Training and Skill Shortage: The Top Investment Drivers for Cyber Security Leaders

The SANS Institute reports that Cyber security staff training and certification is the #1 investment priority for security leaders, driven by a severe skill shortage which is preventing organizations from responding effectively to incidents. This skill shortage is here to stay, with more than 200,000 vacancies in the US alone, expected to reach 1.5 million unfilled positions by 2019 (Forbes Magazine, Oct 2015). Staff churn is increasing due to the lack of proper training and qualification plans. Security leaders are therefore investing in new and effective approaches for qualifying and training their cyber security staff.

Cyberbit Range

Cyberbit Range is a hyper-realistic simulation platform enabling service providers, governments and consulting firms to set up and manage cyber security training centers. The platform enables cyber security professionals to participate in hands-on training in a real-world environment. The Range also serves as a testbed for assessing security tools and architecture in a safe and controllable environment. As the world’s leading training platform, Cyberbit Range enables both cyber security staff and company executives to practice real-world incident management scenarios and significantly improve their performance when an actual security incident takes place. The Range accelerates qualification, reduces certification time, and produces staff which is more competent and up to date.

Cyberbit Range Benefits to Service Providers and Consultancies

- Create a new revenue stream by setting up a training center and offering cybersecurity training and qualification services
- Design and run your own training program: create training plans tailored to your market and audience, and execute them independently
- Add value to your customers with hands-on security training in a customizable environment, that produces a more competent and updated staff
- Differentiate your offering with unique services like individual and team training, executive training, ICS/SCADA simulation and ransomware training
- Provide testbed services for customers to test tools and perform POCs, assess vulnerabilities and test their security architecture in a safe environment
- Support for multiple classrooms in one Range platform
How Does It Work?

Cyberbit Range simulates networks, traffic and threats over virtual machines, and can feature additional appliances and hardware to accurately represent company networks. The simulated network is injected with traffic, simulating typical activity such as user emails, web-surfing, and server communications. In addition, real-life attack scenarios are injected into the network, using Cyberbit’s predefined attack scenario library as well as custom-built scenarios.

Trainees are scored as they identify, track, investigate, respond and remediate threats and reach predefined session’s goals. The session is recorded and documented on a timeline, to be later replayed and reviewed in a debriefing session. Trainees’ skills and capabilities are evaluated for further reference and training. Every session can be rolled-back and repeated.

Cyberbit Range provides IT and OT network simulation with physical OT hardware, and supports both individual and team training.

Simulated Network

Real-Life Settings

Cyberbit Range is the first hyper-realistic cybersecurity simulation platform. By providing a real-life training experience it enables trainees to prepare for the actual challenges they will face during a real-life attack, and confront them effectively. This is achieved by accurately replicating network settings, realistic traffic and evolving threats as they would appear in a real attack, while using the actual security tools trainees would use at work.

Flexible and Customizable

Cyberbit Range is fully customizable so you can either use predefined settings and scenarios or generate your own custom networks, traffic patterns and attack scenarios. Adding security tools is easy, so trainees can use the tools they use at work. As a result, training center operators can tailor the settings and scenarios for specific customers and provide more effective and valuable training.

Fully Automated

Training sessions and simulation scenarios are carried out automatically, with auto-injection of benign traffic and threat scenarios – eliminating the need for conventional “red team” attackers. This allows for full independence in conducting courses and testbed scenarios, while ensuring consistent training which is independent of the expertise of human attackers.
Cyberbit Range Main Capabilities

**Realistic Traffic Generator**
Cyberbit Range generates realistic traffic and injects it into the simulated networks, these replicate user activities and normal network communications. Traffic can be customized before or throughout the session, using various communication protocols and channels including http, https, ftp, smtp, pop3, SCADA and more.

**Complex Attack Simulation**
The attack generator makes it easy to create any attack scenario, based on a toolset that includes hundreds of building blocks. Attacks can be carried out from any network location and can target any network component. Training center operators are provided with extensive tools to create new scenarios independently, or to customize the library of predefined attack scenarios that are provided by default.

**IT and OT Simulation**
Cyberbit provides both IT and OT network training and simulation, with physical OT hardware that integrates with the simulated IT and SCADA environment, and with out-of-the-box networks, scenarios and threat vectors including attacks that start at the IT network and move to attack the OT network, typical of recent high-profile breaches.

**Advanced Training Tools**
Cyberbit Range provides real-time view and monitoring of the whole training session in an instructor’s station, allowing instructors to write remarks, take control of trainees’ workstations, track goals and score performance. Every action is marked on a timeline and in an audit log. Sessions are recorded and can be played back and debriefed with the trainee for optimal feedback. Advanced evaluation tools allow instructors review to assess trainee and group performance on an ongoing basis.

**Controllable Testing Environment**
Cyberbit Range simulation platform can be used as a testbed for evaluating network security architecture, vulnerability assessment, tools testing and POCs in a custom environment simulating the customer’s real network, with realistic traffic and complex attack simulation.
ABOUT CYBERBIT™

CYBERBIT provides advanced cyber security solutions for high-risk, high-value enterprises, critical infrastructure, military and government organizations. The company’s portfolio provides a complete product suite for detecting and mitigating attacks in the new, advanced threat landscape, and helps organizations address the related operational challenges. Cyberbit’s portfolio includes advanced endpoint detection and response (EDR), SCADA network security and continuity, security incident response platform, and security team training and simulation. Cyberbit’s products were chosen by highly targeted industrial organizations around the world to protect their networks.

CYBERBIT is a wholly-owned subsidiary of Elbit Systems Ltd. (NASDAQ and TASE: ESLT)

sales@cyberbit.net | www.cyberbit.net

US Office:
CYBERBIT Inc.
3800 N. Lamar Blvd. Suite 200
Austin, TX 78756
Tel: 1-737-717-0385

Israel Office:
CYBERBIT Commercial Solutions Ltd.
22 Zarhin St. Ra’anana
Israel 4310602
Tel: +972-9-7799800

PROPRIETARY INFORMATION
The information here in is proprietary and includes trade secrets of CYBERBIT Commercial Solutions Ltd. It shall not be utilized other than for the purpose for which it has been provided.