A LEADER IN CYBERSECURITY EDUCATION

Cybersecurity

WE RETURN CYBER READY PROFESSIONALS BACK TO YOU
ABOUT STECA

Vision

To be a Leader in Cybersecurity Education

Mission

To provide cybersecurity professionals a conducive environment to enhance their skills through the practical application of knowledge

ST Engineering Cybersecurity Academy (STECA) prepares talents and enterprises for the challenges in the digital world via the delivery of competency based training, integrated with the state-of-the-art simulated Cyber Warfare Range exercises.

Meeting Today’s Cybersecurity Challenge

The main challenge confronting most companies today is the lack of cybersecurity skillsets. Most cybersecurity professionals are not operationally ready when put to task force.

In addition, there are also insufficient training platforms and courses to level up the competencies in the field of cybersecurity. Even for those available courses, they are mainly theoretically based. Thus most of the aspiring cybersecurity professionals cannot level up their operational competencies and experiences.

STECA’s deep domain expertise and operational experience allows us to impart realistic cybersecurity training to the trainees. Using real life use cases to correlate with key concepts of cybersecurity, trainees are able to comprehend effectively.

Besides identifying training to beef up their technical skillsets, STECA’s intent is to prepare trainees in the shortest time possible to keep up with the shortage of cybersecurity talent pool in the industry.
Established in 2014, STECA was first in Singapore to introduce Cyber Warfare Exercises as part of their training programmes. STECA, being part of the ST Electronics (Info-security) family, taps on ST Engineering’s deep, indigenous expertise to ensure that the training programmes are recent and relevant.

STECA is dedicated to groom cybersecurity professionals by providing individuals and enterprises an opportunity to test their IT and OT infrastructures. Besides that, it also allows them to stress test their competency in handling cyber breaches in a safe and controlled environment.

STECA has trained over 1,500 professionals beyond the Engineering industry from more than 100 organisations to date. STECA is an accredited public Approved Training Organisation (ATO) by SkillsFuture Singapore (SSG) and is also an exclusive partner of (ISC)².

ST Engineering is the first and only official training provider for Systems Security Certified Practitioner (SSCP) course in Singapore. Being actively partnering with government agencies and industry players, STECA offers holistic innovative training programmes worldwide.

### Core Capabilities

- **Deliver industry recognised training programmes**
- **Design and offer hands-on experience on simulated cyber warfare range**
- **Customise training programmes to cater to company’s specific needs**

### Milestones

**2014**
Established and first in Singapore to offer Cyber Warfare Range exercises.

**2015**
Introduced specialised Cybersecurity Operations courses across Asia.

**2016**
First in the world to infuse cyber warfare range into the System Security Certified Practitioner (ISC)² course.

**2017**
Launched Cybersecurity Leadership Programme.

**2018**
Rebranded as ST Engineering Cybersecurity Academy (STECA) and increased training capacity to 50. Introduced Cybersecurity SCADA courses.
STECA’s training methodology caters to both posture building and maturity improvements across cyber defence skills.

At STECA, learners are guided and trained by qualified industry practitioners with case studies that gives them the opportunity to apply relevant cybersecurity theories, concepts, methods and principles. Learners will be exposed to realistic cyber attacks of varying complexities in a simulated environment using the latest technology in cyber warfare tools.

At STECA, learners are guided and trained by qualified industry practitioners with case studies that gives them the opportunity to apply relevant cybersecurity theories, concepts, methods and principles. Learners will be exposed to realistic cyber attacks of varying complexities in a simulated environment using the latest technology in cyber warfare tools.

Armed with posture building knowledge, learners will then be tasked to apply their newly acquired knowledge to improve their maturity in managing a real cyber attack. Thereafter, an after action review will be conducted by the trainer to ensure the retention of learning and knowledge.

Learners will be exposed to realistic cyber attacks of varying complexities in a simulated environment using the latest technology in cyber warfare tools.
Overview of courses

Most of the courses offered by STECA are mapped to the Skills Framework (SFw) for Infocomm Technology (ICT). The SFw for ICT was jointly developed by SkillsFuture Singapore (SSG), Workforce Singapore (WSG), and the Info-communications Media Development Authority (IMDA), together with industry associations, education institutions, training providers, organisations and unions.

STECA offers training programmes that broaden and deepen skills in the ICT sector, specially catered for individuals and companies ranging from Foundation to Vitality stages. The aim is to match the intended competency levels of individuals of teams as their role requires.
CYBER WARFARE EXERCISE

Course Overview:
Cyber Warfare Exercises equip the learners with the necessary skills and knowledge to build cyber breach response expertise in the area of Security Operations Centre (SOC), Network Operations Centre (NOC), Cyber Incident Response Team (CIRT) and Forensic Practitioners.

Upon completion of these exercises, learners will be able to apply their technical skills, decision making skills and adopt cross-team communication skills to manage a cyber breach in their organisations.

Course / Entry requirements
1. At least one year of cybersecurity working experience
2. Fundamental knowledge of cybersecurity

Course Objectives
1. Ensure the retention of cyber response skills against cyber attacks of varying complexities
2. Analyse and discover gaps in response processes & technical competencies through time-critical cyber attack scenarios

Target Audience
1. IT and / or Cyber professionals tasked with cyber defence of their organisations
2. Cyber professionals who are keen to improve their skills on specific roles of cyber defence

Certification Obtained
• Certificate of Completion by ST Engineering Cybersecurity Academy (STECA)

Course Training Duration
This will depend on the number of scenarios required by companies. A minimum 1 day with 2 scenarios.

Course Fees
From S$2,000 (excluding GST) per learner

Mode of Training
Practical Hands on exercises
The Cybersecurity by Design (CSBD) course equips learners with the knowledge and skills to implement cybersecurity measures within an enterprise infrastructure and system design.

Upon completion of this course, learners will have the ability to design systems with security in mind to ensure reliability in the system while mitigating potential threats and risks.

"Good knowledge to learn the reality of Cybersecurity foundation. Good appreciation of Cybersecurity challenges." - Manager, ST Engineering Electronics

Course Overview:

1. At least one year of IT working experience
2. Basic Understanding of the Computers and the Internet

Course Objectives

1. Understand about the cybersecurity threat landscape
2. Understand the needs of cybersecurity architecture and apply the cybersecurity design principles for infrastructure and system design
3. Identify the cybersecurity goals of a system to the organisation

Certification Obtained

- Certificate of Completion by Nanyang Polytechnic and ST Engineering Cybersecurity Academy (STECA)
Course Overview:
The Cybersecurity Forensics Investigator (CSFI) course equips learners with a better understanding of cyber forensics and investigation skillsets using computer based operating systems such as Windows and Linux. Learners will also have hands-on experience in conducting of forensics investigation on simulated real-world cyber incidents in an emulated enterprise network environment.

Upon completion of this course, learners will be able to conduct basic forensics investigation that includes acquisition of forensics evidences, analysis of the gathered evidences, and presentation of the findings.

Course Ref Number
CRS-Q-0032196-ICT (https://www.skillsconnect.gov.sg)

Course Training Duration
4 days (30 hrs)

Course Fees
S$3,000 (excluding GST)
Please refer to the table for funding details.

Funding Validity Period
01 May 2018 to 30 Apr 2020

Mode of Training
Classroom (Cyber Range)
<table>
<thead>
<tr>
<th>Cybersecurity Forensics Investigator</th>
<th>International Participants</th>
<th>S’poreans / PRs (aged 21 and above) 50% of course fee up to $15 per hour</th>
<th>Skillsfuture Mid-Career Enhanced Subsidy (S’poreans aged 40 and above) 90% of course fee up to $50 per hour</th>
<th>Workfare Training Support (S’poreans aged 35 and above, and earn &lt;$2000 per month) 95% of course fee</th>
</tr>
</thead>
<tbody>
<tr>
<td>Full course fee (excl GST)</td>
<td>3000</td>
<td>3000</td>
<td>3000</td>
<td>3000</td>
</tr>
<tr>
<td>7% GST on nett course fee</td>
<td>210</td>
<td>210</td>
<td>210</td>
<td>336</td>
</tr>
<tr>
<td>Course fee (incl GST)</td>
<td>3210</td>
<td>3210</td>
<td>3210</td>
<td>3210</td>
</tr>
<tr>
<td>Less additional funding if eligible under various schemes</td>
<td>NA</td>
<td>450</td>
<td>1500</td>
<td>2850</td>
</tr>
<tr>
<td>Total nett course fee payable, including GST, after additional funding from the various funding schemes</td>
<td>3210</td>
<td>2760</td>
<td>1710</td>
<td>360</td>
</tr>
</tbody>
</table>

Course / Entry requirements
1. At least one year of cybersecurity working experience
2. Fundamental knowledge of cybersecurity

Course Objectives
1. Understand in depth about various forensic tools and its utilisation during actual situations
2. Develop practical skillsets in forensic investigation
3. Apply relevant protective measures when future cyber incidents occur

Target Audience
IT professionals who are tasked to investigate cyber breaches in a forensically sound manner

Certification Obtained
- Certificate of Competency by ST Engineering Cybersecurity Academy (STECA)
- Statement of Attainment by Skills Future Singapore (SSG)

Appeal and Reassessment
The Statement of Attainments (SOAs) will not be issued to trainees who have been assessed as Not Yet Competent (NYC). Trainees who wish to be certified as Competent will have to undergo training and assessment for the entire module again. Where there are reasons to appeal against the Assessor’s decision, an appeal may be submitted in writing to ST Engineering Cybersecurity Academy (STECA) within 5 working days from the date of assessment stating clearly the ground(s) for Appeal. If the appeal is successful, a new round of assessment will be conducted at a fee of $150. If the appeal is unsuccessful, the trainee will have to undergo training and assessment again.
Course Overview:
The Cybersecurity Operations Specialist (CSOS) course equips learners with the essential knowledge and skills to keep an organisation secure. In addition to the imparting of knowledge, it focuses on the cognitive and analytical abilities of learners. It also equips learners with cyber defence operational skillsets.

Upon completion of this course, learners will be able to detect, contain, eradicate and report a successful cyber breach. Learners will also learn about cybersecurity concepts and be familiarised with the functionality of various security products.

"Trainer is good and is able to relate some of the lessons to our job."
- S3, MINDEF

"Trainer is very knowledgeable, able to clarify our doubts and share experiences."
- CSM, SAF
Course / Entry requirements

1. At least one year of cybersecurity working experience
2. Fundamental knowledge of cybersecurity

Course Objectives

1. Apply best practice in cyber defence skills to detect, contain, eradicate and report on successful cyber breaches
2. Understand the team based, communication and reporting skills required to deliver an effective and efficient response to a cyber breach
3. Understand the team based, communication and reporting skills required deliver an effective and efficient response to a cyber breach

Target Audience

IT professionals who are involved with the defense of an IT network. E.g. Cybersecurity professionals, System / Network Administrators, Project managers, Database administrators, IT infrastructure professionals

Certification Obtained

- Certificate of Competency by ST Engineering Cybersecurity Academy (STECA)
Course Overview:
The Systems Security Certified Practitioner (SSCP) course equips learners with a comprehensive review of domains of cybersecurity to implement, monitor and administer IT infrastructure in accordance with information security policies and procedures that ensure data confidentiality, integrity and availability. The SSCP domains are drawn from various information security topics within the (ISC) CBK.

Upon completion of this course, learners will be prepared for the SSCP certification by affirming their technical ability to implement, monitor and administer IT infrastructure using information security policies and procedures.

“The course is helpful in identifying the chapters in the exam... The lab sessions are more insightful.”

- IMDA
### Official SSCP® CBK® Training Seminar

<table>
<thead>
<tr>
<th></th>
<th>International Participants</th>
<th>S’poreans / PRs (aged 21 and above)</th>
<th>Skillsfuture Mid-Career Enhanced Subsidy (S’poreans aged 40 and above)</th>
<th>Workfare Training Support (S’poreans aged 35 and above, and earn &lt;$2000 per month)</th>
</tr>
</thead>
<tbody>
<tr>
<td>Full course fee (excl GST)</td>
<td>5000</td>
<td>5000</td>
<td>5000</td>
<td>5000</td>
</tr>
<tr>
<td>7% GST on nett course fee</td>
<td>350</td>
<td>350</td>
<td>350</td>
<td>350</td>
</tr>
<tr>
<td>Course fee (incl GST)</td>
<td>5350</td>
<td>5350</td>
<td>5350</td>
<td>5350</td>
</tr>
<tr>
<td>Less additional funding if eligible under various schemes</td>
<td>NA</td>
<td>630</td>
<td>2100</td>
<td>4750</td>
</tr>
<tr>
<td>Total nett course fee payable, including GST, after additional funding from the various funding schemes</td>
<td>5350</td>
<td>4720</td>
<td>3250</td>
<td>600</td>
</tr>
</tbody>
</table>

### Course / Entry requirements

1. At least one year of cybersecurity working experience
2. Fundamental knowledge of cybersecurity

### Course Objectives

1. Implement Authentication Mechanisms
2. Understand and Comply with Codes of Ethics
3. Understand Security Issues Related to Networks
4. Understand and Apply Fundamental Concepts of Cryptography
5. Understand the Risk Management Process
6. Understand Network and Communications, Systems and Application Security
7. Participate in Incident Handling

### Target Audience


### Certification Obtained

- Certificate of Competency by ST Engineering Cybersecurity Academy (STECA)
- Statement of Attainment by Skills Future Singapore (SSG)

### Appeal and Reassessment

The Statement of Attainments (SOAs) will not be issued to trainees who have been assessed as Not Yet Competent (NYC). Trainees who wish to be certified as Competent will have to undergo training and assessment for the entire module again. Where there are reasons to appeal against the Assessor’s decision, an appeal may be submitted in writing to ST Engineering Cybersecurity Academy (STECA) within 5 working days from the date of assessment stating clearly the ground(s) for Appeal. If the appeal is successful, a new round of assessment will be conducted at a fee of $150. If the appeal is unsuccessful, the trainee will have to undergo training and assessment again.
Course Overview:
The Cybersecurity Leadership programme (CSLP) equips learners with the knowledge and skills on the principles of Cyber Visibility (V), Cyber Situational Awareness (SA) and Cyber Critical [C] Resource Alignment into their business model with the aim of making effective and timely decisions in times of crisis. Learners will also learn how to mitigate the impact of cyber breaches on their business value chain and stakeholders.

Upon completion of this course, learners will be able to utilise effectively the scientifically proven RS iterative model to implement a cyber defence framework for their organisations.

Course / Entry requirements
1. At least one year of IT security management working experience
2. Fundamental knowledge of cybersecurity

Course Objectives
1. Apply the RS model in the formulation of cybersecurity strategy and tactics to manage a breach in a responsive manner without compromising business operations efficiency
2. Apply V-SA-C to enable critical decision making swiftly & effectively
3. Identify industry specific best practices to accelerate the implementation of the RS model

Target Audience
Professionals who are in senior leadership positions involved with cyber defence of their organisation

Certification Obtained
• Certificate of Completion by ST Engineering Cybersecurity Academy (STECA)