deepwatch

WHITEPAPER

Defining a "Modern SOC"

Build, Buy or Ally to Secure Your Business

Table of Contents

Achieving a Modern SOC with Managed Detection and Response

FOREWORD

Defining a "Modern SOC"

Dear Reader:

Part of being a leader is making difficult decisions. You try your best to make the best decision with the information that you have at that point in time. Often the decision works out very well, while sometimes it backfires.

When it comes to cybersecurity related decisions, the implications of a bad decision can have major, long-lasting consequences for your company in terms of its brand and reputation. Chief Information Security Officers (CISOs) manage incredible risks.

One of the key capabilities that CISOs must develop is that of a Security Operations Center (SOC). The decision to build or buy a SOC capability is not an easy one. There are a variety of business drivers and selection criteria that CISOs must evaluate. Determining whether to build and staff your own SOC, or partner with a Managed Detection and Response (MDR) provider is an important decision.

This white paper discusses key considerations in this decision. If you have any questions or would like me or a member of my team to walk you through the decision process, please reach out to us anytime.

All the best,

deepwatch

Defining a "Modern SOC" Build, Buy or Ally to Secure Your Business

What is a SOC

According to Sid Deshpande, a former Gartner Analyst: “A SOC can be defined both as a team, often operating in shifts around the clock, and a facility dedicated and organized to prevent, detect, assess and respond to cybersecurity threats and incidents.” In a nutshell, a SOC monitors an organization’s systems for Indicators of Compromise (IOCs). SOC analysts monitor and validate potential malicious traffic to stop it before it causes harm, or if a breach has occurred, limit exposure and mitigate the threat.

Deepwatch is the new standard for protection and risk mitigation against cyber threats. We are redefining the modern SOC via the most advanced commercially available platform for detecting threats and vulnerabilities.

What a SOC in Not

A SOC is not a complete security program in and of itself. A SOC is not typically responsible for development of security policies and programs, as these are the responsibility of the security leadership team. A SOC generally is not responsible for the architecture and implementation of security technology controls. Those are typically a joint effort between the security architecture and engineering team with the help of information technology resources. A SOC is not responsible for the assessment and maintenance of the organization’s compliance with regulatory and industry requirements. Since the SOC generally operates many of the controls necessary to meet these requirements, an independent part of the organization is generally appropriate for the assessment of the state of compliance provided through these requirements.

Further, a SOC is not focused on the same issues that a Network and IT Operations Center are: routing issues, capacity issues, uptime issues, and the like are not generally considered part of security operations.

What is a Modern SOC

A Modern SOC analyzes significant volumes of data, contextualizes and correlates this data and delivers critical insights into security logs and alerts in "real time." This cannot be done by manually perusing a SIEM or log aggregation solution. A Modern SOC requires significant automation, a view of the company's security that goes beyond internal logs, but incorporates knowledge of the world outside the organization's borders, and visibility into the logs generated by sources that legacy SOCs would have never ingested in the first place. Modern SOCs focus on team coordination and automation in order to handle the increased event load to reviewed. It is our opinion that the largest jump between legacy SOCs and modern SOCs are the inclusion of:

Modern

- Correlation of Events from multiple
- logging areas
- Threat Intelligence
- Automation
- 24x7x365 Activity
- Monitor, Manage and Advise

Legacy

- Events from Perimeter and Endpoint
- Detection Technologies
- Manual Investigation or Analysis
- 8x5x5 Operations
- Endpoint, Network, and Patch/Vuln separated responsibilities

CORRELATION OF EVENTS FROM MULTIPLE LOGGING AREAS

Security operations are built out of the collection and analysis of logs from different sources or areas. Historically these "areas" have been the perimeter and endpoint spaces. Whether it was logs from the Firewalls, and IDS/IPS or from endpoint Antivirus, these are the logs sources and areas that Security Operations Centers grew up on.

As new "areas" (External Environments) have arrived, like Public Cloud, Software as a Service, Remote Devices, and a plethora of other sources. Security Operations has had to onboard and attempt to understand or correlate logs from all these sources together to understand the state of an organization's security and react to incidents, a significant increase in log volume and alerts to search through.

CYBER THREAT INTELLIGENCE

To have a proper security perspective, Security Analysts need to be able to look externally and internally, leading to the use of Threat Intelligence within different areas of the security architecture, often in the form of blacklists which generate log events. In this way Threat Intelligence has both improved security operations and created a significant additional volume of logs from security technologies, adding to the content that must be reviewed by a SOC.

What is a Modern SOC

AUTOMATION

The increase in the number of detection and protection technologies in place along with the addition of the outside perspective of Threat Intelligence has caused a dramatic increase in the amount of logs that need to be analyzed and validated by security operations teams. Coupled with the ongoing lack of security talent in the industry, we have seen a tremendous increase in the amount of automation applied to event analysis and security operations in general. Automation can be as simple as task creation and resolution, to as complex as multi step phishing analysis, verification and system remediation.

Automation is one of those areas that gets more complex the deeper you go, but also offers greater potential value and return on time.

24/7/365 ACTIVITY

This one is simple. Attackers don't work 9 to 5. They don't take off weekends, and they may not celebrate the same holidays that you or your company does. Monitoring needs to not only be consistent in eyes on glass, but the eyes on glass need to be of equal caliber across the hours of the day.

MONITOR, MANAGE, AND ADVISE?

Security operations have matured and specialized over the years. Security operations traditionally are based around a tiered model of Tier 1, Tier 2 and Tier 3. These tiers are based not only on specialization of differing tools or detection/protection types but also from experience and oversight capabilities. Tier 1 and Tier 2 are generally focused on the traditional security environment of Firewalls (Perimeter), Endpoints (User Land), and Infrastructure (DMZ or Server Land). Tier 3 is usually the team lead and is focused on the forensics and incident resolution capabilities. Think of it like this: Tier1 sees it, Tier 2 validates it, Tier 3 attempts to fix it.

The average SOC has 30 to 40 security tools currently deployed. They are almost constantly in the midst of at least one technology change or major upgrade. The sheer number of events along with the project management of a roll out can overwhelm even well performing SOCs. Meaning they don't have the time to get in front of event analysis, or time to make anything other than reaction-based changes to the tool they monitor and manage.

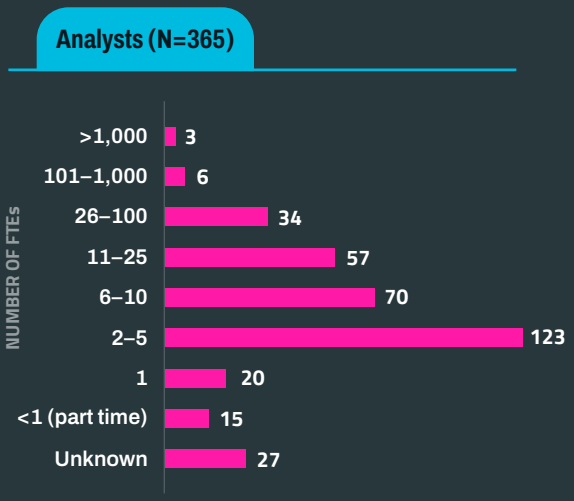
A modern SOC takes advantage of differing correlation and automation techniques and technology to get more time on the clock. This time allows for a modern SOC to more accurately schedule the eyes on glass they need, with the appropriate Tiers of users to keep the analysis assembly line moving. The modern SOC isn't only focused on handling the event load in an accurate manner, but also in partnering with other operating groups to make suggestions on managing security tangential technologies, or advising in appropriate next steps for resolution, remediation or mitigation.

SOCs by the Numbers

A recent SANS study can be used to put some numbers together on the difference between traditional and modern Security Operations Groups. A minimal 24x7x365 Modern Security Operations Group employs Analysts, SIEM/Network/ Forensics Engineers, Threat Hunters, Project Managers and Leadership. Minimal staffing for this availability and capabilities require a headcount of 20 individuals. These estimates include the need for addressing coverage in each role as employees take time away from work. SANS numbers suggest that Modern Security Operations are not the standard across the Industry.

Research suggests that most companies do not attain this level of staffing, nor are they able to provide true 24x7x365 coverage internally. According to the SANS Institute 2019 SOC Survey, the typical SOC today usually employs two to five analysts, with more respondents in the SANS study reporting their staffing levels in this range (please see graphic on the right), scaled by organizational size

Full-Time Analysts Who Use SOC Systems and Services



Source: SANS Institute 2019 SOC Survey

Security Operations Center staffing issues can be **exacerbated by the location and the amount of local talent available.**

Organizations with between 10,000 to 15,000 employees generally run a SOC with 6 to 10 employees; organizations from 15,001 employees up to 100,000 employees put together SOC teams of approximately 11-25 analysts; and very large enterprises with over 100,000 employees stand up SOCs with 26 to 100 analysts.

Two other factors to take into account when working on the numbers for Security Operations Groups is the Compliance and audit requirements the company is operating under and the current cybersecurity talent and skills gap.

There have been volumes written around the gap and the current focus on getting more people into the field, but the thing that has been missing from the discussion is the location of these people. Security Operations Center staffing issues can be exacerbated by the location and the amount of local talent available.

Compliance requirements add more complexity to hiring and staffing numbers in regulated industries. Security mandates can vary based on the industry sector. Retail businesses need to meet PCI DSS, for example. Healthcare providers must comply with the Health Insurance Portability and Accountability Act (HIPAA) privacy and security requirements; publicly traded companies must comply with Sarbanes-Oxley (SOX) constraints. Staffing a knowledgeable team to meet and keep up with the requirements of these mandates can be challenging.

Build, Buy, or Ally?

In order to acquire Modern Security Operations capabilities, customers can choose to either build from scratch or upgrade/update existing Security Operation Groups. Another option is to Buy Modern Security Operations from an MSS (Managed Security Services) Partner. Or to ally with an MDR provider for more specific capabilities and higher return on the security investment.

If the goal is to operate or build a Modern Security Operations Group let's start with some requirements around the technology needed to operate.

Technology Integrations:

- Security Incident and Event Management (SIEM) solution
- Firewalls, Proxy, Web Application Firewalls, Mail Gateways, and any other traditional perimeter based security controls that all need to be logged for visibility and correlation into the SIEM
- Endpoint, HID/HIPS, Anti-Virus, EDR, DLP, Whitelisting, Access Controls
- Cloud access control, Email, Multi-Factor Authentication
- Threat Intelligence Platform, Dark Web Monitoring, Ticketing System Migrations, Security Operations Analytics & Response tools

Education:

- Educate teams to implement and manage these additional technologies

Use Cases:

- Development of additional use cases over time

Additional Resources:

- Recruiting costs & time; Engineering team of SMEs (SIEM, TIP, Dark Web Monitoring, SOAR), Threat Hunters; SOC Analysts with equivalent knowledge and experience

Threat Reports:

- Sharing of information through threat reports from across multiple technology areas

WITH THOSE REQUIREMENTS IN MIND, WHAT MIGHT IT COST TO PROCURE THE TECHNOLOGY, PEOPLE, TRAINING?

FTE Function	Annual (avg)
Analyst Internal cybersecurity analyst resource capable of investigating and validating notable events	**$100,000**
Engineer Internal cybersecurity engineering resource capable of configuring log sources and setting up and maintaining an advanced SIEM	**$150,000**
Team Implementing a SIEM and staffing a 24x7 SOC with cybersecurity talent resources for single-depth, non-redundant resources.	**> $1,000,000**

Build, Buy, or Ally?

If you note the table on the previous page is looking strictly at the people cost of Modern 24x7x365 Security Operations. Security Tooling, support, updates, and Intelligence sources and training costs have not calculated into the greater than 1 million per year number.

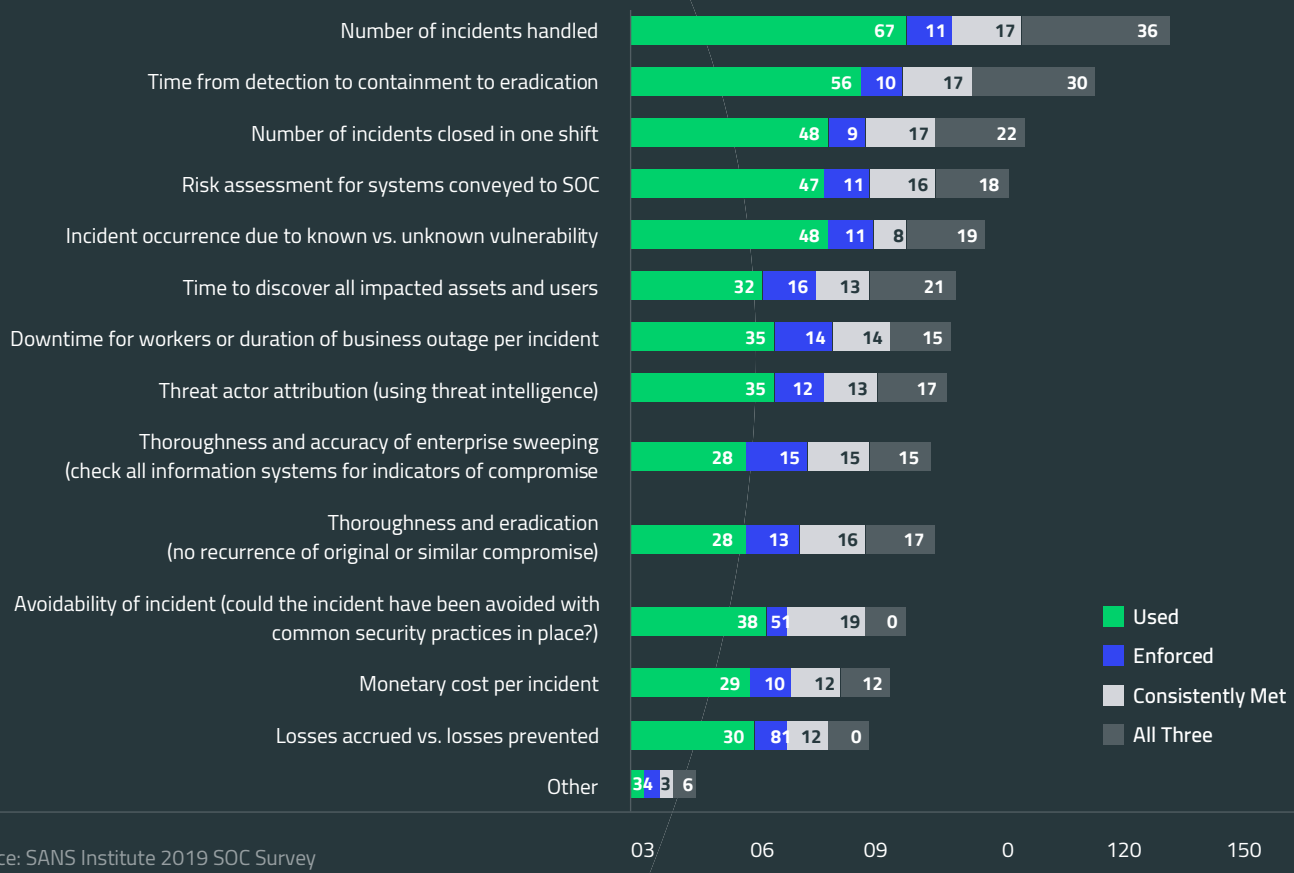
So now a Security Operations Group has been built out. Your company has acquired, implemented the necessary technologies and trained the hired analyst in their capabilities while acquiring or writing out the company's playbooks or runbooks to make sure that the analysis process and false positive vs true positive identification. The next step in building out a Security Operations Group is to determine how to make things better, or how to further refine your Modern Security Operations. Traditionally this is done through the number of incidents handled. However, the real focus should go beyond mere counting of incidents. **To trulymeasure the impact on the core business, key metrics should evaluate the monetary cost per incident and losses accrued versus losses prevented.**

...key metrics should **evaluate the monetary cost per incident and losses accrued versus losses prevented.**

SANS analysts say that if SOC managers are going to get more budget to make the investments they need to move the needle on SOC maturity, they've got to get better at the metrics game (please see graphic below). "To gain management support for resources, SOC managers need to move beyond quantity-based metrics — how many raindrops hit the roof — to business-relevant metrics — zero production downtime due to rain getting through the roof," SANS concludes.

Currently, the number one used metric to track and report SOC performance is the number of incidents handled. Only a very slim number of SOCs track monetary cost per incident or losses accrued versus losses prevented.

WHICH OF THE FOLLOWING METRICS DO YOU USE TO TRACK AND REPORT YOUR SOC'S SERVICE OR PERFORMANCE? (N=145)



Source: SANS Institute 2019 SOC Survey

Build, Buy, or Ally?

According to the Exabeam 2019 State of the SOC Report, time wasted spinning wheels caused some of the biggest pain points for those surveyed.

Approximately one in three said the time spent on reporting and documentation was their biggest complaint. Meanwhile, 27% said alert fatigue was their biggest source of pain, while 24% cited false positives. Other common complaints included out-of-date systems or applications, false negatives and lack of visibility.

The Exabeam report also noted that SOCs today are increasingly outsourcing functions in five of the eight major categories (please see graphic below). Some 43% of organizations report that they outsource certain functions of their work.

The three most popular functions for outsourcing—both in prevalence and growth over the prior year—were malware analysis expertise, threat analysis and threat intel services.

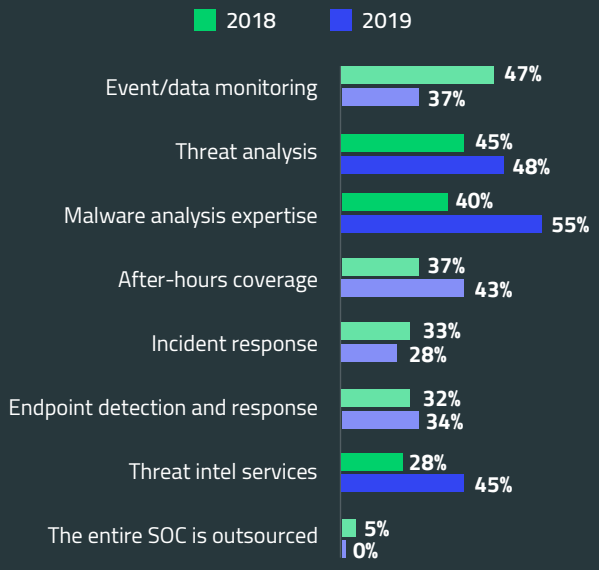
This is in line with SANS outsourcing findings, which broke up categories differently but found that monitoring and detection capabilities were outsourced to some degree by 76% of respondents.

Exabeam's report, which was conducted among organizations in the US and the UK, found that technology makes up the biggest line item for SOC resource allocation and is also the most frequently cited item for insufficient funding. When asked about where they'd like to see more investments, 39% said they'd want to make additional investments in new/modern technology, 35% said they'd like to secure additional funding for staffing needs, and 34% would invest in automation to save time.

Top Pain Points for SOC Personnel

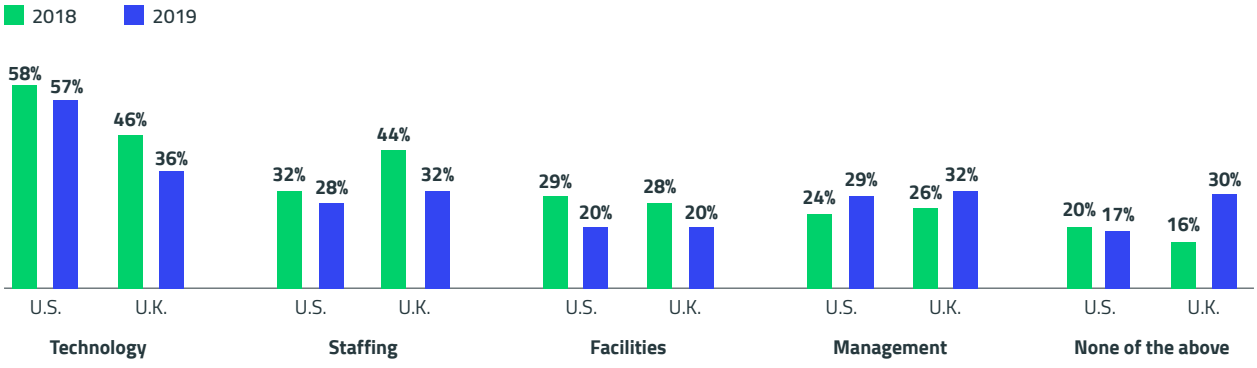
Source: Exabeam 2019 State of the SOC Report

Outsourced Functions



Source: Exabeam 2019 State of the SOC Report

FUNDING DISTRIBUTIONS – 2018|2019



Source: Exabeam 2019 State of the SOC Report

Build, Buy, or Ally?

Buy

A major reason that companies look to Buy into MSS partners is to see the benefit of tooling, training, and common experience with the rest of the partner's customer base or that partner's specific capabilities.

MSSPs purchase, deploy and manage leading technologies for their customers. In other words,MSSP customers utilize leading technologies for a fraction of the cost. Therefore, an MSSP has access tobest-of-breed technologies and thus is able to continuously enhance its technology platform. The costs for these tools are spread across clients, at a negligible cost to each. The benefits include:

Technology Integrations:

- Security Incident and Event Management (SIEM) solution
- Firewalls, Proxy, Web Application Firewalls, Mail Gateways, and any other traditional perimeter based security controls that all need to be logged for visibility and correlation into the SIEM
- Endpoint, HID/HIPS, Anti-Virus, EDR, DLP, Whitelisting, Access Controls
- Cloud access control, Email, Multi-Factor Authentication
- Threat Intelligence Platform, Dark Web Monitoring, Ticketing System Migrations, Security Operations Analytics & Response tools

Education:

- Educate teams to implement and manage these additional technologies

Use Cases:

- Development of additional use cases over time

Additional Resources:

- Recruiting costs & time; Engineering team of SMEs (SIEM, TIP, Dark Web Monitoring, SOAR), Threat Hunters; SOC Analysts with equivalent knowledge and experience

Threat Reports:

- Sharing of information through threat reports from across multiple technology areas

ABC COMPANY 2020 INVESTMENT INSOURCE VS OUTSOURCE

	Insource*	Outsource**
FTEs	$1,000,000 +	–
Training	$50,000	–
Technology (SIEM, SOAR, TIP, ITSM, etc.)	$250,000	–
MSSP relationship		$100,000 - $500,000
Cost Comparison	$1,300,000+	$100,000 - $500,000

* Based on industry average

**Based on actual vendor quote

Companies that buy into MSS offerings often buy to have access to the advanced capabilities highlighted in the Exabeamreport. Threat Analysis, Malware and Forensics, and Threat Intelligence are Modern Security Operations standards, but are some of the most expensive and complex capabilities to do well.

These actions are challenging because they require coordination across the different tiers of analysis and a personalized understanding of the context around an event to be analyzed. Generally, a purchased MSS offering of traditional or ModernSecurity Operations does not have the time, resources or capabilities to offer personalized and effective advanced services for their customers due to scale, cost and time constraints.

Build, Buy, or Ally?

Ally

Allying with an MDR provider is different than buying a MSS or going with an MSSP. The difference is found in the amount of connection between the partner and your team and awareness brought to your company's unique needs, events, and expectations.

Allying with an MDR provider can optimize performance and leverage key resources over and above buying partner services. The central security goals for a business to strive for are:

- Improved communications
- Enhanced focus on business-relevant metrics
- Improved efficiencies through automation
- Increased service levels while containing costs

Partnering with an MDR provider can help achieve these goals by providing:

Cost savings:

An MDR provider can provide 24x7x365 coverage at a fraction of the cost of hiring internal cybersecurity staff, and eliminating the need for large, frequent capital expenditures and licensing costs. Responsiveness and performance metrics defined in a service level agreement ensures your needs are met and you are getting what you are paying for.

A stronger focus on the core business:

Building the internal capabilities to address challenges like dark web monitoring and advanced threat detection can sap resources from core business operations in terms of attention and budget.

Enhanced protection:

Internal teams can get overwhelmed by the noise of actions and incidents, reaching a point of ignoring alerts because they feel they are false positives or don't provide actionable intelligence. An MSS can incorporate machine learning and artificial intelligence to address "noise" issues and synthesize appropriate responses. An Allied MSS uses not only Machine Learning and Automation to reduce noise but also utilizes a deep familiarization with the customer's environment and needs to truly tailor the when and who to communicate with on your team, but to also provide potential next steps or remediation actions based on communal understanding of the environment.

Access to a deep bench of experts:

With capabilities to align with industry-specific standard compliance, an MDR partner can provide specific responses to address a client's specific risks, challenges and threats, while helping maximize internal staff resources through ongoing communication. A true MDR partner will look to provide consistency in contacts between analysts and customers, fostering familiarization and collaborative processes that build trust and expedite responses.
Access to a repository of security use cases:
Use cases inform detection and rapid responses with a library of threat detection signatures, risky authentication behavior searches, automated response workflows, anomalous network activity, and other situations that may be unfamiliar to an internal security team.

Access to advanced technology:

MDR providers have the resources and capability to build tailored, scalable solutions to match clients' needs, while integrating, as needed, technologies that clients currently use. The solutions are service-oriented, thus geared to a specific solution rather than selling a particular technology, and with the ability to communicate across platforms. Allied MDR providers have the ability to not just bring additional resources to bear, but to also tailor these advanced capabilities for the greatest results and effectiveness for their customers.

Benchmarking security operations through a maturity model:

Providing an objective scoring index helps assess the customer's security operational capabilities, and yields metrics that are useful to board and auditors in measuring and upgrading security systems and resources.

Efficiencies:

Higher levels of productivity and performance are achieved through a collaborative managed detection and response solution, with responsibility for crucial tasks that include threat monitoring and proactive threat hunting, while paring back notable events from thousands down to an average of 4-5 events per day through a rigorous validation process, saving clients many hours, and enabling clients to redirect staff previously performing monitoring and validation activities to undertake other essential tasks within an organization.

In Closing

Successful allied security solutions provide a tailored, layered integration of the right people, processes and technologies to move companies from a defensive posture to a proactive position, while implementing constant improvements and efficiencies. **The allied MDR option can provide economies of scale that extend and enhance internal capabilities, freeing companies to focus attention and resources on their core business.**

WHAT'S NEXT?

If you would like to learn more about how Deepwatch ally's with its customers to secure their networks, please visit **www.deepwatch.com** or reach out to us at **sales@deepwatch.com**

deepwatch

ABOUT DEEPWATCH

Deepwatch delivers data-driven managed security services while extending customers' cybersecurity teams and proactively advancing their SecOps maturity. Powered by our innovative cloud-native platform, Deepwatch is trusted by leading global organizations to provide 24/7/365 managed security services.

CONTACT US

7800 E Union Ave, Suite 900
Denver, CO 80237
855.303.3033