cyberbit

# Empowering the Enterprise CISO with SOC Team Readiness

sales@cyberbit.com | www.cyberbit.com

## Introduction

The role and responsibilities of the enterprise CISO is constantly evolving and expanding, but the backbone of the CISO remains the SOC team. The SOC team is the enterprise's last line of defense against cyber-attacks and intrusions. It maintains an organization's security posture and cyber resilience and delivers rapid incident response in case of an attack or breach. 72% of IT respondents to a Ponemon survey said that the "SOC is a key component of their cybersecurity strategy." The SOC is also crucial to reducing cybercrime costs. The average cost of a data breach, according to a recent IBM study, is $4.24 million (in the US $9.05 million) whereas the average savings to companies with an incident response team and an extensively tested incident-response plan is $1.23 million.

## Background

Despite the crucial role SOC teams play in cyber defense, CISOs often lack the staff they need to complete their SOC team. 40% of organizations struggle with SOC staff shortages and finding qualified people to fill the cybersecurity skills gap, according to the Exabeam 2020 State of the SOC Report. This leaves you with a SOC team that is continuously understaffed and lacking critical security skills.

Compounding the challenge is the inability to quantify and benchmark SOC performance and demonstrate its value to C-Suites. When you can demonstrate the value of your SOC team's performance and its security controls and technology, you can increase your team's overall effectiveness. You can better create, develop, and coordinate cybersecurity strategy, ensure adequate cybersecurity talent, prepare budgets, and identify further resources needed for cyber defense.

## The Challenge: A Lack of a Pathway to Cyber Readiness, Assessment Tools, and Benchmarking Tools

The solution to the understaffed SOC seems simple enough: hire more people, specifically more qualified people, and then monitor, quantify, and demonstrate the effectiveness of the team to continue improving its effectiveness.

Unfortunately, CISOs hit a lot of speed bumps when it comes to building a cyber-ready SOC team and monitoring and benchmarking its performance. The challenges can be summarized as follows:

1. **Prolonged searches for qualified candidates, mis-hires, long onboarding times, and low retention rates.** According to the US Department of Labor, mis-hires cost organizations at least 30% of the employee's first-year earnings. Long onboarding times and low retention rates are another significant drain on resources. According to a study by Deloitte, it takes nearly a year to onboard security analysts and then the analysts do not stick around for long. The same study also reported that after a year of onboarding, the average tenure is only about 2 years, resulting in a low ROI and steadily increasing recruiting/onboarding costs. One of the reasons for the low retention is that many frontline employees report a lack of a career path. According to the Ponemon Institute, SOC team members feel that investment in technology, training, and staffing was insufficient for them to do their job. When responding to a survey by ISC2 about possible employers, 88% of cybersecurity workers said that investing in training and certification was very important.

2. **Limited or no upskilling pathway for overcoming the lack of experience.** One of the biggest obstacles to achieving effective cyber resilience for an enterprise is its SOC team's inexperience and inability to upskill to a frontline-ready cyber defense posture. In their study on improving SOC effectiveness, Ponemon reports that 70% of IT security leaders surveyed claimed their SOC team lacked expertise. Without a skilled and experienced SOC, you will face an uphill battle to defend your enterprise, and outsourcing is not a satisfactory solution. For one, it is costly. A Ponemon study on the economics of SOCs, reports that on average organizations spend $2.86 million annually for in-house SOCs verses $4.44 million for outsourced SOCs. Furthermore, the same Ponemon study reported that 58% of organizations using outsourced SOCs rated them as ineffective.

3. **CISOs cannot quantify and benchmark SOC team performance.** Without the ability to determine areas of improvement, provide concrete examples of actionable resilient solutions, and demonstrate SOC team value, it is difficult to prove the SOC ROI to management and C-Suites and proceed with plans to further improve cyber resilience via development and investment in the SOC team.

## The Solution: Boost SOC Team Readiness with Better Talent, Upgraded Expertise, and Faster Response Capabilities

### *Assessing/Onboarding/Retaining*

Cyberbit provides hands-on candidate screening capabilities that improve assessment quality, reduce mis-hires, and shorten hiring by 50%. The Cyberbit platform includes onboarding programs, which reduce onboarding time for new hires by 70%, so you can hire the most qualified candidates and get them operational, faster.

In addition, Cyberbit improves retention by providing the type of training cybersecurity professionals need and want. 88% of cybersecurity professionals named "Invest in Training & Certification" as the most important factor in hiring and retention according to the (ISC)² Hiring and Retaining Top Cybersecurity Talent, 2018 report.

Cyberbit is the world's leading immersive training platform for SOC team professionals, novices, and hopefuls. SOC team members who train on Cyberbit are exposed to real-world attacks occurring on corporate grade virtual networks similar to what a member of a SOC would see daily. Commercial grade (IBM, Splunk, ArcSight, Palo Alto Networks, Checkpoint etc.) tools are provided to ensure that SOC Team members are training with the same tool types and feature sets they would have access to too during the normal course of business. By providing cutting-edge training to your SOC, you will experience better SOC team performance, faster onboarding times, more accurate recruiting, and better employee retention.

### *Upskilling*

The Cyberbit platform provides CISOs with unprecedented insight into the performance of their SOC team's human element, prior to a live incident. Using this information, you can easily identify skills gaps in your SOC or incident response capability, allowing the team to rectify skills and experience gaps in a safe environment purpose built for upskilling. Cyberbit helps you ensure that your SOC team is prepared to protect your enterprise's valuable digital assets and lets you stress-test and validate your SOC in live-fire simulated scenarios.

### *Performance Monitoring and Benchmarking*

Cyberbit dashboards allow CISOs to review and monitor SOC performance and maximize the technology investment. With the dashboard, you can quantify and benchmark the SOC team's performance, help team members understand where there are areas of improvement, measure the effectiveness of security processes, controls, and tools from leading providers including Splunk, Palo Alto Networks, CarbonBlack, Check Point and more, incorporate map training according to NIST, CREST, and the MITRE ATT&CK Framework, and demonstrate proof of the impact and value of investing in the SOC.

## Results:

- A SOC team that is battle-ready and prepared to protect the enterprise's data and systems using appropriate security tools and current frameworks for industry best practices.
- Insight into the human element of the SOC team that helps you identify and rectify skills gaps and prepare your team for an expanding attack surface.
- Enhanced fundamental and advanced skills for team members.
- Quicker and more effective incident response times built via participation in extensive simulated live-fire exercises.
- Compliance with national and international data protection laws.
- Maximization of detection and incident response technology.
- Proof of the benefit of SOC investment to C-Suites.

## Conclusion

SOC team readiness is crucial to the enterprise's ability to mount a powerful defense against cyber-attacks and intrusions. However, despite the critical role SOC teams play in cyber defense and resilience, CISOs often lack qualified staff needed to build a team that is frontline-ready and capable of rapid incident response. The antidote to this nagging issue is to give CISOs a pathway to better assess potential candidates, quickly onboard new hires, increase retention of the talent that is hired, and create an optimally performing SOC team that is ready to take on real world cyber-attacks.

### About Cyberbit

Cyberbit provides the global leading attack readiness platform for enabling SOC teams to maximize their performance when responding to cyberattacks. The Platform empowers security leaders to make the most of their cybersecurity investment by boosting the impact of the human element in their organization. Cyberbit delivers hyper-realistic attack simulation mirroring real-world scenarios. It enables security leaders to dramatically reduce MTTR, dwell time and cybercrime costs, improve hiring and onboarding, and increase employee retention. Customers include Fortune 500 companies, MSSPs, systems integrators, governments, and leading healthcare providers. Cyberbit is headquartered in Israel with offices across the US, Europe, Asia, and Australia.