Government Capacity Building

Program Brochure · 2026

CYBER RESILIENCE FOR POWER SECTOR

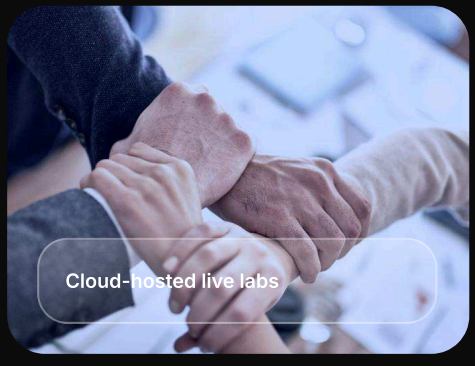
Keep the lights on, securely.

Advanced ↗ | 56 Hours ↗ | SAM-POWERSEC ↗

Government Capacity Building

Capable institutions. Secure nation.

20 programs in this track



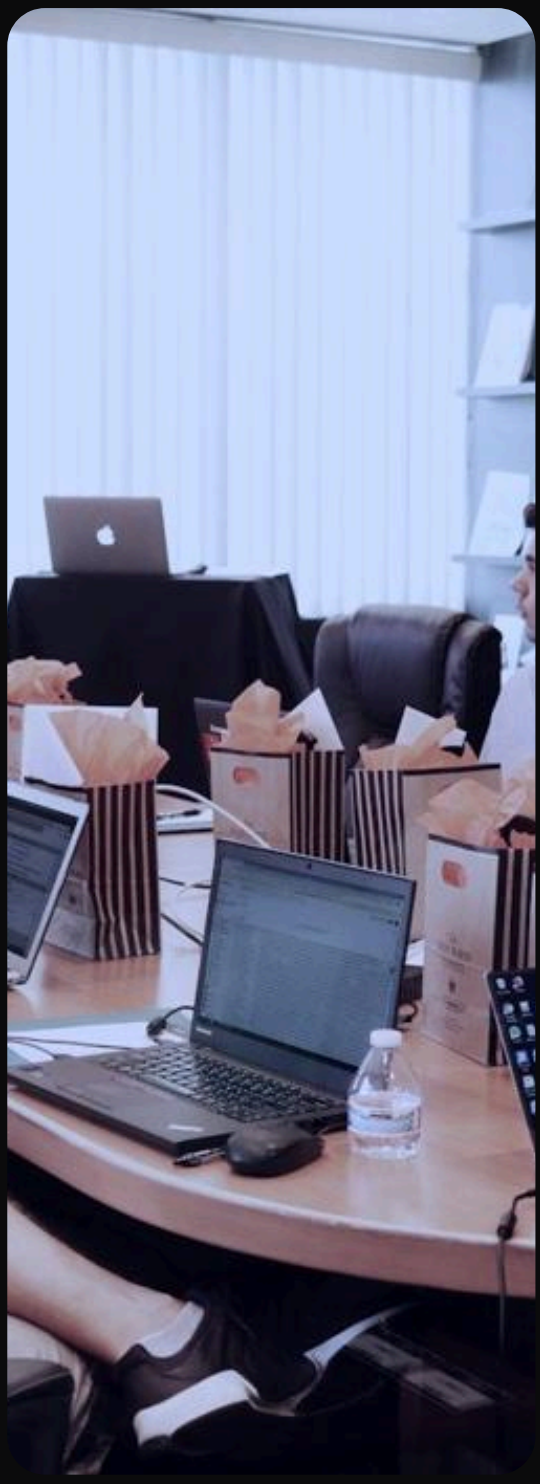
8

modules · hands-on labs · capstone project

Inside this brochure

Contents

Program overview 03
Who it's for 04
Learning outcomes 05
Program runway 06
Detailed curriculum 07
Tools & frameworks 10
Projects & capstone 11
Certification & method 12
Learning path 13
FAQs 14



AT A GLANCE

Level	**Advanced**
Duration	**56 Hours**
Modules	**8**
Certificate	**SAM-POWERSEC**

Program overview

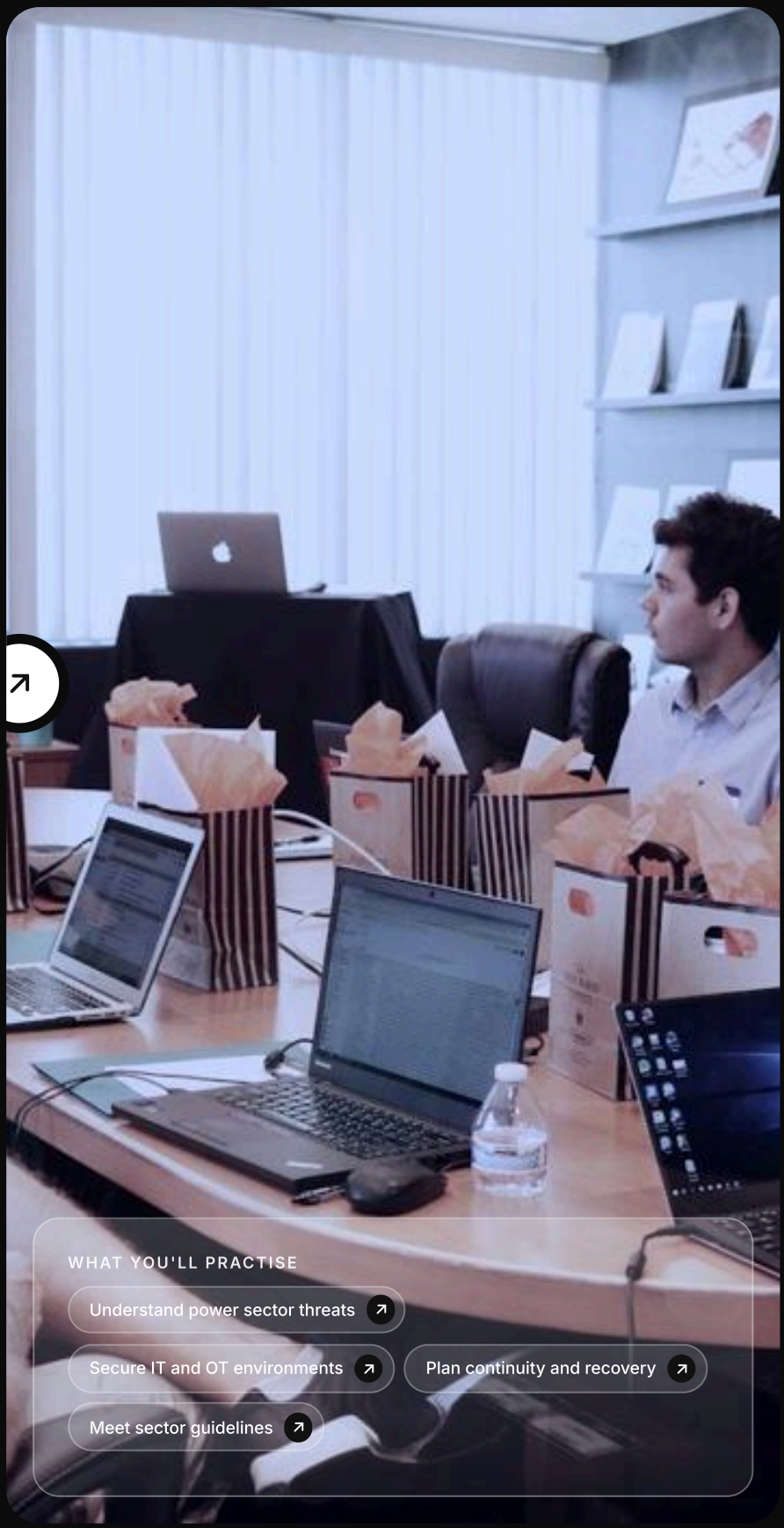
Keep the lights on, securely.

Cyber resilience for power generation and distribution organizations.

Power generation and distribution organisations are rapidly digitising, connecting control systems, smart meters and renewable assets in ways that widen exposure to cyber threats. This program helps power sector professionals understand sector-specific threats, secure both IT and OT environments, meet CEA and CERT-In guidelines, and plan continuity and recovery, through case studies, tabletop exercises and sector-focused planning work.

DELIVERY

Instructor-led · Live virtual · Blended

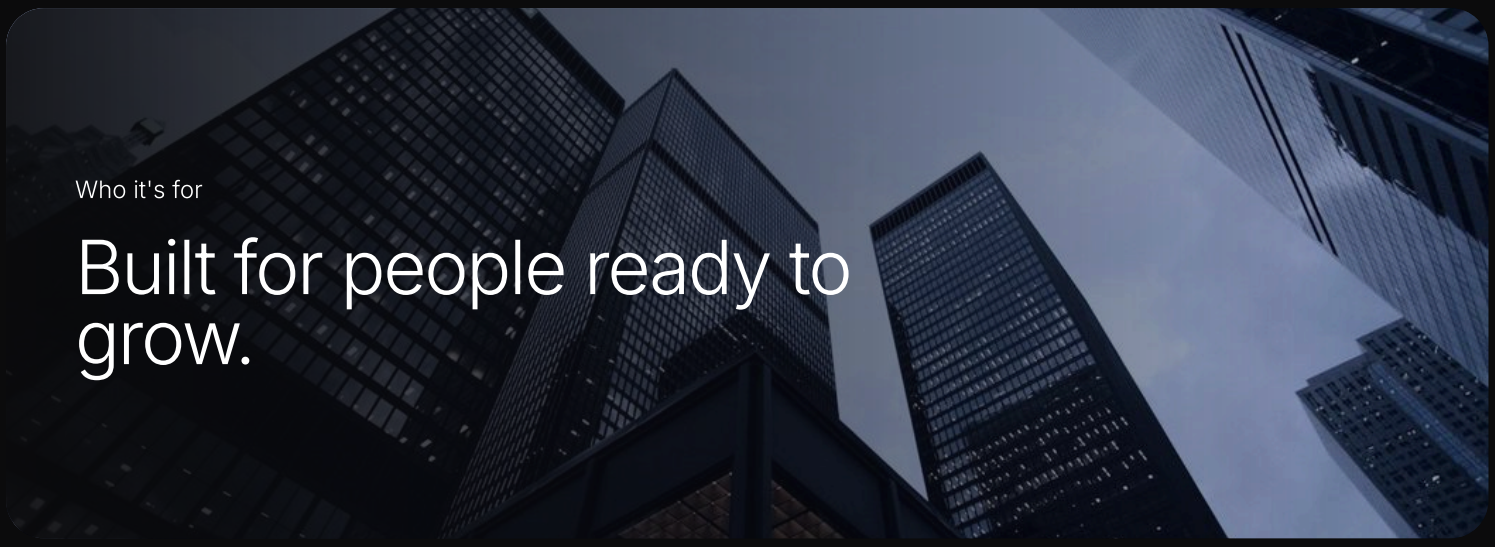


LEVEL
Advanced

DURATION
56 Hours

CERTIFICATION
SAM-POWERSEC

TRACK
Government Capacity Building



Who it's for

Built for people ready to grow.

01

Government officials

Cyber awareness, AI for public service, e-governance

02

Senior IAS / IPS officers

Technology leadership and AI policy

03

PSU workforce

IT security, OT/ICS/SCADA, digital skills

04

Law enforcement & defence

Cyber forensics, CERT ops, defence cyber

PREREQUISITES

Experience in power sector IT, OT or operations	01
Understanding of networks and control systems	02
Familiarity with organisational security policies	03

ROLES THIS PREPARES YOU FOR

- Power utility CISOs and security teams ↗
- SCADA and EMS engineers ↗
- Substation automation engineers ↗
- Utility SOC analysts ↗
- Business continuity managers ↗

Learning outcomes

What you'll be able to do.



01	Map digital systems across generation, transmission and distribution operations
02	Analyse power sector threats using public grid incident lessons
03	Assess compliance with CEA guidelines and CERT-In directions
04	Apply security controls across utility IT and OT environments
05	Respond to grid cyber incidents using sector response playbooks
06	Plan continuity and recovery for critical power operations

Program runway

Module by module.

8
modules · 56 hours

01	**Power Sector Digital Landscape** Generation, transmission and distribution systems, SCADA and energy management systems, Smart meters and grid digitisation	7 hrs
02	**Power Sector Threats** Threats to grid operations, Lessons from public grid incidents, Ransomware in utilities	7 hrs
03	**Sector Guidelines and Compliance** CEA cybersecurity guidelines overview, CERT-In directions for power, Sectoral CERT roles	7 hrs
04	**Securing IT Environments** Identity and access management, Email and endpoint protection, Network security controls	7 hrs
05	**Securing OT and Grid Systems** Segmentation of control networks, Substation automation security, Secure remote access	7 hrs
06	**Detection and Incident Response** Utility SOC operations, OT-aware detection use cases, Incident response playbooks	7 hrs
07	**Continuity and Recovery Planning** Business continuity for utilities, Black start and restoration considerations, Backup control centres	7 hrs
08	**Resilience Governance and Exercises** Cyber resilience metrics, Leadership and board reporting, Tabletop exercise design	7 hrs
★	**Capstone · Utility Cyber Resilience Roadmap** Assessment, capstone review and certification	

The syllabus.

Modules 01–03

Module 01

Power Sector Digital Landscape

7 hours

Hands-on lab
Map digital systems across a generation-to-distribution value chain

TOPICS COVERED

- Generation, transmission and distribution systems
- SCADA and energy management systems
- Smart meters and grid digitisation
- Renewables and distributed energy
- Sector regulators and bodies

Module 02

Power Sector Threats

7 hours

Hands-on lab
Analyse a public grid incident case and identify the control gaps involved

TOPICS COVERED

- Threats to grid operations
- Lessons from public grid incidents
- Ransomware in utilities
- Supply chain and equipment risks
- Insider and contractor risks

Module 03

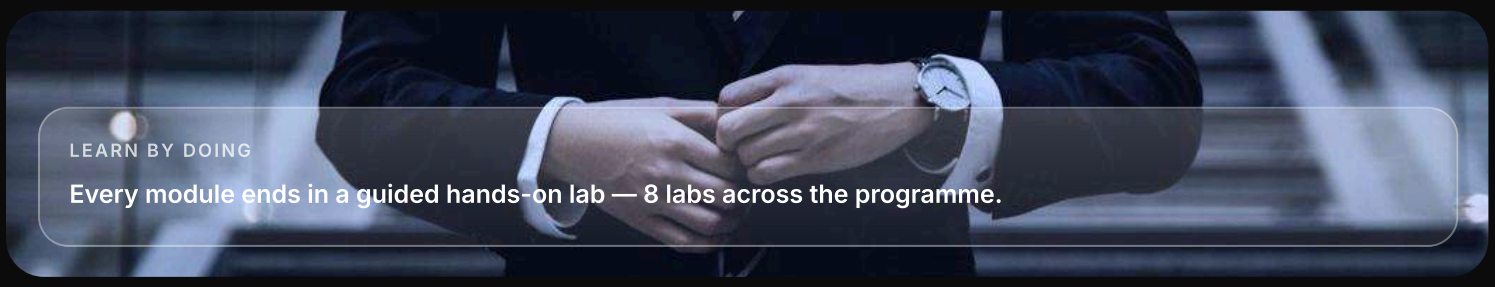
Sector Guidelines and Compliance

7 hours

Hands-on lab
Assess a sample utility against sector cybersecurity guideline requirements

TOPICS COVERED

- CEA cybersecurity guidelines overview
- CERT-In directions for power
- Sectoral CERT roles
- Cyber crisis management plans
- Audit and reporting obligations



LEARN BY DOING

Every module ends in a guided hands-on lab — 8 labs across the programme.

Syllabus, continued.

Modules 04–06

Module 04

Securing IT Environments

7 hours

Hands-on lab
Prioritise IT security improvements from a sample utility assessment report

TOPICS COVERED

- Identity and access management
- Email and endpoint protection
- Network security controls
- Vulnerability management
- Data protection and backups

Module 05

Securing OT and Grid Systems

7 hours

Hands-on lab
Design secure remote access for vendor support at a substation

TOPICS COVERED

- Segmentation of control networks
- Substation automation security
- Secure remote access
- Monitoring OT traffic
- Patch and change constraints

Module 06

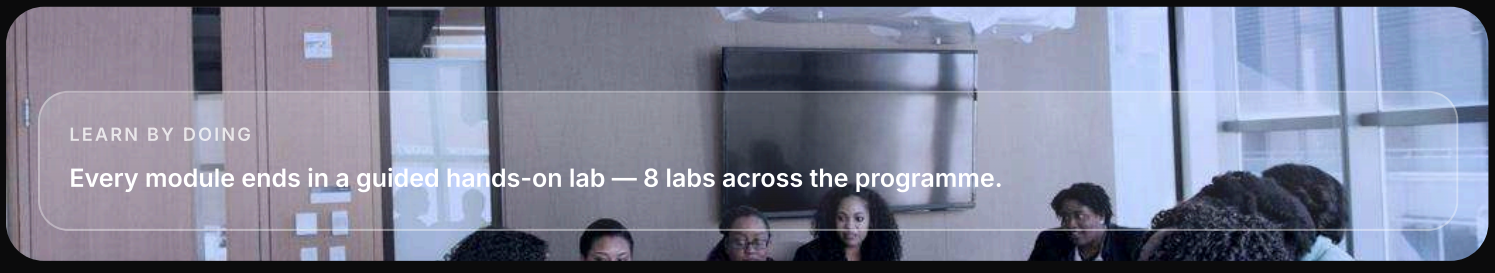
Detection and Incident Response

7 hours

Hands-on lab
Respond to a simulated SCADA anomaly using a structured response playbook

TOPICS COVERED

- Utility SOC operations
- OT-aware detection use cases
- Incident response playbooks
- Coordination with grid operators
- Evidence preservation



LEARN BY DOING

Every module ends in a guided hands-on lab — 8 labs across the programme.

Syllabus, continued.

Modules 07–08

Module 07

Continuity and Recovery Planning

7 hours

Hands-on lab
Develop recovery priorities for a simulated distribution control centre outage

TOPICS COVERED

- Business continuity for utilities
- Black start and restoration considerations
- Backup control centres
- Recovery time objectives
- Stakeholder communication

Module 08

Resilience Governance and Exercises

7 hours

Hands-on lab
Conduct a tabletop exercise on a coordinated cyber incident at a utility

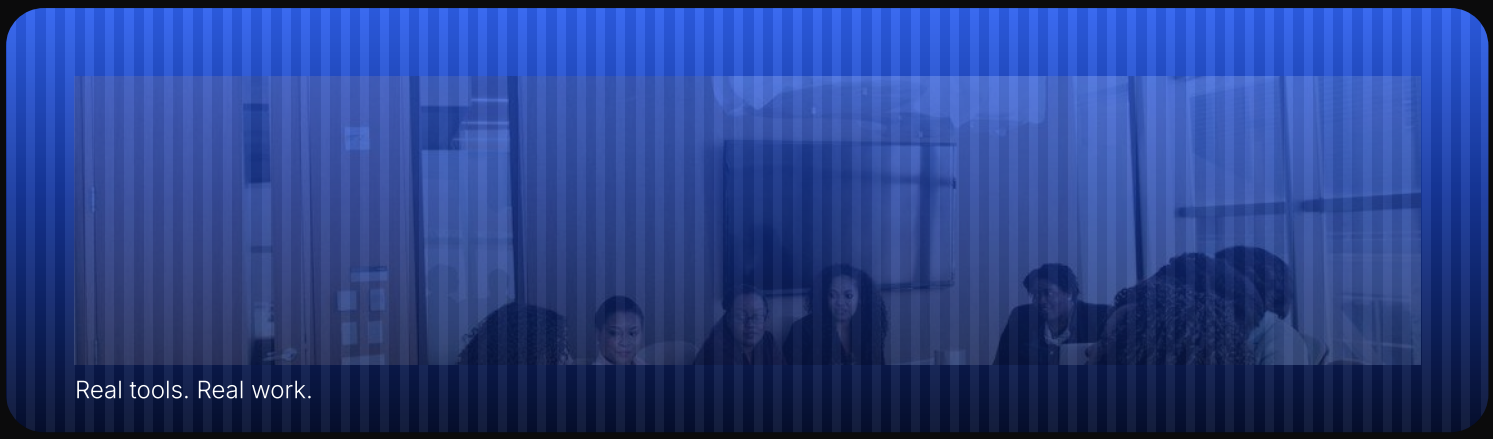
TOPICS COVERED

- Cyber resilience metrics
- Leadership and board reporting
- Tabletop exercise design
- Workforce awareness
- Continuous improvement



CAPSTONE

Utility Cyber Resilience Roadmap



Real tools. Real work.

Frameworks & standards

CERT-In

FOCUS AREAS

Understand power sector threats	01
Secure IT and OT environments	02
Plan continuity and recovery	03
Meet sector guidelines	04



LAB ACCESS

24×7 cloud labs for the length of the program

01

Utility Guideline Gap Assessment

Assess a sample power utility against sector cybersecurity guidelines and produce a prioritised list of gaps and remediation actions.

02

Substation Remote Access Design

Design a secure remote access arrangement for vendor support at a substation, covering approvals, segmentation, monitoring and logging.

03

Cyber Crisis Management Plan

Draft a cyber crisis management plan outline for a utility, defining roles, escalation, communication and coordination with sector bodies.



Capstone project

Utility Cyber Resilience Roadmap

Build a cyber resilience roadmap for a sample power utility, combining threat analysis, guideline compliance assessment, IT and OT security improvements, detection and response arrangements, continuity planning and governance metrics, and present it to a panel acting as utility leadership.

Real-world scenario ↗ Mentor review ↗ Portfolio ready ↗

Certification

SAM-POWERSEC

Awarded on successful completion of the program assessments.

- MCQ assessments
- Practical lab evaluation
- Project & capstone review
- Final presentation



The SAM Learning Framework™

Scenario · Apply · Master · Mentor

Phase 01

Scenario

Real-world attack and use-case scenarios open every module.

Phase 02

Apply

Hands-on lab work, CTF challenges and live projects.

Phase 03

Master

Assessment, peer review and certification prep.

Phase 04

Mentor

Post-program career guidance and support.

DELIVERY MODELS

- Instructor-Led (ILT)
- Virtual Instructor-Led
- Self-Paced Online
- E-Learning Licensing
- Blended Learning
- Corporate Onsite
- Bootcamp Intensive

Learning path · Government Capacity Building

Where this program fits.

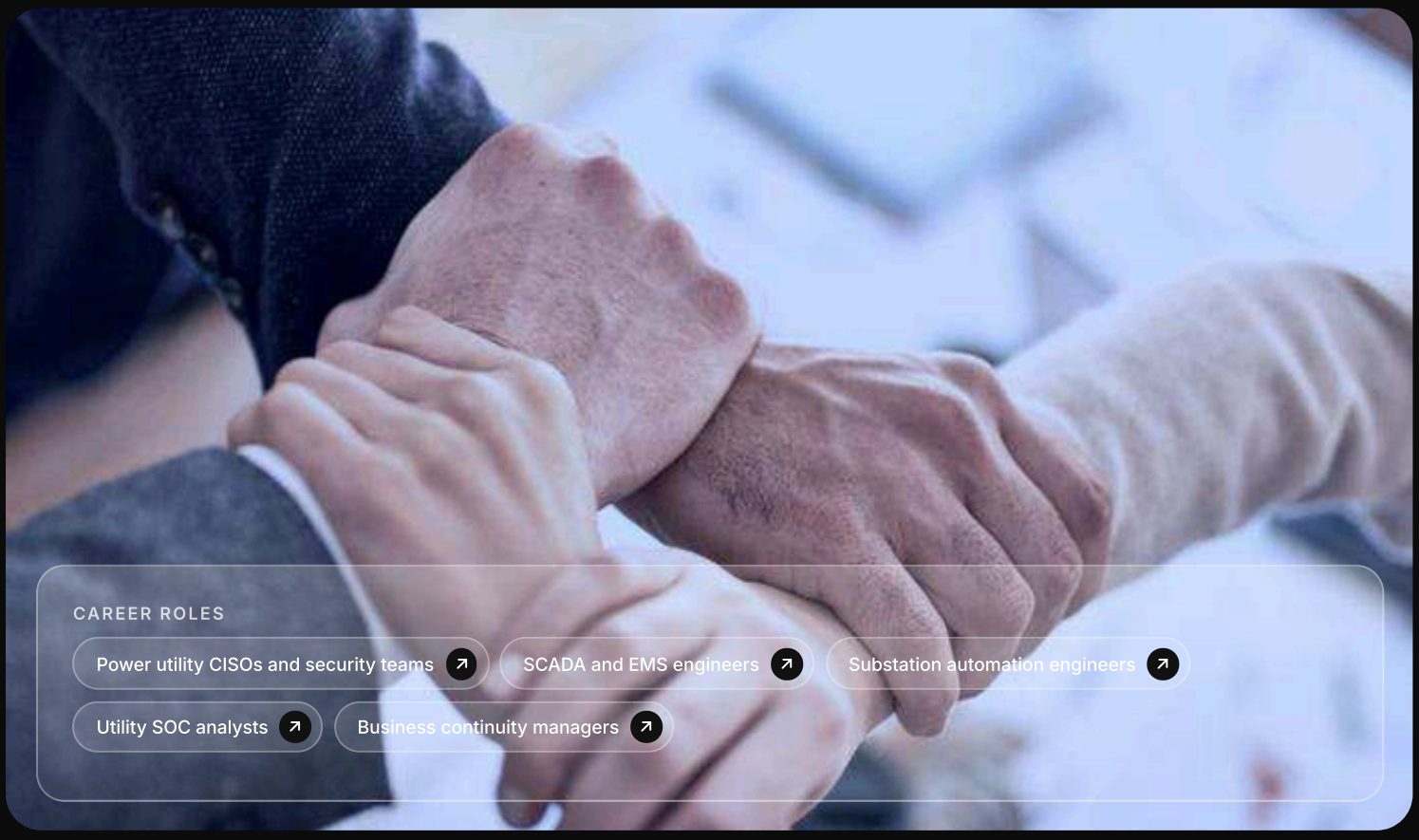
Foundation	Intermediate	Advanced	Expert	Executive
4 programs	5 programs	You are here	1 programs	2 programs

Before this

- **Digital Governance & e-Governance Platforms** — 32 Hours
- **Cybersecurity for Critical Infrastructure** — 40 Hours
- **AI Policy & Technology Regulation Workshop** — 24 Hours
- **OT/ICS/SCADA Security for Industrial PSUs** — 48 Hours

Up next

- **PSU Digital Transformation Advisory** — Custom



CAREER ROLES

- Power utility CISOs and security teams
- SCADA and EMS engineers
- Substation automation engineers
- Utility SOC analysts
- Business continuity managers

Questions, answered.

Q01

Do I need prior experience to join?

Yes. This is an advanced-level program that assumes prior experience in power sector IT, OT or grid operations. It moves quickly into frameworks, case studies and hands-on work, so participants should meet the listed prerequisites before enrolling.

Q02

How is the program delivered and scheduled?

The 56 hours program is instructor-led and can be delivered live virtual, in person at your institution, or in a blended format. Session timings and batch sizes are planned with the sponsoring organisation to fit official working schedules.

Q03

Will I receive a certificate?

Yes. Participants who meet attendance requirements and successfully complete the assessments receive the Samcommunity Academy SAM-POWERSEC certificate. Assessments may include quizzes, practical exercises and a final capstone review, depending on the program format.

Q04

What do the hands-on exercises involve?

Exercises use case studies, templates, tabletop scenarios and guided demonstrations rather than live production systems. Any required materials or sandbox access are shared before the program, and no special software installation is usually needed.

Q05

Is career or post-program support included?

The program is designed for capacity building of working professionals rather than placement. Participants receive learning resources, templates and guidance on further learning paths. Samcommunity Academy does not guarantee promotions, postings, jobs or salary outcomes.



Let's talk

START CYBER RESILIENCE FOR POWER SECTOR.

academy@samcommunity.in

corporate@samcommunity.in

samcommunity.in

@samcommunity_

Learn practical skills. Grow with mentors.

Xylyn Samcommunity Private Limited · DPIIT-recognized startup · Surat, Gujarat, India