cyberbit

Cyberbit’s Rapid Readiness Program

A Case Study in Ramping Up a Large-Scale Incident Response Team

Overview

The Customer described in this case study is a leading Fortune 500 global professional services company and one of the leading providers of managed security operations center (SOC) services. As such, the company employs one of the largest managed SOC teams in the world.

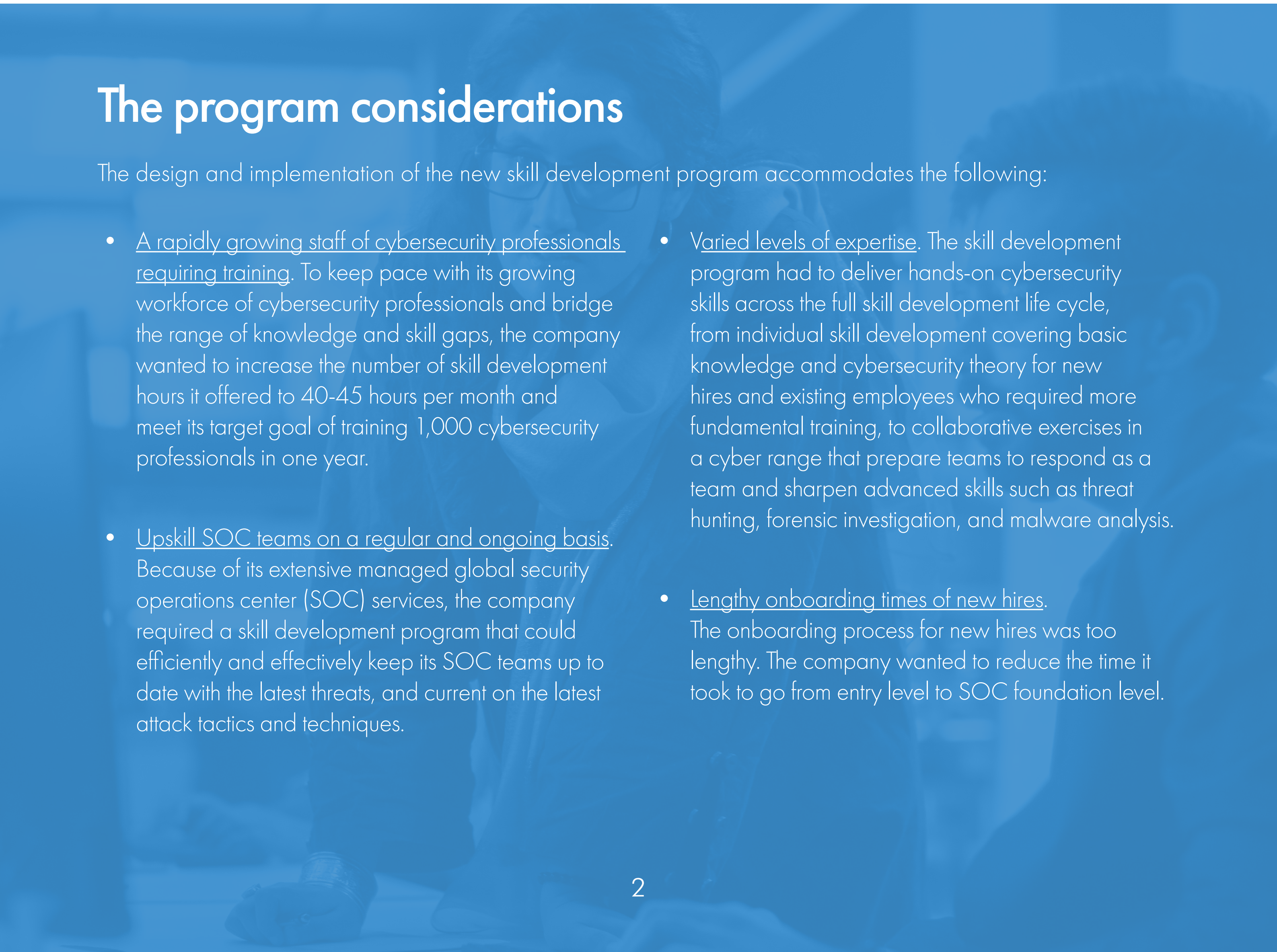
To meet the skill development needs of its rapidly expanding managed SOC team, the company chose Cyberbit’s Rapid Readiness Program. A skill acceleration program, which combines a market leading, scalable, online skill development platform, and a managed service run by an experienced cybersecurity training team.

Cyberbit’s skill development platform provides a comprehensive skill development experience starting with foundational skills in hands-on cyber labs for individuals and concluding with live-fire cyber-attack exercises for teams, on a cyber range. The cyber range includes real-world security tools, real-world networks, and real-world cyber-attack scenarios, providing a hyper-realistic experience that replicates real-world scenarios.
Combined with Cyberbit’s program management team, the organization was able to significantly upgrade the performance and readiness of a large-scale team in minimal time.

The Objective: Significantly Scale up the Skill Development Program for Its Growing Managed SOC Team

As its managed SOC team grew, the customer realized that it must transform its approach to skill development and build a new program that would ensure the team reaches peak performance in minimal time and maintains it continuously. They were interested in creating an elite incident response team that meets the demands of its MSSP customers. The new program was required to accommodate an incident response workforce of over 1000, with more granular training levels beyond the traditional Tier 1, 2, and 3 hierarchy. To do this, the company decided to refresh its entire cybersecurity skill development program:

- Offer five different levels of courses, aligned with its new Managed SOC service structure.
- Aggressively increase the number of cybersecurity employees trained each year to accommodate the growing workforce.
- Encourage ongoing cybersecurity skill development by making 40-45 hours of cybersecurity training per month easily accessible and available on demand to its managed SOC teams.
- Measure individual and team performance and progress.
- Ensure its managed incident response teams are up to date with the latest threat vectors, attacker tactics and techniques, and equipped with the latest cyber defense skills and knowledge.



The program considerations

The design and implementation of the new skill development program accommodates the following:

- A rapidly growing staff of cybersecurity professionals requiring training. To keep pace with its growing workforce of cybersecurity professionals and bridge the range of knowledge and skill gaps, the company wanted to increase the number of skill development hours it offered to 40-45 hours per month and meet its target goal of training 1,000 cybersecurity professionals in one year.

- Upskill SOC teams on a regular and ongoing basis. Because of its extensive managed global security operations center (SOC) services, the company required a skill development program that could efficiently and effectively keep its SOC teams up to date with the latest threats, and current on the latest attack tactics and techniques.

- Varied levels of expertise. The skill development program had to deliver hands-on cybersecurity skills across the full skill development life cycle, from individual skill development covering basic knowledge and cybersecurity theory for new hires and existing employees who required more fundamental training, to collaborative exercises in a cyber range that prepare teams to respond as a team and sharpen advanced skills such as threat hunting, forensic investigation, and malware analysis.

- Lengthy onboarding times of new hires. The onboarding process for new hires was too lengthy. The company wanted to reduce the time it took to go from entry level to SOC foundation level.

The Solution: Build a Full Spectrum Cyber Skill Development Program

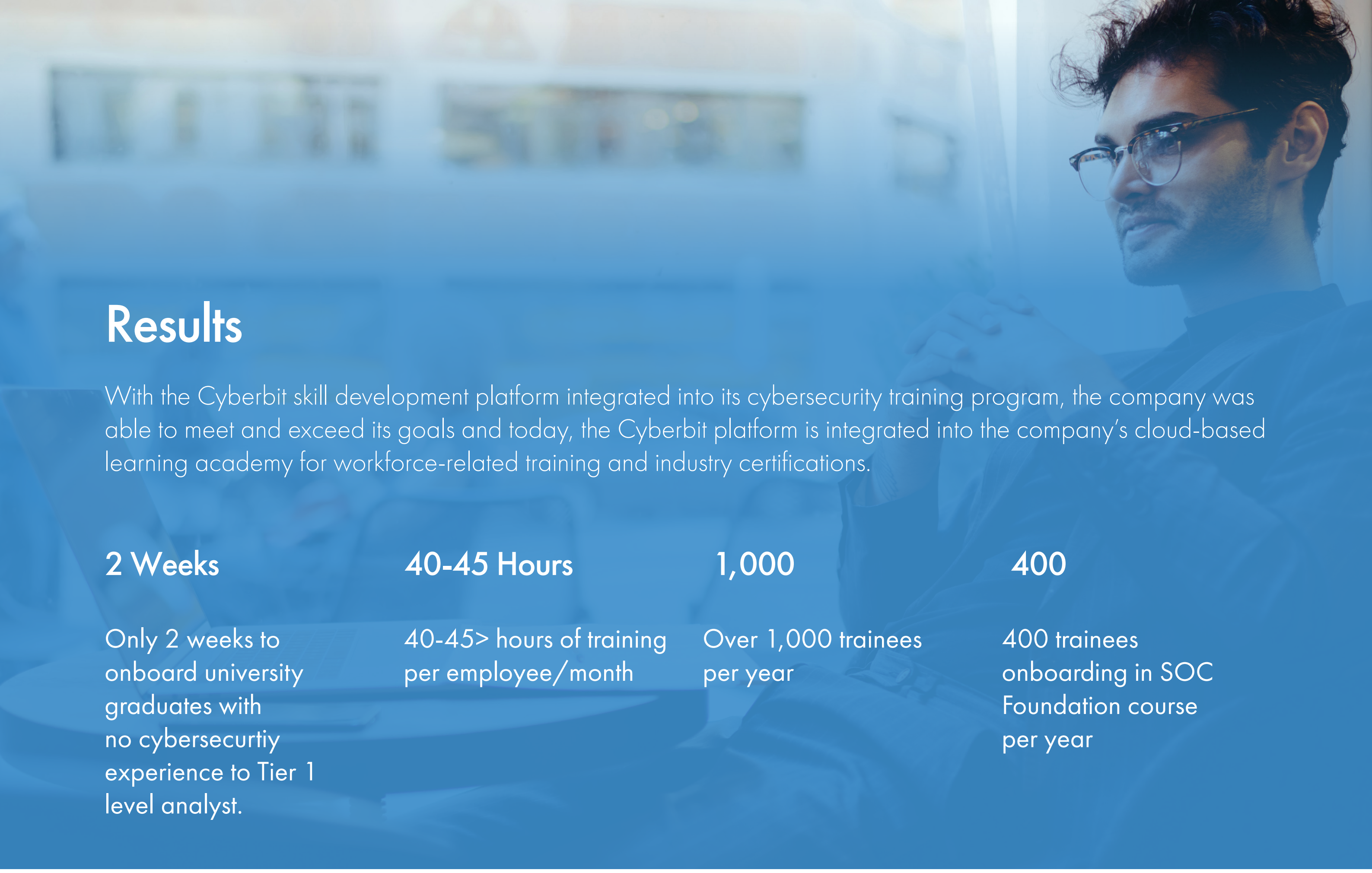
To overcome these challenges, the company looked for a full-spectrum cybersecurity skill development solution that would provide foundational knowledge in theory, security tools, and attacker tactics and allow its new and existing cybersecurity employees to practice in hyper-realistic environments with live-fire attack simulations. The solution had to accommodate the scale, diverse experience levels, onboarding, and upskilling needs of an organization with a cybersecurity staff numbering over one thousand.

The company chose Cyberbit's cloud-based, on-demand cyber skill development and readiness platform, joining numerous other organizations, such as FS-ISAC, Orange, Leidos, Deloitte, Sirius, and many others, that wanted a scalable, advanced, and affordable approach to training cybersecurity teams.
With the assistance of Cyberbit's Customer Success Team, experts in developing and building large- scale cybersecurity skill development programs, the company's cybersecurity skill development program was redesigned to ensure that its new targets were met. This included creating courses customized to accommodate varying levels of experience, specific IR team roles, scalability, and a more effective and rapid onboarding process.
Cyberbit and the customer leveraged the following Cyberbit platform capabilities to develop a structured skill development program:

- Live-fire exercises (LFEs) for providing hands-on experience in a hyper-realistic environment with simulated cyber-attacks. LFEs allow trainees to develop their skills in a safe and controlled environment, while also gaining experience in responding to real-world threats.
- Hands-on labs in a live, virtual environment for building multiple foundational skills and theoretical knowledge. The hands-on labs give trainees a deep understanding of the concepts and techniques they will need to be effective in their roles.
- Spotlights modules to establish and fortify a strong foundation in cyber theory. Spotlights are Cyberbit video and text-based learning modules that develop a comprehensive understanding of the cyber threat landscape and the tools and techniques used by attackers.
- Assessment labs to evaluate skills and assess performance according to roles, tactics, and techniques. Allow managers to screen and benchmark new hires and determine the course levels appropriate to their experience levels.

With the support of the Cyberbit team, the following courses were defined:

Foundational	Intermediate	Advanced	Expert	Pentester
Role: Training to become Tier-1 Analyst	**Role:** Tier-1 Analyst	**Role:** Tier-2 Analyst	**Role:** Threat Hunters, Forensic Investigators	**Role:** Threat Hunters, Forensic Investigators
Experience Level: Beginner	**Experience Level:** Intermediate	**Experience Level:** Advanced	**Experience Level:** Expert Analysts	**Experience Level:** Expert Analysts
Purpose: Onboard new hires and prepare them for Tier-1 role on a SOC team	**Purpose:** Apply detection and mitigation skills learned in Foundational course in a simulated cyber-attack on	**Purpose:** Apply skills that have been learned so far to mitigate and recover from a live-fire cyber attack in the cyber range	**Purpose:** Develop and strengthen skills required for supporting complex incident response procedures	**Purpose:** Train Employee to perform security assessments via authorized simulated attacks
Acquired Knowledge: Basic knowledge for Tier-1 analysts such as SIEM-based investigation, log analysis and firewalls.	**Acquired Knowledge:** Soft skills such as teamwork, communication, host- based investigation, and how to protect systems against malware	**Acquired Knowledge:** Ability to develop and implement a strategy for responding to a complex cyber incident	**Acquired Knowledge:** Threat hunting, forensic investigation, malware analysis	**Acquired Knowledge:** Threat hunting, forensic investigation, malware analysis



Results

With the Cyberbit skill development platform integrated into its cybersecurity training program, the company was able to meet and exceed its goals and today, the Cyberbit platform is integrated into the company's cloud-based learning academy for workforce-related training and industry certifications.

2 Weeks

Only 2 weeks to onboard university graduates with no cybersecurtiy experience to Tier 1 level analyst.

40-45 Hours

40-45> hours of training per employee/month

1,000

Over 1,000 trainees per year

400

400 trainees onboarding in SOC Foundation course per year

> *"The training was simply superb, and I could take more courses like this. Thank you for the wonderfull learning sessions"*

Participant in the SOC Foundation course

> *"Cyberbit has organized these trainings with all the righr ingrediens: great trainer, content, resources, call flow, Q&As. Awesome. 5 stars!"*

Participant in the SOC Foundation course

> *"It was a great experience - trainer was extremely helpful and skilled"*

Participant in the Intermediate Training course

> *"Helped us expand our cybersecurity workforce capacity so we could better serve our clients"*

Executive Management

SOC Foundation

Employee Profile:
New hires, primarily recent university graduates, with little or no cybersecurity experience.

Course Goal:

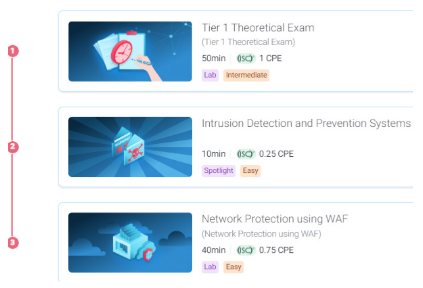
- Onboard and equip cybersecurity employees with foundational knowledge in cyber theory.
- Build the cyber skills they will need to be Tier 1 analysts.
- Prepare them for the next level of training on the cyber range.

Course Description:

- Prior to starting the course, new employees must take an assessment challenge on the Cyberbit cyber range to gauge their fundamental cybersecurity knowledge. Assessments are performed automatically by the Cyberbit platform and allow and in-depth understanding of the employee's knowledge and skill levels.
- Self-paced cyber labs and Spotlights offered over a five-day period.

Course Sample

- Tier1 Theoretical Exam
- Intrusion Detection & Prevention Systems
- Network Protection Using WAF



1 Tier 1 Theoretical Exam
(Tier 1 Theoretical Exam)
50min | (ISC)² 1 CPE
Lab Intermediate

2 Intrusion Detection and Prevention Systems
10min | (ISC)² 0.25 CPE
Spotlight Easy

3 Network Protection using WAF
(Network Protection using WAF)
40min | (ISC)² 0.75 CPE
Lab Easy

SOC Intermediate

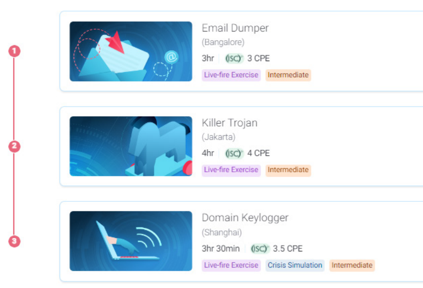
Employee Profile:
Completed the SOC Foundation course or already possesses a level of cybersecurity knowledge similar to what is provided in the course.

Course Goal:
Introduce employees to the Cyberbit cyber range where they will work as a team in a virtual SOC and apply the detection and mitigation skills learned from the SOC Foundation course.

Course Description:
Immerses employees in a hyper-realistic environment with live-fire exercises on the cyber range where they will apply their cybersecurity skills and learn about host-based investigation and how to protect systems against malware.

Course Sample

- Email Dumper
- Killer Trojan
- Domain Keylogger



1 Email Dumper
(Bangalore)
3hr | (ISC)² 3 CPE
Live-fire Exercise Intermediate

2 Killer Trojan
(Jakarta)
4hr | (ISC)² 4 CPE
Live-fire Exercise Intermediate

3 Domain Keylogger
(Shanghai)
3hr 30min | (ISC)² 3.5 CPE
Live-fire Exercise Crisis Simulation Intermediate

SOC Advanced

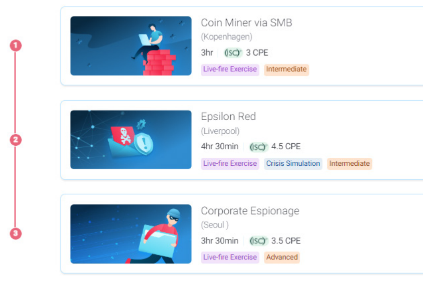
Employee Profile:
Already completed the SOC Intermediate course and exhibits a more advanced understanding of tactics, techniques, and procedures (TTPs) and how to use advanced cybersecurity tools.

Course Goal:
Build upon the skills and knowledge employees learned in the SOC Intermediate course and test whether they can develop a strategy for responding to a cyber incident

Course Description:
Exposes employees to more complex scenarios with advanced cyber-attacks on the cyber range and requires them to effectively mitigate and recover from a simulated cyber-attack in the cyber range.

Course Sample

- Coin Miner via SMB
- Epsilon Red
- Corporate Espionage



1 Coin Miner via SMB
(Kopenhagen)
3hr | (ISC)² 3 CPE
Live-fire Exercise Intermediate

2 Epsilon Red
(Liverpool)
4hr 30min | (ISC)² 4.5 CPE
Live-fire Exercise Crisis Simulation Intermediate

3 Corporate Espionage
(Seoul)
3hr 30min | (ISC)² 3.5 CPE
Live-fire Exercise Advanced

SOC Expert

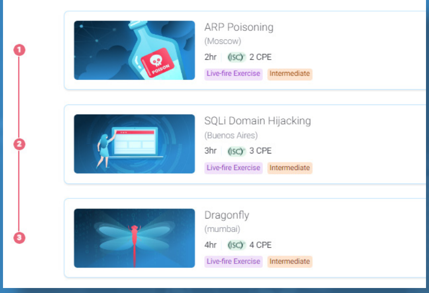
Employee Profile:
Completed the SOC Foundation course or already possesses a level of cybersecurity knowledge similar to what is provided in the course.

Course Goal:
Introduce employees to the Cyberbit cyber range where they will work as a team in a virtual SOC and apply the detection and mitigation skills learned from the SOC Foundation course.

Course Description:
Immerses employees in a hyper-realistic environment with live-fire exercises on the cyber range where they will apply their cybersecurity skills and learn about host-based investigation and how to protect systems against malware.

Course Sample

- ARP Poisoning
- SQLi Domain Hijacking
- Dragonfly



1 ARP Poisoning
(Moscow)
2hr | (ISC) 2 CPE
Live-fire Exercise Intermediate

2 SQLi Domain Hijacking
(Buenos Aires)
3hr | (ISC) 3 CPE
Live-fire Exercise Intermediate

3 Dragonfly
(mumbai)
4hr | (ISC) 4 CPE
Live-fire Exercise Intermediate

Pentester Course

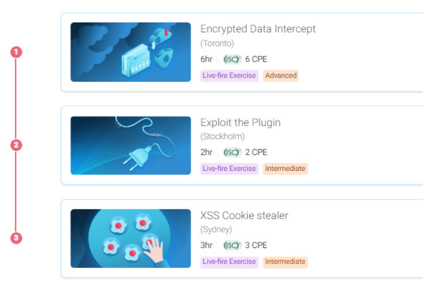
Employee Profile:
Completed the SOC Foundation course or already possesses a level of cybersecurity knowledge similar to what is provided in the course.

Course Goal:
Introduce employees to the Cyberbit cyber range where they will work as a team in a virtual SOC and apply the detection and mitigation skills learned from the SOC Foundation course.

Course Description:
Immerses employees in a hyper-realistic environment with live-fire exercises on the cyber range where they will apply their cybersecurity skills and learn about host-based investigation and how to protect systems against malware.

Course Sample

- Encrypted Data Intercept
- Exploit the Plugin
- XSS Cookie Stealer



1 Encrypted Data Intercept
(Toronto)
6hr | (ISC) 6 CPE
Live-fire Exercise Advanced

2 Exploit the Plugin
(Stockholm)
2hr | (ISC) 2 CPE
Live-fire Exercise Intermediate

3 XSS Cookie stealer
(Sydney)
3hr | (ISC) 3 CPE
Live-fire Exercise Intermediate

Reflection

The main considerations for the customer were scaling their cyber skill development program to meet the needs of its burgeoning cybersecurity workforce for its managed SOC services and accommodating the wide range of experience levels amongst its cybersecurity staff.

Cyberbit was able to overcome these challenges by customizing the skill development program courses to provide full-spectrum skill development from novice to expert. The SOC Foundation course, an intense preparatory course for novices, overcame the dual challenge of upskilling new hires and lengthy onboarding by preparing them for their roles on a SOC team as Tier-1 analysts in only two weeks.

The Intermediate through pentester courses provided the hands-on experience deemed critical to effective incident response teams by 73% of cybersecurity professionals (ISACA, 2022). Learners were immersed in a hyper-realistic environment on the Cyberbit cyber range, which included a virtual SOC, commercial security tools, enterprise grade networks, and live-fire, real-world cyber-attack scenarios.

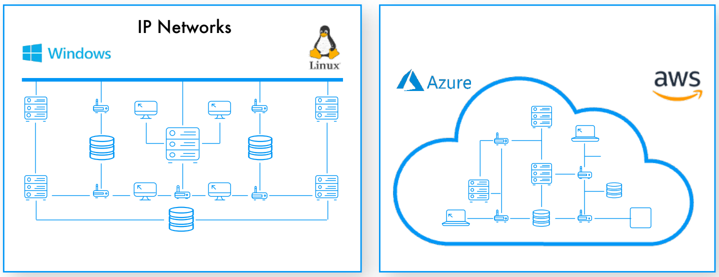
To scale the program, we increased the number of courses and live-fire exercises offered. The company's cybersecurity staff accessed the Cyberbit platform for labs and live-fire exercises twice daily, allowing the company to exceed its goal of upskilling 1000 employees per year.

By meeting its cybersecurity skill development needs, the company has become a leader in managed security operations center services.

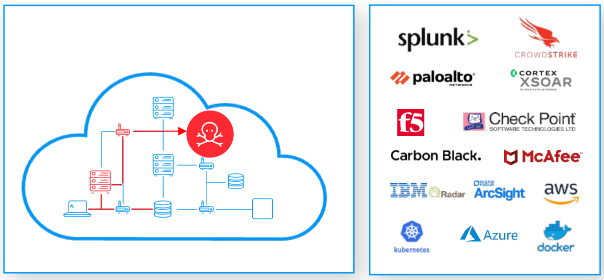
Place Your Team in the Line of Fire

As real as it gets, so you KNOW your team is ready

Prebuilt Enterprise-Grade NetworksDesigned to Maximize Training Impact



Automated Attack GeneratorFully Simulated Kill Chain



Hundreds of courses, labs and live fire exercises from beginner to expert, curated by training experts

Ransomware Log4J Phishing investigation Splunk Log Analysis Dragonfly APTs SOC Analyst Course SSRF Attack
Malware analysis Supply Chain Attack Threat Hunting with Crowdstrike Web defacement TrickBot Azure Attacks
Secure Development Course Data Exfiltration Threat Intelligence Course Coin Mining Attack SSRF Simulation Network Forensics
SQL Injection AWS Attacks Keylogger DNS Hijacking CompTIA SEC+ Course Kubernetes PowerShell investigation Pentesting

About Cyberbit

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

sales@cyberbit.com | www.cyberbit.com