cyberbit

Incident Response: The Bread and Butter of Security Operations Centers (SOCs)

Protecting client data
with a strong frontline defense

sales@cyberbit.com | www.cyberbit.com

Introduction

Organizations within the finance industry continue to be disproportionately targeted by cyber attackers. According to the Verizon Data Breach Investigations Report, the financial sector 'remains a favorite playground for the financially motivated organized criminal element." As a result, the security operations center (SOC) is more crucial to the security and integrity of finance firms than ever before.

Tasked with the job of enterprise security, the SOC team must be able to detect, investigate, prevent, and respond to cybersecurity threats and suspicious activity using a combination of tools, technologies, and techniques. It must be prepared to take defensive actions amidst an ever-evolving threat landscape and expanding attack surface.

Background

Delivering effective cybersecurity in an evolving threat landscape and expanding threat surface requires a combination of technology, intelligence, and human expertise, i.e., the SOC team. The SOC team is at the frontlines of protecting the company's digital assets. Financial institutions know this: more than 70% of respondents to a survey conducted by the Conference of State Bank Supervisors rank cybersecurity as their top concern."

The faster the SOC can respond to security incidents and the greater its expertise, the faster the containment and elimination of the threat and the less damage caused to the organization. The number one KPI today, according to Kaspersky, is the quality and speed of incident response. Critical to the SOC team's ability to mount a fast and quality response to an incident is its skills, experience, and readiness.

The Challenge

The SOC manager's ability to achieve rapid and quality incident response is often stymied because of the team's lack of preparedness, be it with incident response plans or lack of knowledge, skills, and experience. Fortinet reports that "73% of organizations had at least one intrusion/breach over the past year that can be partially attributed to a gap in cybersecurity skills".

The skills the SOC team must possess for fast and effective incident response include the ability to perform under pressure, use relevant security tools (e.g., Splunk SIEM, Palo Alto Networks Firewall, and Check Point firewall), implement and understand technologies, techniques, and security frameworks such NIST and MITRE, and execute these functions within the context of the organization's business needs.

Compounding the problem of a lack of skills is the lack of hands-on experience and overall readiness. According to IBM, "Companies with an incident response team that also extensively tested their incident response plan experience $1.23 million less in data breach costs on average than those that had neither measure in place."

The Solution: Assess New Talent for Quality and Augment Existing Team Skills and Readiness Levels

Overcoming the lack of skills and readiness needed to mount a robust defense is paramount to building a powerful, incident response ready SOC team. SOC managers need the tools to perform candidate assessment during the hiring process, speed up the onboarding process for new hires, and upskill the talent that has already been hired.

Better Assess Cyber Talent

Being able to assess talent at the hiring stage can reduce critical mis-hires that can later impact an organization's cybersecurity posture. "By hiring the right talent", Experis reports, "business will be better placed to fully protect their operations from malicious attacks – to do that, they need to have a broad perspective on how, who, and what they hire, and how they develop their existing staff." Cyberbit hands-on candidate assessment capabilities help SOC managers accurately and quickly determine if a potential candidate has the right skills for the job and shorten the hiring process by 50%.

Rapid Onboarding

Hiring and onboarding a SOC analyst takes over 7 months. The Cyberbit platform includes onboarding programs which reduce onboarding time for new hires by 70%, so SOC managers can hire the most qualified candidates and quickly get them operational. Any aspect of the program can be customized, including scenarios, infrastructures and SOC roles (Tier 1, 2, and 3 analysts, threat hunters etc.).

Upskilling Current Talent

Assessing whether an employee has the right skills and knowledge to be an effective member of the SOC team should not stop after the hiring process has been completed. Continuous performance improvement and assessment are crucial to preventing and resolving incidents and making the SOC team cyber ready for real-world, real-time cyber threats. According a report issued by ESG (Enterprise Strategy Group) and ISS (Information Systems Security Association), "a cybersecurity career demands continuing education, so infosec managers must make education and training a top priority." Furthermore, employees agree, and are willing to stay late to invest in performance improvement: 81% of all cybersecurity talent is willing to spend time beyond office hours for training.

With the Cyberbit platform, SOC managers can monitor each team member's performance (scores, activity, progress etc.), and measure competency with incident response frameworks (MITRE ATT&CK, NICE), tools from leading providers including Splunk, Palo Alto Networks, Checkpoint, CarbonBlack, Microsoft and more), and techniques. These KPIs give the SOC manager unprecedented visibility into team strengths and weaknesses that can be used to create a plan for skills and readiness improvement.

Stress Test Incident Response Plans

SOC analysts and incident response teams use cyber-attack playbooks to respond to incidents, giving the playbook a vital role in the SOC environment. The SOC team must understand the playbooks so they know how to quickly and correctly respond under pressure during a breach. Stress testing via Cyberbit's live-fire simulations helps SOC managers validate the readiness of their SOC team members while optimizing to reduce incident response times (MTTR).

The team's participation in these simulations provides the SOC manager with unprecedented insight into the performance of the team's human element. With this insight, managers can easily identify and rectify skills gaps in their SOC or incident response capability, optimize the response plans to use the best talent available for a specific use case (e.g., best firewall or EPP guy) and change response plans to account for the human element (incident escalation, data analysis, communication etc.).

Results:

- A SOC team that is battle-ready and prepared to defend the organization using appropriate security tools and current frameworks for industry best practices.
- Insight into the human element of the SOC team that helps SOC managers identify and rectify skills gaps and prepare their team for an expanding attack surface.
- Enhanced fundamental and advanced skills for team members.
- Quicker and more effective incident response times built via practice using playbooks and participation in extensive live-fire exercises.
- Reduction in mis-hires, 50% reduction in hiring time and 70% reduction in onboarding time.

Conclusion

Building a skilled SOC team that operates at full potential is vital to the security of every organization, but SOC managers lack a viable way of making sure their SOC achieves the level of readiness and experience required to effectively defend their organization against attack campaigns. Simply hiring and building a team and investing in cybersecurity does not build a sufficient cyber defense. SOC managers need to be able to optimize their SOC team in terms of skillsets, experience, and readiness by exposing them to attack simulations and live-fire exercises. Cyberbit offers a way for SOC managers to develop the hands-on skills and experience of their SOC team so it can perform at optimal levels and deliver the type of rapid and robust incident response needed for a powerful defense.

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.

sales@cyberbit.com | www.cyberbit.com

cyberbit