
deepwatch™
Overcoming the Security Talent Shortage
Practical Staffing Strategies for Security Leaders
www.deepwatch.com

Table of Contents

01. Introduction

According to research by Cybersecurity Ventures, the number of unfilled cybersecurity jobs stabilized in 2022, and yet 3.5 million jobs will go unfilled in 2023, with more than 750,000 of those positions in the U.S.[1] The challenges with recruiting, hiring, and retaining experienced security personnel have reached a whole new, maddening level, driven by a system straining to fill a vast number of security positions with an insufficient talent pool. Staff turnover, high salaries, recruiting issues, and lean budgets all contribute to this perfect storm.

An added challenge faced by security leaders is that, despite advanced security tools and technologies, the lack of experienced security staff hinders most organizations from realizing the full capabilities of these technologies. It also means they're unable to sufficiently manage their risks in order to securely scale along with business growth.

The most recent study revealed a critical finding: "Two-thirds of study participants report a cybersecurity staffing shortage is placing their organizations at risk."[2] This shortage means that in-house security teams often work extra hours and give up vacations and holidays just to stay marginally on top of their workloads. The long working hours and increasing threat pressures placed on IT security decision-makers and teams will not be sustainable at this pace. This is especially worrying in an enterprise landscape where the average cost of a data breach in 2022 was $4.35 million and will likely only get more expensive throughout 2023.

In this eBook, you'll find actionable guidance to help make the case for security program funding to gain these benefits:

- An improved security staffing process that meets the organization's need for skilled personnel within budget.
- A fully optimized security operations center that supports growth, is secure against threats, and facilitates security in cloud, hybrid, and multi-cloud environments.
- A risk management mechanism to mitigate security risks associated with technology and staffing the security operations functions to secure the increasingly distributed enterprise.

02.
Security Staffing **Is a Never-Ending Task**

Whether you're staffing a Security Operations Center (SOC) or integrating a Security Operations (SecOps) program into the organization, your security team needs access to experienced staff that are available 24/7/365 to manage all incoming security risks and provide adequate protection against an evolving threat landscape.

Three Key Facts Underscore Critical Secops Staffing Challenges In The Current Environment:

1. **Recruiting and hiring SecOps staff, particularly personnel skilled in security event detection, threat hunting, and incident response,** is an incredibly difficult undertaking for many organizations since the skill sets are less common and in high demand.

2. **Cybersecurity practitioners experience alert fatigue when an overwhelming number of security alerts are firing from disparate security technologies,** causing desensitization and staff burnout. If a real security event is lost in millions of daily alerts, a threat actor can lurk longer in the network, increasing 'dwell time.'

3. **The cybersecurity staffing shortage is worsening an already challenging hiring environment.** As threats have evolved, cybersecurity requirements have increased. The U.S. government has outlined the NICE Framework demonstrating the increasing complexity organizations face when hiring in house security staff.

50+ cybersecurity work roles are described within the Workforce Framework for Cybersecurity (NICE Framework), developed by the U.S. Government, as a free resource tool for the public, private, and education sectors in the United States.

03. The Challenges of **Operating a Modern-Day SOC**

To operate efficiently and effectively, SOCs need the right people, processes, and technologies. They need to be staffed with enough analysts possessing the right capabilities and experience to evaluate what artificial intelligence (AI) cannot.

Despite progress in automation technologies, every SOC still needs human intelligence, imagination, and experience to identify patterns and assess threat outliers that could indicate that an attack is underway. An expanding attack surface, an increase in total threats, and increasingly sophisticated obfuscation techniques, combined with the cybersecurity skills shortage, means most modern, in house, enterprise SOCs cannot fully react to the growing complexity of security operations.

A Day in the Life of A Security Analyst

- Monitoring the SIEM for suspicious events and anomalous activity;
- Investigating suspicious events and incidents using open-source and proprietary intelligence sources;
- Managing incident response;
- Tuning SIEM alerts to improve detection engineering;
- Keeping current with information security news, techniques, and trends;
- Monitoring log collection activities;
- Reporting any changes in the security environments to the SOC Manager or CISO.
- Notifying other critical stakeholders of security incidents.

Some of the challenges today's enterprises face when it comes to SecOps include:

- Staffing shortages (both lack of staffing both in quantity and skill level)
- Alert fatigue and burnout
- Work/life balance, Disparate security technologies
- Managing security compliance and risk

04. Alert Fatigue

Alerts arrive from disparate security tools, each with a limited scope within the environment, and therefore with a very limited ability to be contextualized before being logged. Inadequate ability to to efficiently correlate and filter these raw alerts risks inundated analysts with meaningless alerts, making it extremely difficult for them to identify the true positive needles in the proverbial haystack, the result is the problem known as alert fatigue.

Meaningful alerting is created by a useful mix of threat intelligence, indicators of compromise (IOCs) watchlists, machine learning, and automation in order to avoid this condition. This sophistication requires continuous adjustment and improvement in the alerting process.

Consequences of alert fatigue include:

- Favoring or adjusting certain types of alerts to reduce overall volume.
- Ignoring certain alert categories.
- Ignoring alerts in general because of the high false positive rate

An excessive number of alerts creates a series of additional problems by:

- Contributing to analyst burnout, as the daily onslaught of alerts eventually becomes too much to bear in an already stressful career.
- Adding costs to the security team and company, as skilled staff are taken away to work on more important tasks, instead of analyzing potential threats, and tuning security technologies to eliminate false positives.
- Increasing the risk of an actual security incident occurring due to the tendency of analysts to ignore alerts.

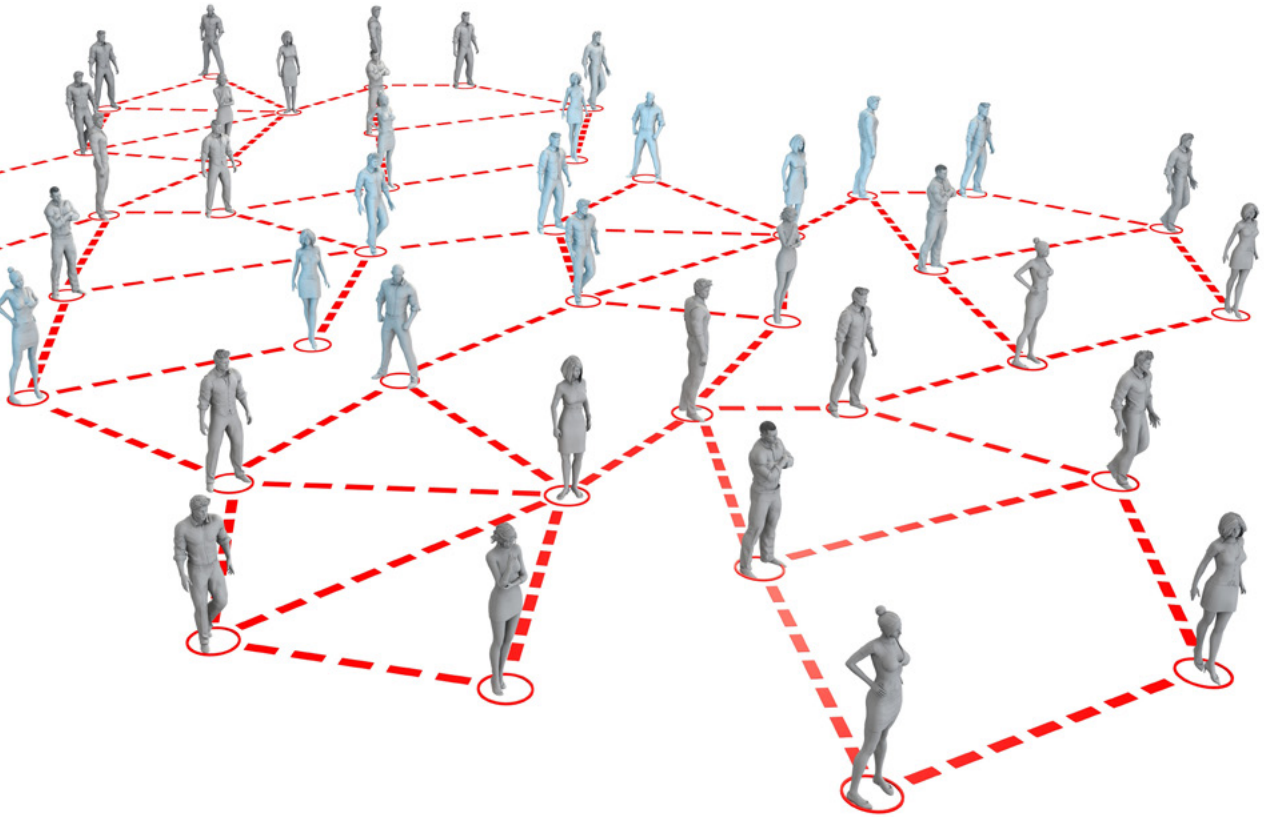
05. SOC **Staffing Problems**

Staffing a modern SOC can be difficult, and an inadequately staffed SOC can be dangerous to business.

60%

Of businesses surveyed **said the lack of skilled cybersecurity professionals was putting their business at risk.**

- ISC2 STUDY



Organizations attempting to staff their own SOC often struggle with the following challenges:

- **Maintaining optimal staffing** and creating an effective SOC staff structure.
- **Prioritizing roles** to ensure the right team is in place.
- **Balancing automation** with the right personnel.
- **Ensuring the SOC staffing model** has enough flexibility to scale.
- **Staffing for maturity** and future growth.
- **Providing career progression with a limited budget** and competitive hiring landscape.

06. **Disparate** Security Technologies

To cope with stretched security budgets and the inability to find skilled staff, businesses often decide to expand their security operations and SOCs by investing in more in house security technology, like security information and event monitoring (SIEM) solutions and intrusion detection systems (IDS), incorrectly assuming that automation and AI and ML can somewhat augment for a lack of qualified staff. Advanced technology still can't fully compensate for the skills and expertise that an experienced cybersecurity professional can bring to SOC activities. The addition of new technology can also serve to increase the burden on personnel.

In the study "The Life and Times of Cybersecurity Professionals 2023,4" a cooperative research project by the Enterprise Strategy Group (ESG) and the Information Systems Security Association (ISSA), a third of the participants said that the skills shortage had created a scenario that prevented them from learning about or utilizing some of the company's security technologies to the fullest potential.

Security Compliance and Cybersecurity Risk Management

- As organizations try to cope with increasing cyber risk, governments and industry continue to build cybersecurity and data policy to protect both businesses and consumers. The increasing number of complex regulations and the risk of non-compliance fines put pressure on enterprises to hire knowledgeable staff to facilitate security compliance and risk management concerns.
- SOCs need to be staffed with individuals who understand compliance issues and risk management processes and can monitor systems accordingly. The current staffing shortage makes it difficult for maturing businesses to adequately address regulatory, risk, and compliance concerns.

Overcoming the Security Operations Staffing Shortage

Companies today can choose from one of the following three options to improve their security operations:

- Hire an in house Security Operations team and build an in house Security Operations Center.
- Hire an in house team to work with a Managed Security Services Provider (MSSP) for basic security service support.
- Partner with a Managed Security Services Provider for fully managed, outsourced 24/7/365 security operations experts and technology services.

07. Benefits of Using an MSSP to **Staff Your SecOps and SOC**

Partnering with a Managed Security Services Provider can help businesses optimize the entirety of their security operations. Outsourcing SecOps and SOC activities to an MSSP offers cost-effective benefits over attempting to manage security in house.

Working with an MSSP to deliver security services can help:

- Reduce Cybersecurity Costs by offering the expertise and latest technology solutions
- Reduce Alert Fatigue through a combination of automated alert monitoring and analysis by expert staff
- Inventory Management by helping SecOps and SOC teams inventory all endpoints and users on a network
- Ongoing Management and Maintenance of Security Tools and help determine which tools to purchase, facilitating the purchasing process, and installing the technologies, then managing and maintaining the tools
- Incident Response with the SOC staff the support necessary to ensure no alert, anomaly, incident, or attack gets missed, particularly on holidays, weekends, or at night
- Improve Visibility with experts with the skill sets to analyze and correlate attacks across millions of transactions
- Seamless Integration due to the experience and expertise to integrate operations, staff, and additional technology solutions seamlessly with existing enterprise SEIM, vulnerability management, and active response
- Improve ROI by leveraging existing technology solutions to improve ROI by maximizing the value of your existing tools

08. **The Deepwatch Managed Security Platform** Fortifies Security Operations Staffing for the Future

Deepatch is the leading managed security platform for the cyber resilient enterprise. We partner with your team to help you anticipate, withstand, recover from, and adapt to threats in your unique environment. We operate as an extension of cybersecurity teams by delivering unrivaled security expertise, unparalleled visibility across your attack surface, precision response to threats, and the best return on your security investments.

The Deepwatch Managed Security Platform includes our threat management capabilities, Deepwatch Security Center engagement technology, and Deepwatch Experts including named analysts, engineers, and threat hunters that serve as an extension of your organization.

The trusted Deepwatch Managed Security Platform helps organizations scale investments and improve security maturity with expert staff for 24/7/365 threat detection and incident response. This choice covers the organization for business continuity in the short-term, and strengthens security maturity over time to build cyber resilience and secure the future of the business in the long-term.

Conclusion

The frequency and complexity of today's ransomware attacks require more time and resources than most security teams have to fight them. Managed detection and response can help fill cybersecurity skills gaps, and provide faster response to ransomware incidents. As the leading managed security platform for the cyber resilient enterprise, Deepwatch helps teams identify risk, withstand and recover from successful attacks, and helps teams adapt their security programs to better prepare for novel or complex threats in the future.

Sources

- **1 Cybersecurity Jobs Report:** 3.5 Million Unfilled Positions In 2025, https://www.kron4.com/business/press-releases/ein-presswire/627962642/cybersecurity-jobs-report-3-5-million-unfilled-positions-in-2025/#:~:text=The%20number%20of%20unfilled%20jobs,remain%20through%20at%20least%202025
- **2 Overworked CISOs are Skipping Family Vacations and Holidays;** https://www.infosecurity-magazine.com/news/overworked-cisos-are-skipping/
- **3Citation: IBM Cost of a Data Breach 2022:** A Million-Dollar Race to Detect and Respond https://www.ibm.com/reports/data-breach
- **4 ESG RESEARCH REPORT,** The Life and Times of Cybersecurity Professionals 2023, Volume VI, A Cooperative Research Project by ESG and ISSA; https://www.issa.org/wp-content/uploads/2023/08/ESG-eBook-ISSA-2023.pdf