deepwatch

WHITEPAPER

Maximizing SOC Effectiveness with MDR

www.deepwatch.com

Table of Contents

Executive Summary

Organizations can experience an immediate positive impact from an efficient and effective security operations program.

This whitepaper creates a framework for understanding and achieving overall effectiveness by presenting key beneficial approaches to building and running a security operations center (SOC).

Key Whitepaper Highlights

1. The concept of effective security operations means different things to different individuals and groups within your organization. Take time to understand how your board of directors interprets effective security compared with other groups like IT or HR.

2. Corporate and customer goals and risks define how your business operates. These goals and risks should also define your approach to security operations. Understand what's important to your business and customers to help drive SOC strategies and tactics.

3. Not all security operations metrics are equal. Understand which metrics are most relevant to your organization. Identify metrics that are realistic and align directly to corporate and customer goals. Don't limit metrics to quantitative tactical ones. Include qualitative and strategic metrics as well.

4. Collaborate with other divisions and departments, such as IT, marketing, HR, and your board of directors to promote security operations goals and objectives, and understand the security operations needs and requirements of external stakeholders, such as customers, regulators, and third-party vendors/suppliers.

5. Evaluate the overall costs of a do-it-yourself SOC vs. outsourcing. In many cases, outsourcing expertise can be more cost effective.

Introduction

A well-managed security operations center (SOC) can benefit organizations in a multitude of ways—from improved threat detection and protection to better understanding of the strategic and tactical implications of budgets, staffing, and security solutions. But, with the myriad of other daily challenges security operations programs face, such as staffing shortages, increased global threats, and compliance and risk oversight, **it can be difficult to determine which processes can and should be implemented to maximize program success.**

In this whitepaper, we'll explore the best practices associated with maximizing SOC effectiveness, focusing on what "effectiveness" means and what methods and techniques are useful, including:

- **Cybersecurity standards and benchmarks**
- **Choosing and using metrics**
- **Managing and balancing vulnerabilities**
- **Creating budgets and managing expectations around "return on investment"**
- **Maximizing success through collaboration**
- **Evaluating the costs and benefits of in-house efforts vs. outsourcing**

What does it mean to have an “effective” SOC?

The key to understanding “effectiveness” is recognizing that the term can mean a lot of different things to different audiences. For your security staff, it may simply mean they’re meeting certain internal quantitative metrics and goals, such as the number of blocked threats and minimizing system downtime. For your organizational staff, it may mean they’re not seeing any spam in their email folders. And, for your senior executives and board members, “effectiveness” may relate to security operations’ overall impact on strategic business goals and objectives. This means you can’t always fall back on using the same measures of “effectiveness” across all organizations and with all groups.

Ultimately, an “effective” security operations program isn’t just about one tool, technique, or measurement—it is about understanding which methods and metrics will best serve your organizational needs at both the micro and macro level—and then implementing the right blend of metrics and best practices to meet the goals of the entire organization.

When determining the metrics and best practices to use to maximize effectiveness, there are three critical beginning steps. First, know your business and clients, including basics such as company size, its age, and its primary industry, as well as overall corporate and client goals, objectives, and risks. Second, understand that strictly quantitative measurements and numbers can’t be the only answer to determining overall effectiveness. And, third, recognize that your approach to effective and successful security operations will need to change as technology and the industry evolve.

STEP 1

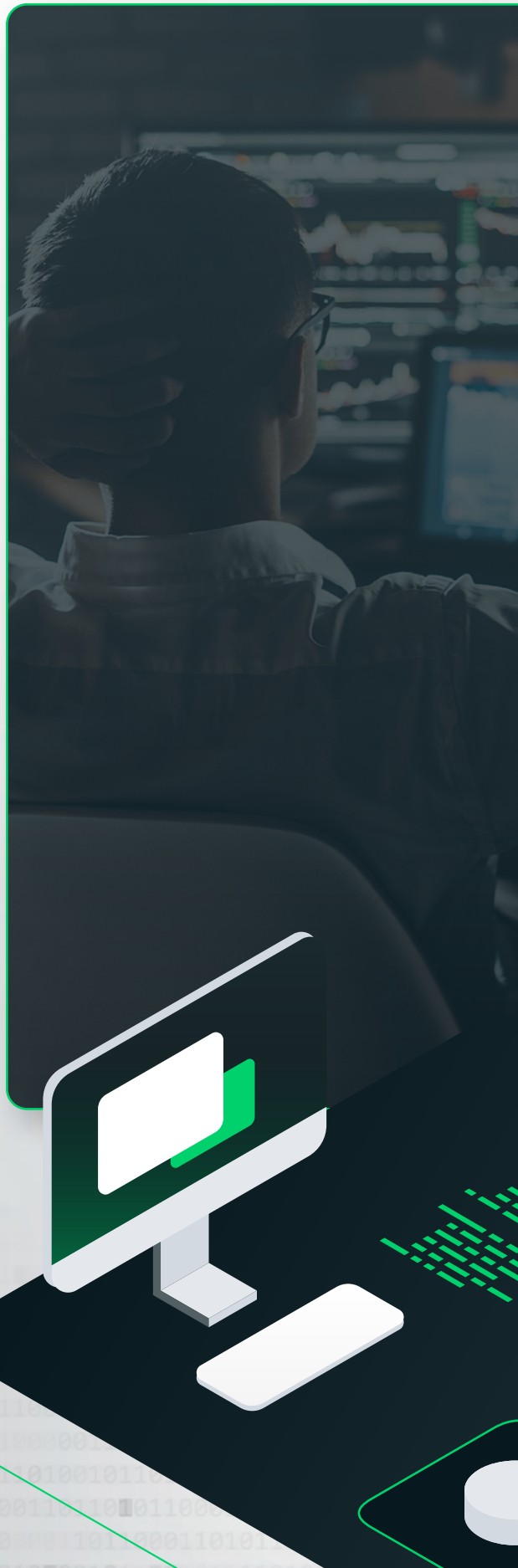
Know your business. Know your clients.

STEP 2

Move beyond the numbers.

STEP 3

Evolve and innovate.



Know your business. Know your clients.

Effectiveness begins by knowing your business and clients. Each organizations' goals and risks are different—and the goals and risks of their customer base are different too. Security operations needs to understand business and client objectives, key success factors, and risks as a first step before finalizing any metrics or best practices.

Understand business goals

Business goals vary from organization to organization—for example, the goals of operating a health care services firm are very different from a business consulting organization. Things like customer service levels, stock goals, sales goals, brand reputation, and website uptime are all examples of the types of priorities that factor into the overall goals of a business.

Understand your business risk

Risks are different—and each risk comes with different mitigations and tolerance levels. For example, risk and tolerance levels for a company holding data composed of simply customer names and email addresses may be entirely different from a company that holds sensitive personally identifiable information (PII), passwords, or credit card numbers. Equally, successful risk mitigation requires that security operations be intimately involved in developing the risk mitigation plan.

Understand customer goals and risks

A key customer's business priorities, goals, and risk levels can also impact how a security operations team measures the overall effectiveness of its program. Knowing what to measure and what best practices to implement needs to be informed by an understanding of what is important to your customers.

Move beyond the numbers.

The very nature of security operations activities means it is easy to fall back on traditional data, such as mean time to detect or the number of assets on a system. But, as you begin the process to maximize security operations effectiveness, remember that sole reliance on metrics and numbers won't always help you achieve your goals.

Recognize that it's hard to tell the whole story with just numbers

When relying on traditional SOC metrics, remember that a single number or a small group of numbers isn't going to always give you the complete picture. Metrics that lack clear definitions can make the overall impact of the number meaningless. For example, when tracking incidents, what definition are you using for an "incident"? If an employee clicks on a link and downloads malware, but the existing security prevents the malware from installing, does this count?

Make sure metrics are realistic

It is important to avoid setting impractical quantitative goals when determining whether your SOC is effective or not. For example, it is becoming increasingly difficult to stay on top of every app that your employees may download or the number of devices your employees may be using on a daily basis. Therefore, is it realistic to set a goal of 100% vulnerability management when it is virtually impossible to identify with certainty every single asset or app on the IT systems? Even if you can identify them, few security professionals can claim they have 100% control over every asset or app in the environment. When developing meaningful measurements, security professionals need to focus on what is realistic and how your team can encourage overall "improvements" to security.

Pick the most useful and valuable metrics

In terms of sheer numbers, the absolute volume of cybersecurity information available at a given organization can make data analysis complex, costly, and potentially challenging to model. Few security operations organizations have the staff, budgets, time, or expertise to do a thorough in-depth analysis of all the data available to them. Therefore, it is important to pick the metrics that are going to give you the best overall picture as aligned to not only your SOC's needs, but also your overall corporate goals.

It's not just about the quantitative

Your security staff can be all set up to track total monthly phishing incidents, but if your organization isn't offering security training or your organizations' employees don't understand or don't know how to implement the training they've received, then how meaningful is the "total number of phishing incidents" going to be? Qualitative metrics—such as how well employees comprehend and apply security training in their day-to-day activities can be as important as how many times your company is targeted by a phishing attack.

NUMBERS DON'T MEAN EVERYTHING

SOC effectiveness isn't just about numbers. It is also about the people in your organization and how they prioritize security operations and react to and interact with cybersecurity tools and threats.

step three

Evolve and innovate.

By its very nature, the world of security operations is in constant flux. Technology evolves sometimes more quickly than we can keep up. Cybercriminals are increasingly more innovative in their attacks. Cybersecurity tools are constantly changing and improving. And security budgets may increase or decrease from year to year. On top of it, the needs, objectives, and goals of your business and your customers may change as the company grows or as new products and services are added. This means that the end goal of "effective security operations" can become a moving target.

Prioritize and align business and customer needs

Corporate objectives and goals are constantly changing. Security operations needs to always re-evaluate their own internal practices and metrics to make sure they align with changing corporate objectives and strategies.

Think outside the box

A rapidly changing technology and threat environment means that even though your way of doing things has always worked, tomorrow that may change. Keep an eye on trends and threats and don't be afraid to explore other ways to evaluate how your team or your company is managing a new technology or addressing an evolving threat.

Start with a common benchmark

There are numerous models and methods available to security professionals to help them create a common standard for effective security operations. Two of the most common—the NIST Cybersecurity Framework (CSF) and the Department of Energy Cybersecurity Capability Maturity Model (C2M2)—are designed to complement an existing cybersecurity program. Their structure is also usually adaptable and scalable to organizations of different size, industries, budgets, or levels of maturity.

Ensure effective framework implementation.

Deciding on a standard framework can provide a meaningful opportunity to identify where gaps exist or where processes can be strengthened. Frameworks also help to support cybersecurity risk management at all organizational and internal process levels. But, to make the benchmarking process successful, the security operations team needs to be straightforward with itself and others about where security is at present and where you hope to be in the future.

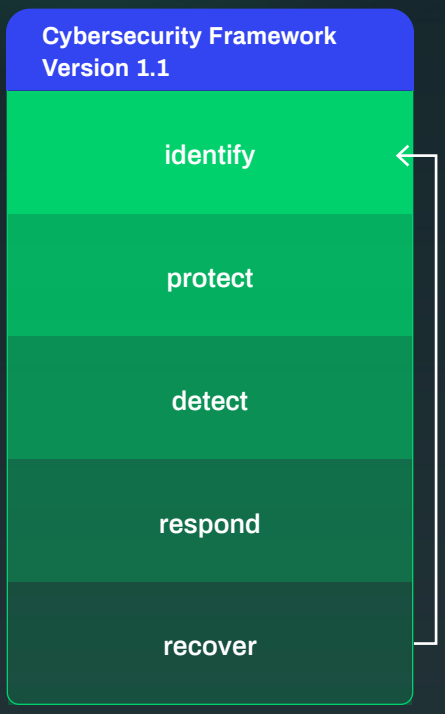
Be honest and transparent—Once you've decided on a benchmark, be honest about your organization's actual security capabilities and maturity.

Engage—Spend time engaging with other parts of your business, such as operations, supply chain, HR, and marketing so you can better understand corporate goals and risks and assess benchmark realities.

Prioritize—Once you've identified risks, prioritize your actions in terms of investment in people, budget, and technologies to help reduce risk.

Baseline—After you've engaged other teams, identified risks, and prioritized actions, baseline your overall existing security capabilities through assessments, performed by an internal team or a third party.

Develop a Process to Track Progress—With your baseline completed, develop a process to track your progress at least quarterly, focusing on domain-specific initiatives.



NIST Cybersecurity Framework (CSF) Model

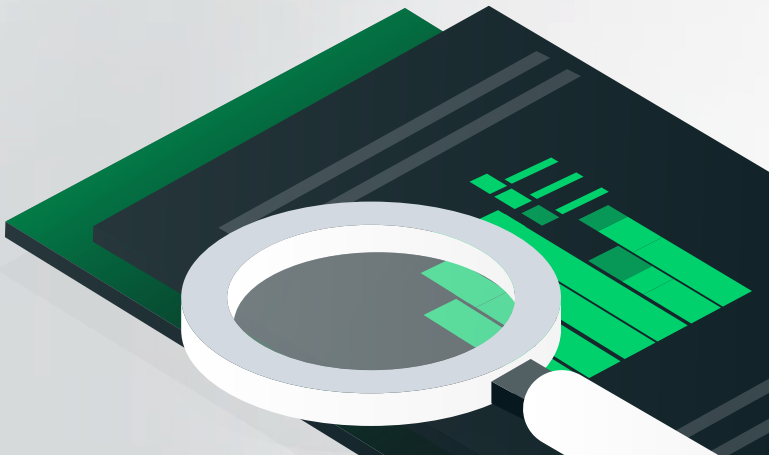
Choosing and using the right metrics

Once you've selected and established your framework, another key component in effective security operations is identifying what to measure and how to measure it. Recognizing the value of metrics means understanding that they are more than just a series of numbers. They can be tactical or strategic, quantitative or qualitative, and used collectively to develop a broader analysis. As you seek to maximize your security operations effectiveness, **it is critical to select metrics that are aligned to organizational goals and objectives.** It is also important to use your metrics to ensure you are measuring not only daily issues, such as threats, but also your progress and improvement in addressing and managing those threats.

Identify Metrics

Knowing what to measure is as important as the measuring process itself.
When identifying metrics, a security operations team should consider all of the following:

- **Define metrics as they relate to corporate goals and business and security policy**—As you identify your metrics, consider corporate goals and objectives as well as business policies, security policies, and the business and security controls that are currently in place.
- **Define metrics by audience**—Metrics can also be defined based on internal and external audiences, such as internal staff, business units, stakeholders, and the board. And, each of these groups may require slightly different metrics.
- **Define both strategic and tactical metrics**—Strategic metrics are often more focused on outcomes and aligned to corporate concerns or business goals. For example, demonstrating to stakeholders or leadership the relationship between the number of incidents that occurred as a result of the shortage of staff or the lack of a key position would be considered a strategic metric, because you're using the metric to address a known issue or the longer-term objective of hiring more staff. In contrast, tactical metrics are often aligned to quantitative concerns, such as mean-time-to-detect. Tactical metrics might also be a series of numbers that individually mean little, but when combined into a larger analysis contribute more broadly to an overall strategic initiative.
- **Leverage both quantitative and qualitative metrics**—It is often too easy, particularly in the world of cybersecurity, to concentrate on only quantitative metrics. Don't ignore valuable qualitative metrics, such as risk assessments that focus on perceptions and probability or the extent to which staff actually understand and apply cybersecurity training. Qualitative metrics can have an equally profound impact on the overall effectiveness of your security operations as typical quantitative number sets.
- **Avoid arbitrary metrics**—Don't select metrics simply for the purpose of having a metric. All metrics should tie directly to corporate goals, objectives, and risks, as well as have a clear path for improvement.



Define key metrics

While it is important to track as many metrics as are needed, not all metrics are equal. Some metrics may be more critical than others depending on the audience—such as board members or key customers. When defining critical metrics, it is important to not only focus on the standard ones, such as the total number of advanced persistent threats (APTs) or the number of malware blocked during a given day. Examples of critical metrics may include:

- **Access**—Companies that have a solid grasp of the time frame for managing system access or system "downtime" often are much better at analyzing and measuring the overall success of their security operations program. Consider metrics that look at how long on average it takes to get up and running again if access is lost. (Often this number is bigger than most people expect due to the ticketing queue process.)
- **Third-party Access**—Third-party risk is often overlooked. Yet, it's no secret that some of the biggest breaches in corporate history occurred via third-party access points. Ensure you know the number of third-party entities that have access to your corporate systems as well as the number of systems they've been granted access to.
- **Phishing**—Phishing is often the main point of entry in the majority of breaches. Keep track of all phishing metrics (not just click rate), such as fill-in rate, repeat offenders, forwarders, web filter security functionality (did it stop the phishing attempt?), and the types of devices staff were using when they clicked on a phishing link.
- **Cyber Violations**—People are often the weakest link in the security chain, and there is a long list of security incidents that can be tied directly back to staff. In addition to phishing, track corporate cyber violations, including malware downloads, stolen or lost assets, or policy violations (such as the installation of unauthorized software or inappropriate use of assets). Observing the types of staff cyber violations can provide insight into possible weak links in security training. In addition, track repeat offenders to better understand where security gaps might exist.
- **Cyber Program Adoption Rate**—The overall adoption rate of your cyber program is an important strategic metric that every business should track. It is also a good metric to report to the board. When evaluating your cyber adoption rate, think about the following:
  - **Look at the total number of critical and high vulnerabilities discovered during your software development lifecycle (SDLC) scanning compared with the percentage of every application in your environment that has or has not actually been scanned.**
  - **Identify the owners of every application in your environment.**
  - **Make sure you know where the repository sits.**
  - **Look at the number of systems in the active directory/configuration management database (AD/CMDB) vs. the number of systems in your security stacks management console.**
- **Complexity Reduction**—Another set of key metrics to consider are those associated with complexity reduction. Things like domain consolidation (going from 20 domains with 2-way trust to only 5 domains) can strengthen your overall message to stakeholders. Security operations can also look at measuring the reductions in firewall rules, VPNs, groups within groups in the active directory, and the number of service accounts. In addition, technology consolidation and vendor standardization can reduce complexity—for example, collapsing three firewall vendors down to one vendor. Finally, look at single sign-on (SSO) adoption and standardization to reduce complexity by minimizing identity stores and authentication methods.

Use metrics to measure progress and improvement

Once you've defined and prioritized metrics, you also need to understand how to use them effectively to measure progress and improvement and ultimately demonstrate both team performance and operational impact. For example, to demonstrate team performance, consider metrics that clarify the amount of time an analyst has to investigate and validate a certain number of events over a period of time. When demonstrating how your SOC is impacting overall corporate operations, examine how many times downtime has impacted the delivery team, customer team, infrastructure team, or platform or system.

SECURITY RAISES DIFFICULT QUESTIONS

One of the issues faced by companies is what to do with repeat cyber violators. **Are we ready as an industry to hold staff to the same cyber standards as we do in HR?**

Managing and balancing vulnerabilities

Maximizing SOC effectiveness also means **understanding where your corporate vulnerabilities exist and knowing how to manage them.**

Understand the costs, risks, and impact of vulnerable systems

In order to successfully manage vulnerabilities, security operations personnel first need to understand the costs and risks of vulnerable systems and the impact those systems may have on not only other connected systems, but also the company as a whole. Key things to consider include:

Age—Spend some time identifying the oldest vulnerabilities in your network, and don't forget legacy systems, such as EOL Operating Systems, Products, & Frameworks. Windows 2000, Classic .NET/ASP apps, etc.

Maintenance Purpose—Why are you maintaining vulnerable systems? What are the systems used for?

Risk—What are the risks—both system and corporate—associated with these vulnerable systems?

Impact—What is the current or potential impact of these vulnerable systems on your business? How critical is the aging system to overall corporate priorities?

Balancing vulnerability risk and cost

Once you identified vulnerable systems and assessed their vulnerability impact, it is critical to balance that information against overall cost and risk. Ask the following questions about legacy or vulnerable systems:

- Is it more cost effective to mitigate an old system that can't be patched, or would it be simpler to just get rid of it?
- Is the system making your company more or less money than it is costing you to keep it safe and operational?
- Even if it is making your company some profit, is that profit worth the risk and impact if that system were compromised?
- How much would a compromised vulnerable system cost your company both in dollars and reputation?

Many companies keep legacy platforms operational because they earn the company money. But the cost of a compromised vulnerable system could end up being far more in both dollars and reputation if the legacy system infects other systems. Be honest when you evaluate the true risk and cost of a vulnerable or legacy system.

THE COST OF "TIME TO PATCH"

Understand the true cost of a time-to-patch scenario. How many FTEs and how long will it take to patch legacy systems to 100%? **And have you fully identified 100% of the legacy assets on your network or just 100% of the critical assets?**

Managing budgets and ROI

Budgets have a direct impact on a team's ability to successfully manage security operations. Therefore, **it is critical to create and manage a SOC budget so it aligns to corporate and client outcomes and accurately reflects people, products, initiatives, and risks.** At the same time, both the SOC team and the CEO and CFO need to understand that there is a difference between corporate "return on investment" (ROI) and the overall value that security people, products, and services bring to the company and the client.

Budget—correlation, focus, and risk

When developing a SOC budget, align it to identified risk and the cost of the initiative—both the people and the product. Consider backing into the budget based on desired outcomes for the next 12 months and not corporate revenue or last year's budget. In addition, consider the following:

- **Define your budget based on corporate priorities and needs, not corporate maturity**—When developing your SOC budget, don't define it based on the maturity level of your organization. Some medium-sized organizations have established a SOC that requires no significant expansion. By the same token, both a mature organization or a start-up may find that the needs and impact of a new product or client may drastically increase overall corporate risk and require a significant increase in the security budget.
- **Be prepared to deliver**—If you ask for budget to support enhanced security or more staff, be prepared to deliver based on your budget ask.
- **Understand key dependencies**—Your security operations budget may also be tied to the requirements of other teams, such as marketing or sales. For example, if your marketing team is planning on launching a new online ordering system or your sales team is planning on a more complex customer management database, then security needs are going to change. Your team may also need support from other IT teams, such as infrastructure, but their priorities may not be your priorities. Be sure to align the needs and requirements of all teams as you build your budget.
- **Don't be afraid to outsource**—Sometimes the needs of the organization may require you to outsource areas of expertise to maximize budget effectiveness and ensure goals are met.

The value of internal security operations vs. return on investment

It has become commonplace in many companies to try to align a product, service, staff, or budget to ROI. But the truth is that an internal security operations team simply doesn't generate revenue and will likely always remain a cost center. Therefore, defining a new security solution based on its return on investment can be difficult.

However, if your stakeholders and executives still require you to calculate your ROI, then consider focusing on metrics that relate directly to incidents and their effect on business operations. Examples include:

- Security Information and Event Management (SIEM) Log Source ROI
- Next-generation Firewall (NGFW) Feature ROI
- Next-generation Antivirus (NGAV) / Endpoint Detection and Response (EDR) Prevention ROI
- Data Loss Prevention (DLP)-confirmed IP Theft ROI

You may also need to wait until your new cyber technology matures before you can accurately calculate its ROI. For example, an initial investment in a new cyber solution may require the addition of software or hardware further down the road. But this may not be immediately apparent or necessary.

Value and cost avoidance

Ultimately, if you're running or managing an internal security operations team, rather than thinking of cyber solutions and security operations in terms of overall return on investment, think in terms of overall value and cost avoidance. Work with your stakeholders and executives to help them understand that security is a long game and investing in certain technologies can help later down the road. Make sure to highlight areas where costs were avoided or describe scenarios where costs could be avoided. For example, the cost of a security problem could cost a certain amount in incident response (IR) fees, resource capacity, project stall, or delayed timelines. Therefore, the company can avoid these costs by avoiding the problem by incorporating a certain security solution.

PEOPLE (NOT TECHNOLOGY) ARE YOUR REAL ASSETS.

When calculating overall SOC 'value' remember that your staff are your most important asset. **Technology comes and goes, but the expertise and experience of a security operations professional is hard to replace.**

THE SQUAD DELIVERY MODEL

- See how the deepwatch Squad Delivery Model provides named resources to foster collaborative, high touch, tailored services that meet your specific security needs and requirements.

Maximizing success through collaboration

One of the most important things to remember when maximizing effectiveness is that security operations is not an island and your team can't do it by themselves. **Cybersecurity is a team game, and everyone needs to be involved.** Your security operations team needs to collaborate with other divisions and departments to understand priorities, goals, and objectives.

Information Technology (IT)

Security operations and IT often work hand-in-glove. Therefore, it is critical to communicate regularly with the IT team, meeting weekly at minimum. Align both teams' priorities, even if it means you need to give and take a little with the budget and resources. Most importantly, make sure security operations and IT share common goals and that the teams partner up often to ensure efficient solution implementation.

Human Resources (HR)

Value your people and make sure they know they're valued. Your staff are the ones that are going to make sure you succeed. Stay on top of the working environment and balance staffing needs carefully. You may find, for example, that it makes more sense to give staff salary increases instead of hiring several new staff members. Don't be afraid to praise staff when appropriate and definitely force staff to take time off if overwork or burnout is threatening the overall product/service quality or increasing the risk that you might lose staff.

In addition, work closely with your HR team to make sure they understand any issues or needs your team may have. The cybersecurity workforce gap is a significant and real problem. Ensure your HR recruiting team promotes professional development opportunities in cybersecurity and understands how to appropriately set cybersecurity applicant qualifications.

Marketing

Marketing can help the security operations team facilitate a culture of company-wide cooperation and support, just like they might with any company initiative. Don't be afraid to leverage the skills of the marketing team to generate internal buzz for a new security product, feature, or cybersecurity training. Marketing can also help build cyber awareness through promotion and internal communications.

The Board

Approach your organization's board of directors differently than you might other departments. Remember that boards tend to think 'big picture'. Therefore, give them strategy, and don't weigh them down with tactics and minutiae. Consider the following:

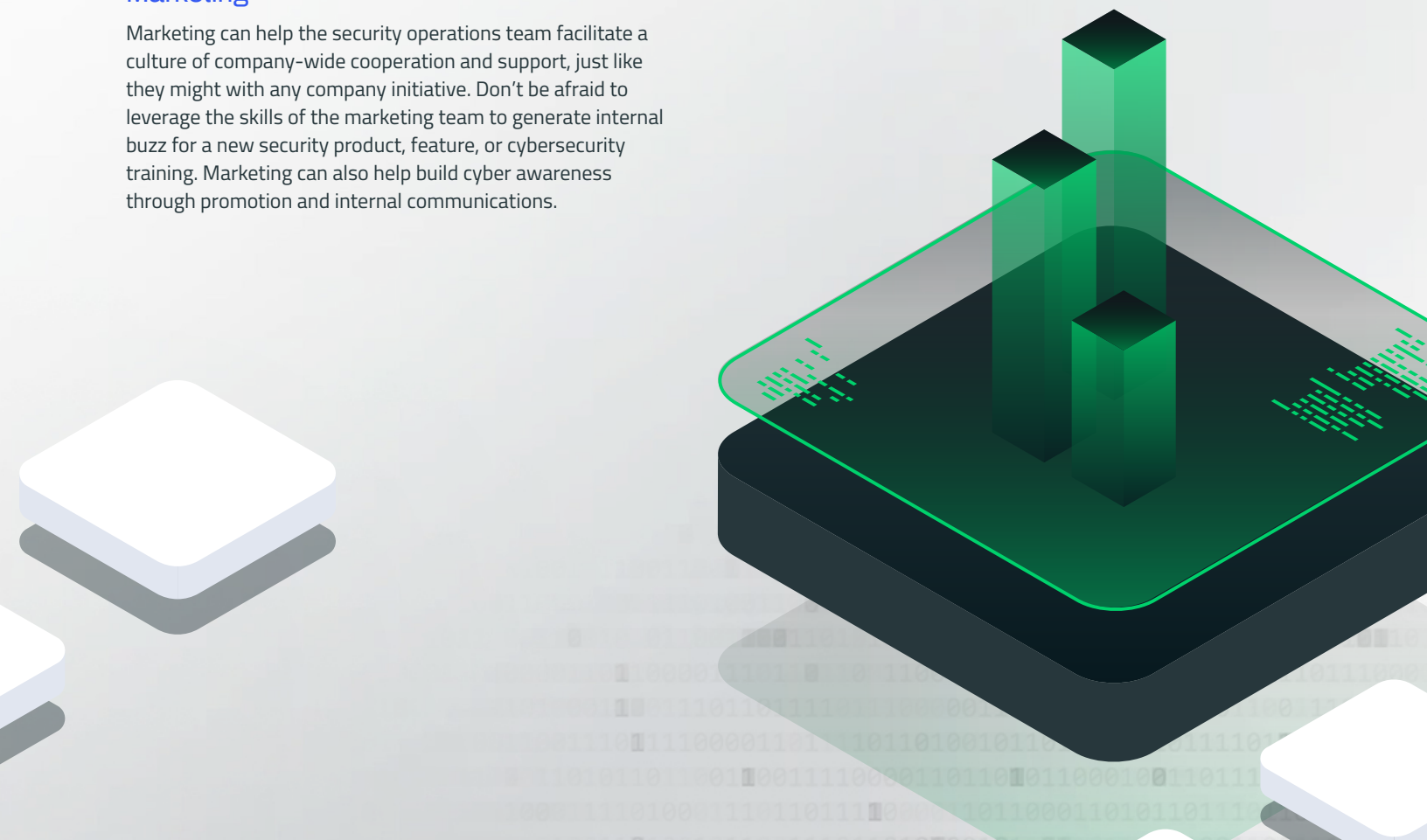
Focus on overall business impact—When meeting with the board, focus on overall business impact and how security capabilities reduce corporate risk.

Don't spend time focusing on new gadgets or statistics—New security software details or the number of blocked IP addresses likely means nothing to non-tech savvy board members. Use your time with the board to discuss overall strategic initiatives.

Correlate security initiatives to business goals—When discussing security initiatives with your board, make sure you correlate the initiative to corporate goals and objectives—and be sure to align security risk to business risk.

Be transparent and honest with the board—Don't minimize security risks or the level of your security maturity, even if you find it tough to admit or it puts your organization in a less-than-stellar light.

Demonstrate business value—Describe to your board how your security operations activities mitigate business risks and contribute to overall business goals. Don't just show them metrics and key performance indicators (KPIs).



External Stakeholders

Different groups require different collaboration and engagement approaches.

Customers and Clients—Customers and clients often need encouragement to take cybersecurity seriously. (This is also a good opportunity to leverage the marketing team for ideas on how to promote cyber with customers and clients.)

Auditors & Regulators—You should communicate with auditors and regulators at least once a year and use their knowledge and expertise to obtain information and opinions on new laws and regulations.

Vendors, partners, and third parties—Vendors, partners, and third parties need to be held accountable for whatever security solutions and regulatory requirements are relevant to them. Remember that their risk is your risk. Evaluate the security practices of all vendors and partners and consider creating supplemental agreements requiring vendor security audits and assessments. In addition, meet with your vendors and partners to find out:

- Which of your corporate networks and what data does the vendor have access to?
- What is the vendor doing with the information?
- What is the risk to your business if that vendor is breached?
- Does that vendor share your company data with any other external organizations?

Tracking activities and success

In collaborating with these groups, it is critical to set regular meeting schedules and track not only how often you meet, but what you discussed and the purpose and outcomes of the collaboration points. In addition, keep track of how many projects, releases, and 'go lives' happened in conjunction with other teams where someone from cyber was directly involved. Finally, ensure that security issues are discussed when and where appropriate—for example at "all hands" meetings or during October's annual Cyber Awareness Month.

THIRD-PARTY VENDORS MAY BE ONE OF YOUR BIGGEST SECURITY RISKS.

A recent study suggests that **more than 56% of large corporate data breaches originated with a third-party entity**, such as a vendor or supplier. Businesses need make sure that any risks associated with vendors, suppliers, and partners are prioritized, addressed, and mitigated.

Evaluating the costs and benefits of in-house efforts vs. outsourced MDR

When you're evaluating the benefits and costs associated with maintaining an in-house SOC compared with outsourced solutions, **it is important to look at the implications and value of the various in-house/outsourced options available.**

DIY Insourcing

There are several metrics to measure with when you decide to maintain your own in-house security operations team, as well as pros and cons to consider. The total number of employees is going to be a direct cost on your budget, while recruiting and training will be an indirect cost. Insourcing means that talent stays in house and there are career growth opportunities for your staff. You also have the ability to customize all the workflows and processes and procedures that may be needed.

On the flip side, DIY insourcing also means that certain areas of expertise are subject to the talent pool that is available in a given geography. You are also faced with personnel management issues, turnover, and continuing education.

Managed Detection & Response (MDR) Outsourcing

Managed detection and response (MDR) is an outsourced service that provides organizations and security teams with additional resources and capabilities for threat hunting, advanced detection, and effective response and mitigation to threats. The most effective MDR providers act as an extension of an organization's internal team and provide value through technology management (i.e. managed SIEM and firewall) and 24/7/365 alert monitoring, validation, and escalation.

Estimates suggest that you can use three times fewer internal staff when you outsource, reducing direct and indirect personnel costs. And your business will not necessarily have to front all the costs associated with technology infrastructure. In addition, outsourcing means that services are usually implemented fairly quickly, typically within 60 days of contract execution. You will also have access to named personnel that are trained on current best-of-breed technologies.

In general, the overall value to outsourcing outweighs the costs. Companies that outsource some or all of their security operations activities benefit from expanded operational capabilities, such as a broader range of skills, knowledge, and experience with security operations center (SOC) analysts and engineers. Businesses also enjoy a more comprehensive list of value-added technologies without needing to build and maintain them in house. Outsourcing also enables your internal team to focus on remediating the threats, instead of spending hours identifying the threats.

Benefits when partnering with an MDR provider:

- Reduced personnel costs
- Quicker time-to-value
- 24/7 access to named resources
- Technology expertise
- Increased ROI

Finally, there are cost savings associated with an MDR outsource, particularly given the current shortage in staffing. The MDR provider invests in the technology, tools, skills, staff, and operational best practices, creating cost savings for the business.

Estimates suggest that you can use three times fewer internal staff when you outsource, **reducing direct and indirect personnel costs.**

FROM THE DEEPWATCH BLOG

Why Aren't You Outsourcing Your Cybersecurity Operations?

Conclusions

An effective SOC is more important than ever. While the latest security solutions can help protect your organization's assets, solutions aren't the only answer. To maximize security operations' effectiveness, businesses need to approach security comprehensively, aligning the overall SOC framework to an in-depth understanding of corporate and customer goals and risks, and identifying and leveraging critical metrics to help drive a deeper understanding of threat impact. Additionally, SOC teams need to operate collaboratively, engaging with not only IT teams, but also HR to help drive recruiting and hiring efforts and marketing to help promote security efforts corporate-wide. Finally, SOC teams need to evaluate the costs and benefits of all operational efforts, identifying the cost and risk impact of potential system vulnerabilities and recognizing that it could be more beneficial to outsource certain components or areas of expertise to an MDR provider.

Security stakes are higher than ever. By partnering with a proven MDR provider, organizations can build and maintain an advanced SOC that minimizes the overall impact of security threats and maximizes effectiveness and ROI.

Interested in maximizing the effectiveness of your security operations?
Schedule a chat with a security expert at Deepwatch today.

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 secures enterprises via its unique, highly automated cloud based SOC platform backed by a world class team of experts that protect your network and digital assets 24/7/365. Deepwatch extends your team and proactively improves your cybersecurity posture via our proprietary maturity model. deepwatch's managed security services are trusted by leading global organizations

CONTACT US

sales@deepwatch.com
7800 E Union Ave, Suite 900 Denver, CO 80237
855.303.3033

www.deepwatch.com