MTTD) and Mean Time To Respond (MTTR) were excessive, placing their businesses at risk.

Their experience with AWN CyberSOC, a 24x7 operation, turned this situation around. All security alerts and system-generated logs were processed, and only security incidents that mattered were escalated to the customers. When legitimate IoCs were qualified by the CST, customers were promptly notified with actionable trouble-tickets and supporting evidentiary documentation. Working directly with each customer, the CST understood which IoCs called for immediate notification, and each customer's preferred means of notification and sequence of notification if initial points of contact were non-responsive.

Lack of Dedicated InfoSec Talent

Each of the interviewees expressed a common viewpoint of many businesses: cybersecurity is not their core business, but it is essential to business resiliency. Consequently, each is prudent in its company's expenditures on cybersecurity staffing and technology, with return on investment a prime measurement. In their prudency, however, dedicated InfoSec staff members are very few in number.

The interviewees also recognized that their lack of formalized threat detection and response capabilities was a significant risk to the business, and that it had to be remedied. Moreover, relying on their limited staffs in an ad hoc and part-time basis, with technologies and processes assembled out of necessity, was incompatible with their need for disciplined and continuous cyber threat management. A new approach was required.

In their assessments, growing their IT staff to include InfoSec-dedicated members would be challenging, inconsistent with their lean staffing direction, and, as noted earlier, prohibitively expensive. InfoSec staffing challenges, in general, are a growing concern. According to the Ponemon Institute, in its *2018 Study on Global Megatrends in Cybersecurity*, 48% of the survey respondents cited 'Inability to recruit and retain qualified IT security personnel' as an operational risk today. Looking three years out, this operational risk was cited by 63%. In a similar 'today' and 'future' comparison, 19% of the survey respondents rated cyber threats as 'very frequent' today; and 42% predict that cyber threats will occur very frequently in three years.

With both the risk of cyber threats and the challenges of InfoSec staffing increasing, the companies we interviewed faced the same conundrum as countless other businesses: effectively combating the growing risk of cyber threats with a keen eye on cost efficiency. To that point we turn our attention to the next section: threat detection and response solution requirements.

THREAT DETECTION AND RESPONSE SOLUTION REQUIREMENTS

Regardless of whether an organization started with an intention to build and operate its own SOC, and then concluded that a SOCaaS approach was better, or immediately chose SOCaaS, we find the solution requirements are similar. Those requirements include the following:

- High Accuracy—The primary measure of effective threat detection and response is in identifying genuine threats, and only those threats. False positives, if a frequent occurrence, also mean that time and focus are siphoned away from true threats. A balance is required. To achieve this, human-assisted machine learning combs through the mountain of alerts and logs with speed and reliability, and confirms through context-prioritized analysis. Noted earlier, the interviewed customers gave AWN CyberSOC high marks on accuracy.
- Comprehensive Visibility—Organizations today leverage multiple IT environments to support their businesses: on-premises data centers; public cloud platforms (e.g., AWS, Microsoft Azure, Google Cloud Platform); private clouds; managed hosting; Software-as-a-Service applications (e.g., Microsoft Office 365, Salesforce, GSuite, and Box); and Security-as-a-Service offerings (e.g., Okta). Each is a potential attack surface and a source of threat intelligence. Visibility must extend to all. AWN CyberSOC is designed to retrieve and process logs and alerts across all of these environments.

- Tailored Services—Each organization is unique. Its composition of IT resources, cyber threats, and compliance requirements vary. An effective threat and response solution is tailored to each customer. Cookie-cutter approaches risk missing attacks unique to the customer. Universal among the interviewed customers, all viewed the CST as a true extension of its organization in providing threat perspectives and remediation guidance aligned with its circumstances and needs.
- Scalability—Threat detection is a big data function. The number of system logs and security alerts will fluctuate in number from day to day, but over time will unquestionably increase. Therefore, the platform supporting threat detection and response must have cloud-like attributes to scale immediately without compromising efficacy. At the same time, the solution's cost must also remain predictable. AWN CyberSOC's cloud-based platform scales without limits or delay. From a pricing perspective, AWN buffers customers from escalating charges based on number of logs and log-generating devices. Charges are determined by the number of end-users, servers, and AWN sensors; attributes grounded in the size and attack surface area of the organization, and attributes that change less frequently than number of logs and log-generating devices.

SOC ROLES AND RESPONSIBILITIES

Considerable resources are required to maintain a 24x7 SOC. Typically, a SOC team has members in two types of basic responsibilities—SOC Analysts and SOC Engineers—in addition to a SOC Manager.

- Security Analysts—These analysts typically are the first responders to security alerts that pop up on the SOC console. In military terms, they are the front-line soldiers responsible for constantly monitoring the SOC dashboard(s), triaging alerts, prioritizing the alerts that require actions, and following runbooks on how to respond in a SOC-as-a-service model. SOC Analysts are on-call in multiple shifts to cover 24x7 round the clock. Depending on the size of the organization's IT footprint (endpoints and servers), we contend that three to seven Security Analysts are needed to staff a 24x7 SOC.
- Security Engineers—These SOC members manage the SIEM platform, and create and refine correlation rules to accurately identify known threats and minimize false positives. They also merge appropriate threat intelligence (e.g., known bad IP addresses, bad URLs/domains, geo-locations, snort rules, etc.) into their rule-making and forensics analysis, and analyze new types of malware using SecOps tools. Also dependent on the organization's IT footprint, two to four System Engineers are needed to conduct these functions.
- Security Manager—A Security Manager within a SOC team is responsible for overseeing operations on the whole. This person is charged with managing team members and coordinating workflows within and between Security Analysts and Security Engineers. The Security Manager is also responsible for creating policies and protocols for hiring, and building new processes.

COST COMPARISON OF SOCaaS VERSUS DIY SOC

For our cost comparison, we first identified the prominent cost contributors to building and operating a DIY SOC.[1] As each of these items is functionally included in the AWN CyberSOC service, the functional comparison between these two options is valid.

As noted earlier on SOC staffing costs, perspectives on number of SOC staff members and compensation vary considerably. This is to be expected, given the variability in cybersecurity talent compensation in different geographic regions. To accommodate this variability, our comparison covers a range for each cost element, and the creation of aggregate low and high cost estimates. Ranges for the other SOC cost contributors are also provided, with reasons for variation.

Our cost comparison is based on a three-year total. We combined first year non-recurring costs with recurring costs to produce a three-year Total Cost of Ownership (TCO). SOC staffing, an annual recurring cost, is the most dominant cost contributor for a DIY SOC. Based on our calculations, SOC staffing costs represent 96% of total three-year DIY SOC costs. If compensation levels rise faster than other cost components, a distinct possibility in the tight InfoSec labor market, staffing's relative share of total DIY SOC costs will increase. For our comparison, we did not include allowances for cost changes over the three-year period.

DIY SOC Costs

COST COMPONENT	THREE-YEAR COST RANGE*	DESCRIPTION AND COMMENTARY
SOC Staffing	$2,310,000–$4,620,000	Staffing includes Security Analysts, Security Engineers, and a SOC Manager. Our range captures a low of three Security Analysts for a small business and seven Security Analysts for a large business; and a low of two Security Engineers for a small business and four Security Engineers for a large business. Each business would also require one SOC Manager. Annual compensation and benefits range from $120,000 to $145,000 per SOC staff member. From our perspective, around-the-clock staffing is critical to minimize the available time for intruders and malicious insiders to conduct reconnaissance, capture credentials, and start building backdoors and obfuscate their activities. Furthermore, with AWN CyberSOC operating 24 x 7, a staff of eight to 12, rather than only six staff members, is a realistic SOC requirement.

1 There are SOC cost contributors that we did not explicitly include. For instance, facilities and end-users' workstations for SOC members were not explicitly estimated, as their incremental costs could vary significantly based on each organization's circumstances. Nevertheless, these and other SOC cost contributors, if included, would only further add to the economic advantage of AWN CyberSOC.

COST COMPONENT	THREE-YEAR COST RANGE*	DESCRIPTION AND COMMENTARY
SIEM	$70,000–$440,000	Options are plentiful for organizations to build the technology backbone of their SOCs. Options include on-premises SIEM hardware appliances, virtual SIEM appliances, and SIEM-as-a-Service offerings. Our range estimate is structurally conservative as we anticipate organizations building their first SOC would price-shop options and vendors for a 'starter' SIEM, and eventually refocus on a replacement SIEM with more premium-grade features, as their SOC matures. Our upper range assumes a SIEM hardware appliance purchase price in excess of $200,000, annual maintenance fees of 15% of purchase price, and a conservative allowance of $22,000 for professional services (installation, configuration, and training). The low-end estimate is for SIEM-as-a-Service. Also adding to the conservatism of this range is the SIEM price structure. For some SIEMs, the number of logs processed has a material bearing on total costs. For organizations that underestimate their log volume, cost shock can be significant. As we cite later, SIEM is a challenging technology to master, and frequently requires challenging customization. For SOC staff, this adds to the demands on their time.
External Threat Intelligence	$25,000–$55,000	External threat intelligence is critical to clarify likelihood of attack, evolving and emerging attack types and methods, profiles of recent victims, and severity.
Vulnerability Scanning	$5,000–$30,000	Like SIEM, various options are available, and we applied the same conservative logic of price shopping for initial vulnerability scanning in building a SOC. Also like SIEM, usage fees based on number of endpoints can contribute to cost unpredictability, depending on the scanning product or service selected.

* Based on customer size (small to large)

Source: Frost & Sullivan

For the cost of AWN CyberSOC, we used three customer sizes based on the number of end-users, servers, and AWN sensors, as shown in the table below.

EXHIBIT 2: **AWN CyberSOC Costs**

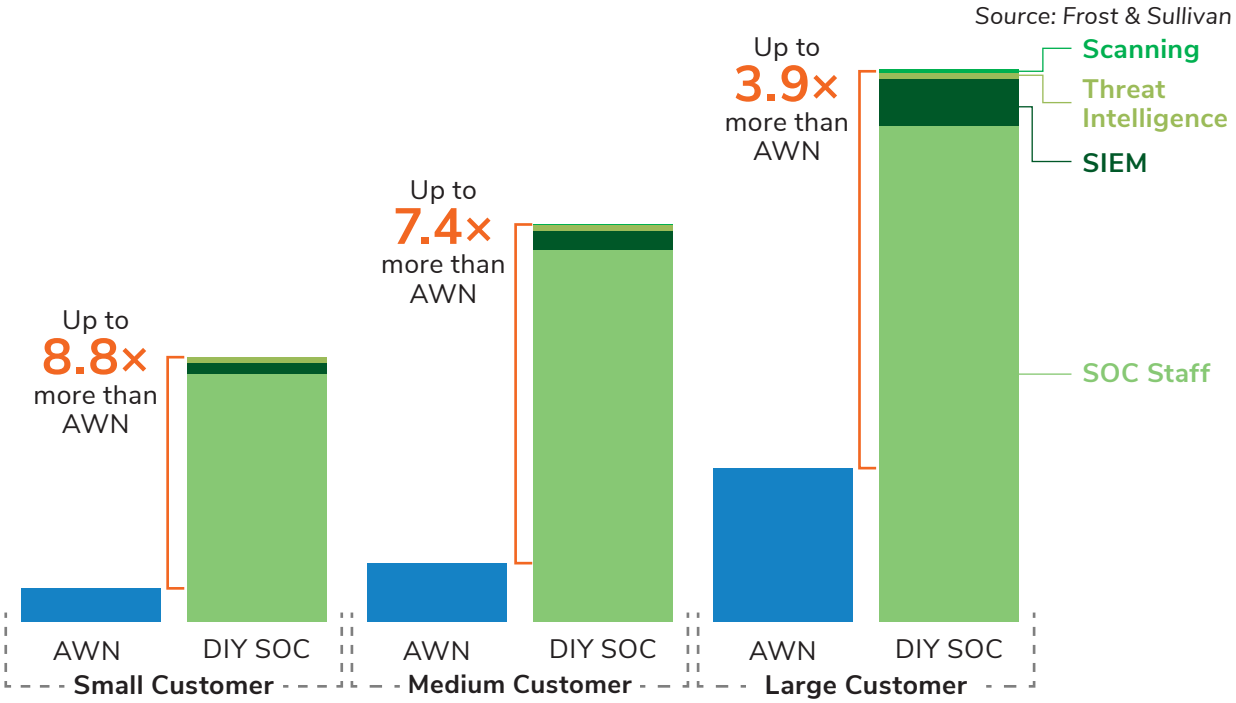
CUSTOMER SIZE	Small	Medium	Large
NUMBER OF END-USERS	500 end-users	1,000 end-users	3,000 end-users
THREE-YEAR CYBERSOC COST RANGE*	$279,000–$346,000	$502,000–$591,000	$1,304,000–$1,563,000

* Based on customer size (variation due to number of servers and sensors)

Sources: Frost & Sullivan and AWN

A side-by-side comparison of the three-year costs of DIY SOC versus the cost of AWN CyberSOC for three customer sizes is shown in the following chart.

EXHIBIT 3: **Three-year Cost Comparison: AWN CyberSOC versus DIY SOC**



Principal observations from this comparison are:

- The three-year cost of building a DIY SOC is up to 8.8 times that of subscribing to SOCaaS, such as AWN CyberSOC—This 8.8x multiple is calculated based on an estimated cost of DIY SOC for a small customer (six SOC staff members, SIEM, threat intelligence, and vulnerability scanning) versus the lower end of the AWN CyberSOC cost range for a similar customer size (500

end-users). Similar cost comparisons for a medium customer (nine SOC staff members and the other cost contributors versus 1,000 end-users for AWN) and a large customer (12 SOC staff members and the other cost contributors versus 3,000 end-users for AWN) were also calculated.

- Staffing costs dominate the cost of operating a DIY SOC—Repeating an earlier point: SOC staffing costs quickly led each of the AWN CyberSOC interviewed customers away from the DIY SOC option. As staffing costs are annually recurring, the sizeable cost efficiency of AWN CyberSOC continues beyond the three-year time horizon.
- DIY SOC costs vary widely—Demonstrated in the cost estimates for DIY SOC, their cost components have significantly higher variability than the more predictable pricing structure of the AWN CyberSOC service (i.e., based on number of end-users, servers, and AWN sensors).

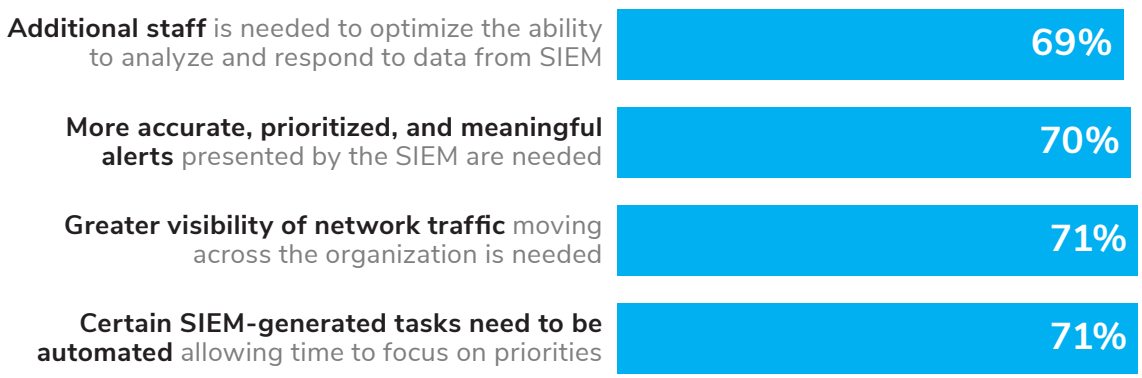
SIEM's Expensive Complexity

An additional facet to note in this DIY SOC versus SOCaaS comparison is that technology supporting threat detection and response can be expensively complex. With a DIY SOC, managing and optimizing technology falls upon SOC staff members. Conversely, in SOCaaS, those responsibilities are completed by the SOCaaS provider.

SIEM, as previously highlighted, is a foundational SOC technology. SIEM is also complex and has a tendency to contribute to the following consequences:

- Configuring and implementing a SIEM requires significant effort—According to Ponemon Institute in its Challenges to Achieving SIEM Optimization (March 2017), 40% of survey respondents stated that the configuration and implementation effort with a SIEM was 'very significant'; and another 35% stated 'significant'. For organizations building a SOC, this SIEM effort must be incorporated into their implementation costs and timelines.
- Current SIEMs fail to deliver on users' expectations on several fronts—The next chart highlights missed expectations. These missed expectations force organizations to compensate with alternatives—principally, more creative staff effort, to meet the objectives SIEMs could not.

EXHIBIT 4: **Challenges with Current SIEM Technologies (Strongly Agree and Agree survey responses combined)**



Source: Ponemon Institute, Challenges to Achieving SIEM Optimization (March 2017)

- **Technology obsolescence creeps up over time**—Obsolescence adds an extra set of tasks to the SOC owner. Replacement technologies require evaluation, proof of concepts, vendor negotiations, and then a transition to new technology to facilitate. In totality, another set of necessary tasks that can also be fraught with complexity and risk.

FEATURE COMPARISON OF SOCaaS AND DIY SOC

In this final section of analysis we compare SOCaaS and DIY SOC attributes. As SOCaaS offerings differ, we used AWN CyberSOC with its included Concierge Security team. Our overall take-away is that SOCaaS alleviates the significant burdens of building and operating a SOC, while providing highly customized threat detection and response services with a high level of cost efficiency.

ATTRIBUTE	AWN CYBERSOC (SOCAAS)	DIY SOC
Cost	Predictable and economical	Unpredictable and cost prohibitive for small to midsize with no/limited security staff
Staffing	Fully managed by AWN	Entire responsibility of recruitment, training, and retention rests with the organization
Deployment	Turnkey	Months to potentially years for full deployment
Customization	High within the AWN CyberSOC platform's feature set, with customer-customization orchestrated by tenured experts	High within the feature set of SOC technologies purchased, but dependent on SOC staff's time and expertise to customize
Resiliency	Cloud-based design to ensure enterprise-grade service reliability	All factors that could contribute to downtime must be identified and accommodated by the organization
Technology evolution	Fully managed by AWN with new features and upgrades offered to all customers following testing and implementation	Timing and frequency dependent on organization's planning, budgeting, and implementation efficacy

Source: Frost & Sullivan

THE LAST WORD

Hope that cyber defenses will hold threat actors at bay, and data breaches will only affect another business, is just that—hope. The frequency, severity, and business implications of damaging cyber attacks and data breaches are only heading in an upward direction. Consequently, it is truly just

a matter of time before you become a victim. And once attackers succeed, more often than not, they will return again and again until they are detected and steps are put in place to thwart their nefarious activities.

AWN CyberSOC offers a very compelling approach for around-the-clock threat detection and response. AWN CyberSOC is proven in its effectiveness, customer-tailored fit, accuracy, and scalability—all the attributes you would demand if you built and managed your own SOC. As we also demonstrated, there is a significant price tag for a DIY SOC; and the cost, primarily driven by staffing, is a very visual reminder of money that would be spent year in and year out. **Comparing three-year costs, the cost of a DIY SOC can range from 3.9 to 8.8 times more than the AWN CyberSOC service, depending on the size of the business.**

Our advice is that you should examine your threat detection and response options NOW. Waiting until after an expensive and damaging cyber incident has occurred will only increase your financial burden. We also recommend that you examine AWN CyberSOC—it does the heavy lifting for you without you breaking your budget.

Michael Suby
VP of Research
Stratecast | Frost & Sullivan

msuby@stratecast.com

ABOUT STRATECAST

Stratecast collaborates with our clients to reach smart business decisions in the rapidly evolving and hyper-competitive Information and Communications Technology markets. Leveraging a mix of action-oriented subscription research and customized consulting engagements, Stratecast delivers knowledge and perspective that is only attainable through years of real-world experience in an industry where customers are collaborators; today's partners are tomorrow's competitors; and agility and innovation are essential elements for success. Contact your Stratecast Account Executive to engage our experience to assist you in attaining your growth objectives.

FROST & SULLIVAN

SILICON VALLEY
3211 Scott Blvd
Santa Clara, CA 95054
Tel +1 650.475.4500
Fax +1 650.475.1571

SAN ANTONIO
7550 West Interstate 10, Suite 400,
San Antonio, Texas 78229-5616
Tel +1 210.348.1000
Fax +1 210.348.1003

LONDON
566 Chiswick High Road,
London W4 5YF
Tel +44 (0)20 8996 8500
Fax +44 (0)20 8994 1389

877.GoFrost • myfrost@frost.com
http://www.frost.com

NEXT STEPS

- Interested in learning more about the topics covered in this report? Call 877-463-7678 or email us at inquiries@stratecast.com
- Visit our Stratecast web page.
- Attend one of our **Growth Innovation & Leadership (GIL)** events to unearth hidden growth opportunities.

Frost & Sullivan, the Growth Partnership Company, works in collaboration with clients to leverage visionary innovation that addresses the global challenges and related growth opportunities that will make or break today's market participants. For more than 50 years, we have been developing growth strategies for the Global 1000, emerging businesses, the public sector and the investment community. Is your organization prepared for the next profound wave of industry convergence, disruptive technologies, increasing competitive intensity, Mega Trends, breakthrough best practices, changing customer dynamics and emerging economies?