CYBERBIT
TRAIN FOR REAL

2020 SOC SKILLS SURVEY

How do security leaders build their SecOps team?

Introduction

The SOC Skills Survey Report of 2020 reports the results of Cyberbit's SOC Skills Survey, conducted in the fourth quarter of 2020, during SOC training workshops. The survey examines respondents' views around the cybersecurity employee lifecycle, hiring processes, skill development and training. The report highlights the challenge organizations are facing in hiring, retaining and upskilling cybersecurity professionals. Responses confirm the lack of skilled staff in cybersecurity, the struggle to locate the right talent to fill in open positions, and the lack of investment in effective training programs for existing talent. Much of these issues stem from hiring practices that were not adapted to cybersecurity needs as well as a lack of awareness of existing skill levels, and an inability to track the effectiveness of cybersecurity team or individual training.

Contents

Executive Summary

Cyberbit's first SOC Skills Survey asked respondents to report their experiences, gaps and challenges relating to the lifecycle of security operations and incident response staff, specifically around hiring practices, workforce development, skills levels, and training.

With more organizations launching security operations centers (SOCs), organizations increasingly rely on manual work to complement automated systems to manage their complex security stack. SOCs are becoming proactive, transitioning from an "alert center" to a threat hunting and incident response center, strongly relying on the skill level of its staff.

The Survey's findings offer insights into the makeup and strategy behind the building of information security teams inside enterprise organizations around the globe.

Respondent metrics indicate a significant gap between cyber leadership and human resources across the entire recruitment process. The largest barriers to recruiting an effective team seem to be the qualifications of incoming applicants, a lack of understanding of the requirements to join the team, and ineffective screening processes. In fact, 65% of respondents believe that less than 50% of applicants are qualified for the role for which they applied.

Regarding the skills within the SOC, half of respondents believe they are prepared to deal with a cyberattack while, on average 50% believe they are not prepared across the board. Technical Defensive Cyber Skills was where respondents felt the most prepared at 54% while Intrusion Detection and Network Monitoring led the skillsets in which respondents felt least prepared.

When it comes to training, SOC teams feel that their current form of training is impactful (54%). Once exposed to hands-on training like cyber labs and cyber ranges, 89% of respondents felt that this training type was more effective than their current training mechanism and 92% of respondents would recommend using immersive training for their organization.

A major avenue to improvement is focusing on building a better line of communication between cyber leadership and HR while focusing training on detection of attacks. Moving away from on-the-job and course-based training to hands-on training was heavily favored by respondents who are looking to improve their technical skillsets.

Key Results:

- Information security leadership needs to educate the HR department, which is missing critical knowledge when it comes to defining cybersecurity roles: Only 33% of respondents felt that HR understands the requirements to work in a cybersecurity team.
- SOC teams believe themselves to be the most underprepared in two areas: Intrusion Detection (55% unprepared) and Network Monitoring (58% unprepared).
- SOC teams rely on on-the-job training (41%) and offsite courses (26%) to advance their skillsets. Simulation based training (Cyber Labs (9%), Range (6%), and Red vs. Blue (7%) are only used by a combined 22% of respondents.

Survey Methodology

Cyberbit surveyed over a hundred cybersecurity professionals across 17 countries **(Figure 1)** from organizations with a SOC team of larger than five and IT budgets of over $20 million. Respondents supervise or are responsible for such activities including information security, threat detection and remediation, security operations management, and more. Respondents range in experience levels with 60% of respondents having at least 5 years of hands-on experience in cybersecurity **(See Figure 2)**. Survey data was collected via SurveyMonkey using multiple choice, Likert scale-format, and open-ended responses broken into three distinct sections: Hiring Practices, Team Skills Evaluation, and Cyber Training & Impact.

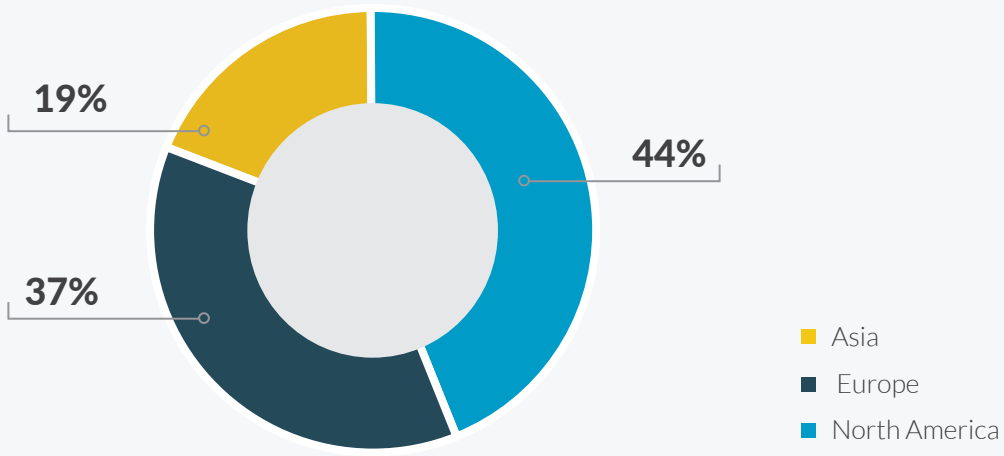


Figure 1 - Survey Respondent Breakdown

How many years of cybersecurity experience do you have?

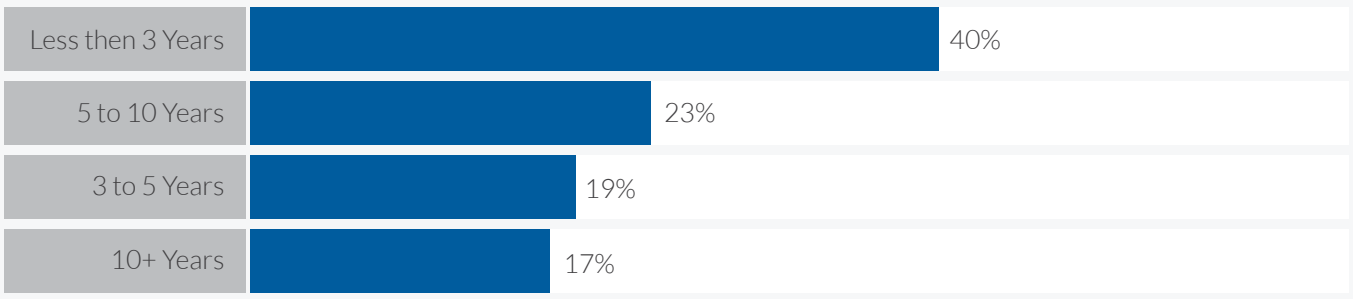


Figure 2 - Survey Respondent Experience

HR and Cyber Leadership Do Not Align on Recruitment Standards

Demand for cybersecurity talent has grown over 2020[1] which is great news for existing, new, and aspiring cybersecurity practitioners. However, according to the survey results, there may be a different problem contributing to the lack of skilled professionals in the workplace. Human Resources do not understand the requirements to work in the cybersecurity team. In fact, **only 33% of respondents felt that HR usually or always understand the requirements to work in a cybersecurity team (See Figure 3)**. Cyber leadership and talent recruiters need to ensure they are closely aligned on the specific requirements to work on the team to attract the right type of talent.

> *Only 33% of respondents felt that HR usually or always understand the requirements to work in a cybersecurity team.*

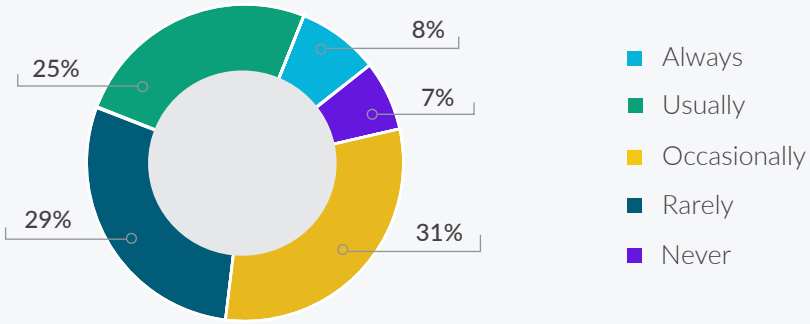
Given the lack of talent available on the market this is a major concern, especially when **65% of respondents felt that, at most, 50% of applicants are qualified for the positions for which they applied (See Figure 4)**. While this could be attributed to the gap between information security leadership and HR, it is more likely a result of a combination of factors. The skills gap may cause underqualified applicants to apply; it is imperative that candidate screening processes filter these underqualified applicants. Furthermore, applicant screening processes are not adequate and **70% of respondents are screening their candidates by means of conversation (See Figure 5) only**. This means that organizations are not reliably evaluating information security candidates' hands-on skills, as well as soft skills, during job interviews. The risk is that these underqualified candidates will complete the hiring process based on successful interviews, and the gaps will only be revealed during an incident.

To summarize:

- Information security leadership and HR need to better align on candidate qualification requirements.
- Job applicants are underqualified and lack hands-on skills.
- Applicant screening is ineffective, mainly relying on a conversation, and does not evaluate candidates in real-world scenarios to assess hands-on skills, technical skills, and soft skills.

1. https://www.scmagazine.com/home/research/cyber-skills-gap-shrinks-but-lack-of-talent-remains-major-risk-factor/

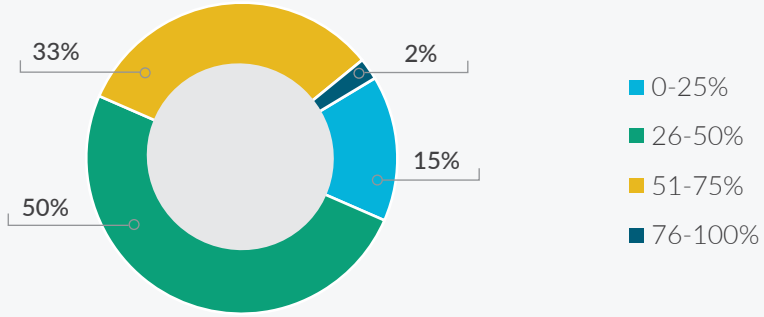
How often do you feel your HR department fully understands the requirements to work in a cybersecurity team?



Only 33% of respondents felt that HR usually or always understand the requirements to work in a cybersecurity team.

Figure 3 - HR Understanding of Cyber Team Requirements

How many cybersecurity applicants are qualified for the position for which they are applying?



65% of respondents felt that at most 50% of applicants are qualified for the positions for which they applied.

Figure 4 - Qualified Cybersecurity Applicants

How do you currently screen your cybersecurity candidates?

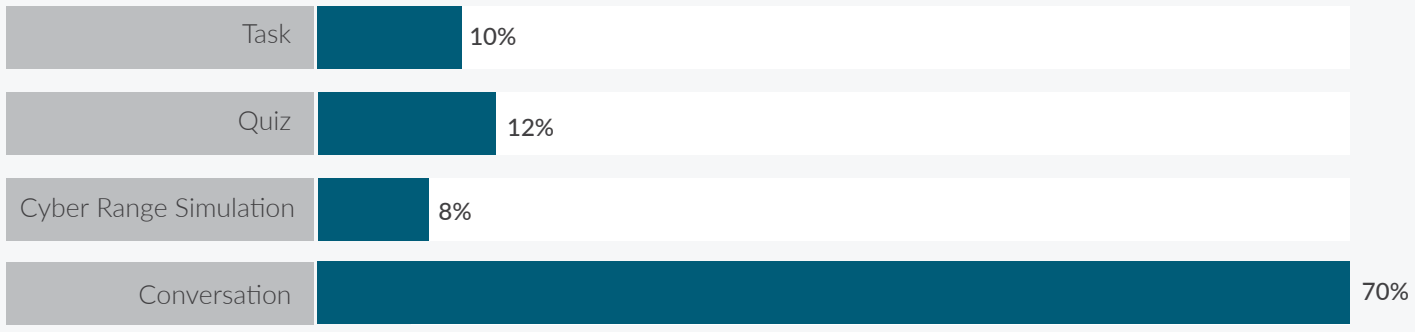


Figure 5 - Current Cybersecurity Screening Mechanisms

Cyber Pros Are Not Confident They Are Prepared to Detect Incident

Cybersecurity professionals need to be prepared to detect, investigate, and mitigate incidents. To accomplish this, cybersecurity professionals must be prepared with a variety of skills to excel in their role. **According to the survey results, respondents feel they are most prepared when it comes to Technical Defensive Cyber Skills (54%). However, respondents are least prepared (See Figure 6) for Intrusion Detection (45% and Network Monitoring (42%).** These skills are the most necessary when it comes to detecting an attack. According to IBM, the average time it takes to detect a malicious actor is 207 days (6.8 months), providing the attacker with more than enough time to accomplish their objectives before the SOC team begins the process of removing them from the network (additional 73 days)

> *Respondents are least prepared for Intrusion Detection (45%) and Network Monitoring (42%)*

How would you describe the skill level of your SOC or Incident Response team?

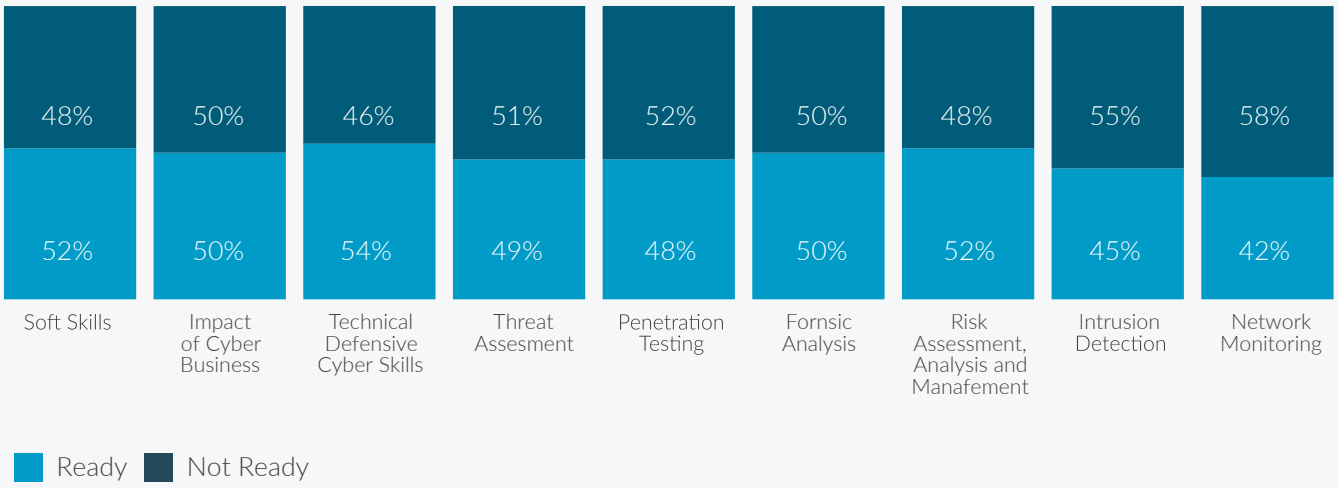


Figure 6 - Level of Preparedness for Cybersecurity Skills

As per Figure 6, few respondents are very confident in their team preparedness levels. Across the board, respondents were evenly split in their level of preparedness, excluding the categories listed above. Reducing time to detection is a key element in lowering cybercrime costs for organizations, especially as respondents were more confidents in their Technical Defensive Cyber Skills.

Despite Availability of Advanced Training Methods, Most Organizations Still Train on the Job

Many organizations believe they can train their employees on the job, forgoing more advanced and effective training methodologies. In fact, most organizations rely on "on-the-job" training or go to courses **(See Figure 7)**. Unfortunately, on-the-job training is a distraction for other teammates, leading to a decrease in production from employees involved in on-the-job training, as well as carrying higher training costs due to the slowdown. Many of the courses are theoretical in nature which would not develop the skills required. More hands-on training like cyber labs, cyber range, and red vs. blue training bring up the tail end of the training spectrum, making up only 22% of adopted training when combined.

What form of cybersecurity training do your currently receive/use?

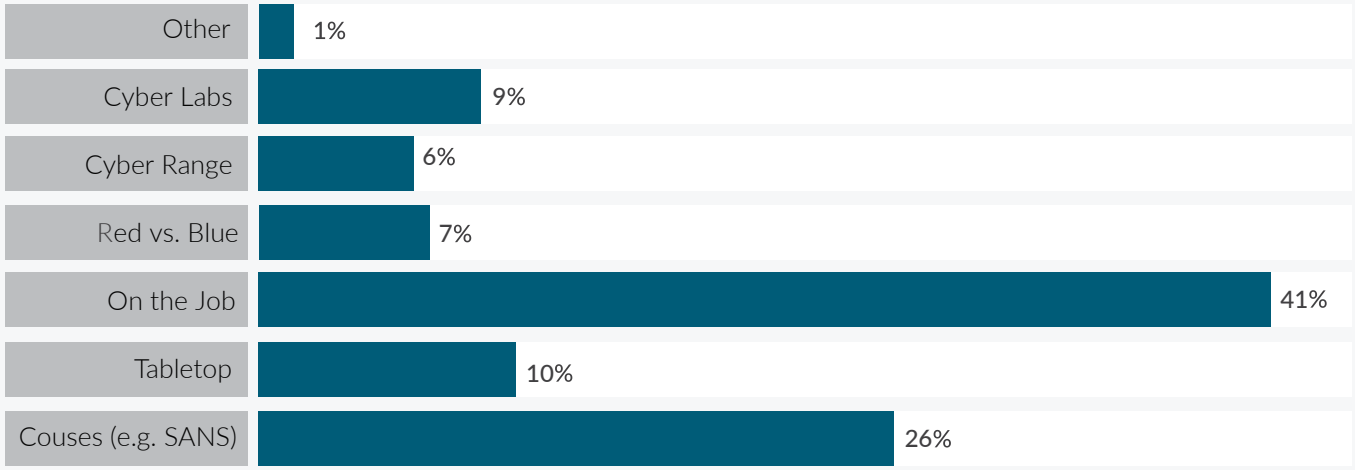
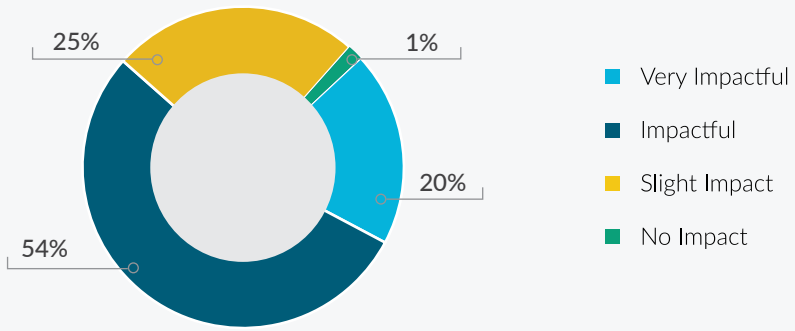


Figure 7 - Current Training Mechanisms

Effective training is key to upgrading the human element of a SOC. Without it, cybersecurity professionals will not be prepared for continually evolving attacker behaviors and attack vectors. When asked about the effectiveness of their current training methodologies, only 20% of respondents felt that current training is very impactful on their job performance **(See Figure 8)**. Following exposure to hands-on training on a cyber range, 89% of respondents felt that hands-on training was a more effective training model when compared with their traditional cybersecurity training **(See Figure 9)**. Additionally, when respondents were asked if they would recommend immersive training for their organization, 92% responded in the affirmative **(See Figure 10).**

> *Most organizations rely on "on-the-job" training or go to courses with no or little hands on components involved*

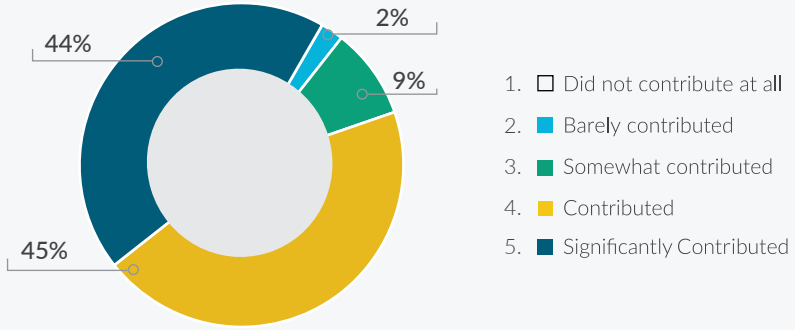
What level of impact do you feel the current training you receive at work has on your ability to perform on your job?



74% of feel that their current training is impactful, while they remain unaware of other, more advanced forms of training

Figure 8 - Level of Impact of Current Training

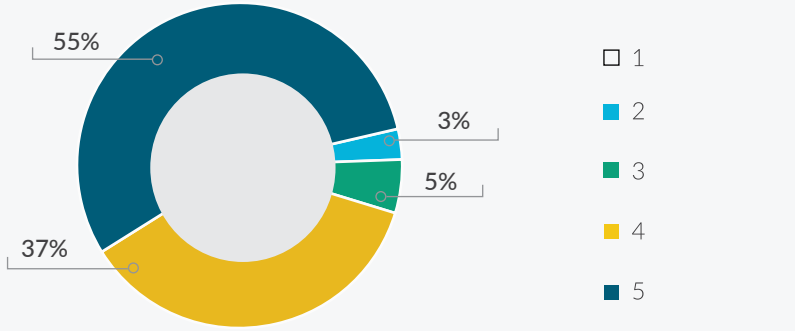
How much did immersive training contribute to your ability to learn when compared with traditional learning/training models?



89% of respondents felt that immersive training was a more effective training model when compared with traditional cybersecurity training.

Figure 9- Level of Impact of Immersive Training

On a scale from 1-5, how likely are you to recommend immersive training for your organization?



92% of respondents recommend immersive training for their organization.

Figure 10 - Immersive Training Recommendation

Conclusion: Organizations Must Act on Recruiting, Workforce, and Training Challenges

The cybersecurity workforce shortage is not a new problem, nor is it going away anytime soon. Organizations have difficulty locating individuals with the desired experience and talent required to excel in the cybersecurity team, but recruiting practices are not helping them to identify the right talent. Focusing job descriptions and evaluation criteria will vastly improve the level of talent and reduce the number of mis-hires in an organization. Most organizations have experienced a bad hire which can prove costly, especially in cybersecurity. The cybersecurity seller's job market is not going to disappear anytime soon, but with budgets leveling out, the cost of a mis-hire will increase, so ensuring you get the right talent the first time will have a massive impact on the effectiveness and success of your cyber team.

The current cybersecurity workforce does not feel overly prepared to deal with a cyberattack. Attack detection, the most time sensitive element, is where they feel the least prepared. Investing in training to improve the overall level of preparedness, with a focus on attack detection would be suitable for every organization. Invest in familiar, motivated, and realistic individuals with effective training practices to ensure retention of employees who can help to satisfy the recognized skills gaps in your organization. These effective training practices means moving away from on-the-job training and into immersive training practices in labs and cyber range environments to develop skills and experience in a safe environment. Encourage employees to go out and test different immersive training platforms and return to you with conclusions so that you can quickly make a decision and implement new training practices to drive your organizations cybersecurity posture forward.

ABOUT CYBERBIT™

Cyberbit is a market-leading provider of cyber skill development platforms. Cyberbit addresses one of the most acute cybersecurity challenges: preparing cybersecurity teams for attacks. The Cyberbit platform delivers a "Zero to Hero" skilling, training, and assessment solution on-demand dramatically increasing security team performance, improving teamwork, and improving evaluation, hiring, and certification processes. Customers include leading Fortune 500 companies, MSSPs, system integrators, academies and governments in 5 continents. Cyberbit is headquartered in Israel with offices in the US, Europe, and Asia. For more information visit www.cyberbit.com

Disclaimer

Cyberbit has designed and created the 2020 Cyberbit SOC Skills Survey as an educational resource for professionals. Cyberbit makes no claim that use of any of the included work will guarantee a successful outcome. The Work should not be considered inclusive of all proper information, procedures and tests or exclusive of other information, procedures and tests that are reasonably directed to obtaining the same results. In determining the propriety of any specific information, procedure or test, professionals should apply their own professional judgement to the specific circumstances presented by the particular systems or information technology environment.

sales@cyberbit.com | www.cyberbit.com

CYBERBIT
TRAIN FOR REAL