Background

In recent years, the cyber security industry in Singapore has experienced rapid growth, leading to a substantial shortage of skilled cybersecurity experts. As a result, security operations staff had no option other than on-the-job training to enhance their skills in handling more complex security incidents.

As the local cyber security industry lacked an authorized entity that could train, certify, and produce skilled cybersecurity professionals, ST Electronics decided to provide hands-on operational cybersecurity training and generate a consistent flow of high-quality, certified cyber security professionals.

ST Electronics chose Cyberbit’s cyber range because of its cyber training and simulation capabilities and experience. This was of particular advantage to DCSC, as it aimed to redesign trainings that are suited for Singapore’s organisations.

The Challenges

When DCSC was first established, the only way for local cyber security professionals to train for their job was by means of theoretical courses as they did not have any option for a hands-on, "real world" training experience using a simulated environment. ST Electronics wanted to create a training facility that combined theory with true-to-life attack simulation. Along with insightful feedback, this would arm cyber security professionals with the knowledge and skills required to combat the security incidents they would experience in the field.

This presented five main logistical challenges:

1. **Realistic simulation:** Providing the right tools and infrastructure to build an entire real life replica of the trainee’s enterprise network, which could accurately simulate threats, traffic and network infrastructure.

2. **Network versatility:** As trainees would come from a diverse range of organizations, the platform had to be highly versatile and customizable to simulate a variety of network configurations and topologies, and support a wide range of security products. This would allow every organization to train with the security tools they actually used at work, within a familiar network setup.

3. **Threat diversity:** ST Electronics knew that one of the main challenges of its customers was the diversity of threats. Confronting an unknown attack type for the first time will often result in a breach, while an attack which you have been trained for will often be mitigated successfully. One of the requirements for the DigiSAFE platform was to simulate different types of attack scenarios and accommodate the individual threat priorities of each organization, including complex, evolving incidents, typical to present-day targeted attacks.

4. **Adaptable curriculum:** ST Electronics intended to offer a range of training courses that could be tailored to the needs of various organizations, security roles and attack scenarios. In addition, it wanted to customize those courses to support all stages and levels of the incident response cycle: protection, detection, response and recover.

5. **Training tools, analysis and feedback:** For an effective training experience, ST Electronics wanted to ensure that beyond the simulation itself, the training facility would include comprehensive tools to provide real-time feedback to trainees and trainers, and would enable them to track progress across the training courses.
Cyberbit Range was able to address these challenges in a single integrated solution, giving DCSC the versatility they wanted without compromising on the ultimate goal of highly realistic threat simulation.

Using Cyberbit’s Range platform, ST Electronics successfully realized its goal of building a versatile cybersecurity simulation and training system, marked by the opening of its training facility in 2014. All courses are customized to the specific requirements of the trainees, and yet, each one is based on the following four cornerstone capabilities:

**Accurate Network Simulation**
Cyberbit’s Range utilizes live network and traffic simulation to train DCSC trainees in real-world environment simulating a real enterprise network. The training platform supports a wide range of enterprise security tools including firewalls, IPS, IDS and SIEM products. This enables trainees to practice based on the specific products and tools they use in their day-to-day work, including ICS/SCADA networks and controllers for OT security staff training.

**Real-Life Threat Scenarios**
DCSC trainings are able to simulate a wide range of attack scenarios using Cyberbit’s cyber range threat generator. Scenarios include Trojan, Malware, DDoS, Phishing and more. The simulation also includes normal traffic and white noise to simulate real life environment. This enables DCSC to provide consistent quality training across all courses offered.

**Interactive Learning and Actionable Feedback**
The system equips the instructor with visibility of the cyber attack events and also its desired performance matrix. This provides the trainer a comprehensive ability to track and manage the trainees’ activities with time-stamped notes and events. The trainer is able to interact effectively with the trainees to train them in the cyber exercises and also revert to the recording for effective debrief.

The DigiSAFE Cyber Security Center, Powered by Cyberbit Range
Results: Immediate Impact on Trainees

In an anonymous survey issued by ST Electronics, 85% of trainees who attended the course said they were better prepared to confront attacks and take appropriate defensive action. They also stressed how DCSC gave them the hands-on experience they did not get to experience at work.

“I learned a great deal from the more direct experiences of a cyber attack, the way the team communicated and how everyone reacted when the servers were down. The course also taught me not to overlook any minor alerts that could help lead to the real intention of the attacker, and it helped me to become better prepared for an actual event happening in the future.”

Sample response from survey

The survey revealed that trainees experienced new attack scenarios that they had not encountered before, and the training had helped them to work better as a team during a cyber attack.

A Secure Future

Since the launch of DCSC in 2014, ST Electronics has leveraged the Cyberbit Range platform to accelerate the educational development of security professionals in Singapore. It brings hundreds of new entrant cyber defenders to the market.

In March 2016, DCSC achieved the Approved Training Organization (ATO) accredited by the government’s Workforce Development Agency. This status qualifies DCSC to conduct courses and assessments that are mapped to the National Infocomm Competency Framework. It recognizes its quality and depth of the cyber training offerings.

“The versatility of Cyberbit’s Range platform empowers ST Electronics to address a wide range of organizations, by customizing the training environments and attack scenarios to meet the organizations’ specific needs. With the Range platform ST Electronics can provide an effective, high-fidelity simulation that bridges the cyber security operations skills gap in the marketplace by providing individuals hands-on cyber training preparing them to be operationally ready - faster.”

Mr Victor Yeo | Deputy General Manager, ST Electronics (Info-Security)

To learn more about ST Electronics, visit www.stee.stengg.com
To learn more about ST Electronics (Info-Security), visit www.digisafe.com

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)