CYBERSECURITY
ACADEMY

A LEADER IN CYBERSECURITY EDUCATION

Returning Cyber Ready Professionals Back to You

ST Engineering

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 1,700 professionals beyond the Engineering industry from more than 100 organisations to date. STECA is an exclusive partner of (ISC)^2.

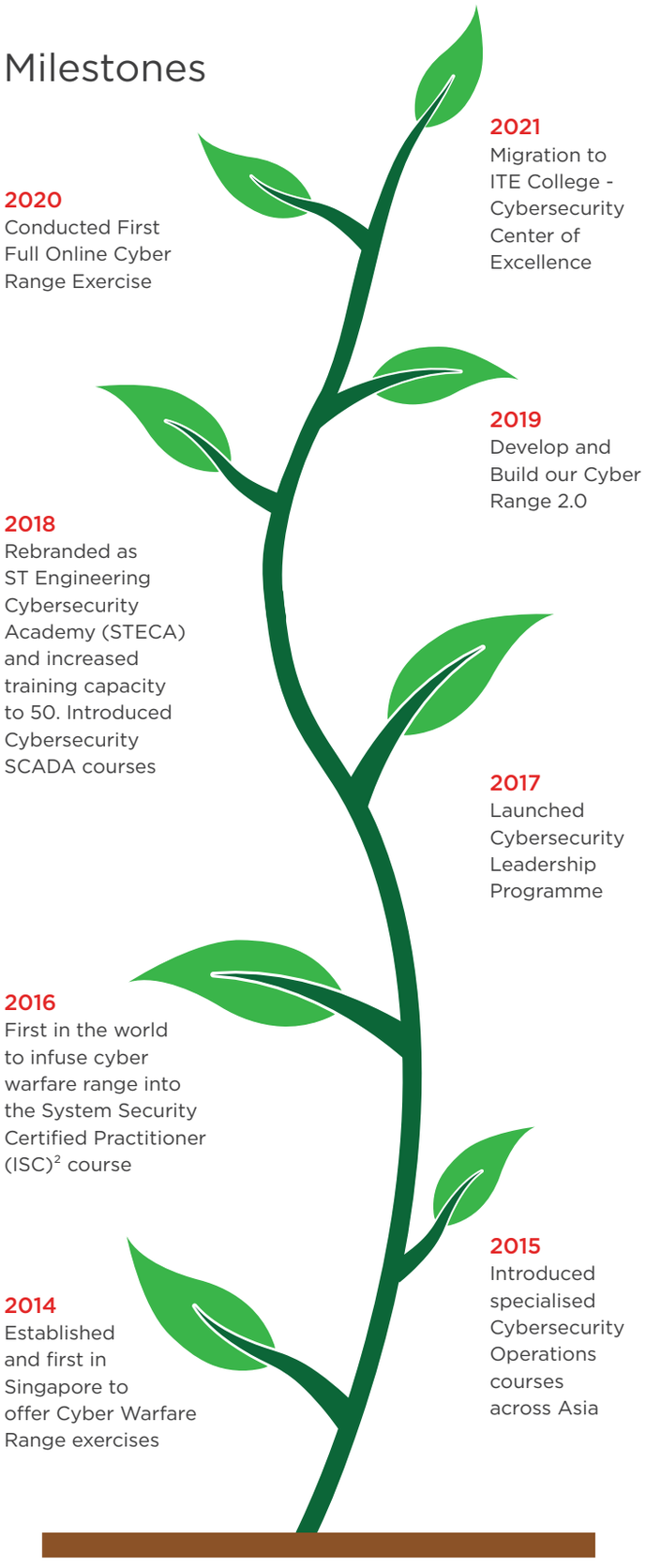
Core Capabilities

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



2021
Migration to ITE College - Cybersecurity Center of Excellence

2020
Conducted First Full Online Cyber Range Exercise

2019
Develop and Build our Cyber Range 2.0

2018
Rebranded as ST Engineering Cybersecurity Academy (STECA) and increased training capacity to 50. Introduced Cybersecurity SCADA courses

2017
Launched Cybersecurity Leadership Programme

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

2015
Introduced specialised Cybersecurity Operations courses across Asia

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

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.

OVERARCHING TRAINING METHODOLOGY

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.

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.

MOST COURSES BY STECA ARE MAPPED TO

SKILLS FRAMEWORK FOR INFOCOMM TECHNOLOGY

JOINTLY DEVELOPED BY

SkillsFuture SG

Workforce Singapore

INFOCOMM MEDIA DEVELOPMENT AUTHORITY

- Cybersecurity By Design (CSBD)
- Cybersecurity Bridging Programme (CSBP)

- Cybersecurity Operations Specialist (CSOS)

- Cybersecurity Operations Specialist (CSOS)
- Cybersecurity Bridging Programme (CSBP)
- Cybersecurity ICS Engineer (CSIE)
- ICS Cybersecurity Foundation for Operators (ICS CSF)
- Cybersecurity By Design (CSBD)

- Cyber Warfare Exercises

CYBER WARFARE EXERCISE

Course Training Duration

Depends on the number of scenarios required by companies.
A minimum 1 day with 2 scenarios.

Mode of Training

Practical
Hands on
exercises

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)

CYBERSECURITY BY DESIGN (CSBD)

Course Training Duration

2 days

Mode of Training

Classroom
based

Course Overview:

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

Course / Entry requirements

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

Target Audience

IT professionals who are involved in the design of IT / OT systems. E.g. Project Managers / Leads, Solution Engineer, Solution Architect

Certification Obtained

- Certificate of Completion by Nanyang Polytechnic and ST Engineering Cybersecurity Academy (STECA)

CYBERSECURITY BRIDGING PROGRAMME (CSBP)

Course Overview:

The Cybersecurity Bridging Programme (CSBP) equips learners with the knowledge and skills to implement sufficient IT security controls to protect their IT assets. In addition, they will gain an overview of the cybersecurity landscape, as well as cybersecurity principles with hands-on lab sessions.

Upon completion of this course, learners will have a better understanding of the cybersecurity competencies and be able to further enrol in other cybersecurity courses offered by ST Engineering Cybersecurity Academy (STECA).

Course Training Duration

3 days

Mode of Training

Classroom
based

Course / Entry requirements

1. At least three years of IT admin working experience
2. Fundamental command line skillsets covering Windows, Networks and Linux (an advantage)

Course Objectives

1. Understand fundamentals of cybersecurity concepts and principles
2. Define key terms and concepts in the field of cybersecurity
3. Learn and appreciate basic cyber-attack procedures
4. Identify, detect and perform basic defence controls to different cyber threats

Target Audience

IT professionals who are involved in the design of IT / OT systems. E.g. Project Managers / Leads, Solution Engineer, Solution Architect

Certification Obtained

- Certificate of Performance by ST Engineering Cybersecurity Academy (STECA)

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.

CSBP

CYBERSECURITY OPERATIONS SPECIALIST (CSOS)

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 Training Duration

5 days

Mode of Training

Classroom / Online

Enable By Cloud Cyber Range

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. Be able to explain the entire kill-chain of various cyber-attacks

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)

ICS CYBERSECURITY
FOUNDATION (ICS CSF)

Course Overview:

The Industrial Control Systems Cybersecurity Foundation (ICS CSF) course equips learners with a comprehensive understanding on the protection of SCADA networks within a realistic control system environment. Learners will also have hands-on practice on the various tools to handle potential attacks on the control systems.

Upon completion of this course, learners will be prepared to identify analyse, respond and investigate cyber-attacks and successfully safeguard their organisation from cyber threats.

Course Training Duration

2 days

Mode of Training

Classroom
based

Course / Entry requirements

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

Course Objectives

1. Understand various attacks and how they could have an impact on ICS
2. Identify the tools and techniques to investigate possible breaches into ICS
3. Demonstrate the various tools to mitigate cyber risks based on detected and design vulnerabilities

Target Audience

OT Operators and IT Cybersecurity Practitioner

Certification Obtained

- Certificate of Competency by ST Engineering Cybersecurity Academy (STECA)

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.

CYBERSECURITY

ICS ENGINEER (CSIE)

Course Overview:

The Cybersecurity Industrial Control Systems Engineer (CSIE) equips learners with the knowledge and skills on how to mitigate and protect SCADA networks.

Upon completion of this course, learners will gain the skills in understanding SCADA network and the security tools needed to protect the infrastructure against potential cyber threats. With hands-on approach in the classroom guided by the trainer, learners will be able to apply the best practices of the industry back at their workplace.

Course Training Duration

3 days

Mode of Training

Classroom
based

Course / Entry requirements

1. At least two years of cybersecurity working experience
2. Basic understanding of Industrial Control System (ICS), Cyber Physical System (CPS) or Operational Technology (OT)

Target Audience

Professionals who are involved in industrial control system environments, primarily in four domains:
1) IT (includes operational technology support),
2) IT security (includes operational technology security),
3) Engineering,
4) Corporate, industry and professional standards.

Course Objectives

1. Understand the OT Cybersecurity ecosystem with concepts covering embedded systems, protocols fundamentals, known vulnerabilities discovery,
2. forensic investigation and process exploitation

3. Learn about threats and cyber risks to Industrial Control Systems (ICS), as well as the different types and stages of a cyber-attack

Experience real-world use cases and examples, hands-on applications and exercises that are incorporated with realistic scenarios built around operational cyber physical testbeds.

Certification Obtained

- Certificate of Competency by ST Engineering Cybersecurity Academy (STECA)

CSIE

www.stengg.com
cybersecurity@stengg.com

www.stengg.com/cybersecurity