Networking & Infrastructure

Program Brochure · 2026

ZERO TRUST NETWORK ARCHITECTURE

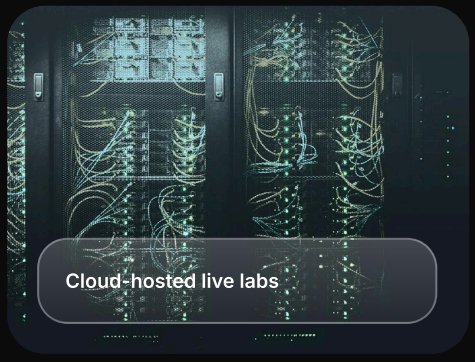
Never trust. Always verify.

Expert ↗ 48 Hours ↗ SAM-ZTNA ↗

Networking & Infrastructure

Connect. Secure. Scale.

10 programs in this track



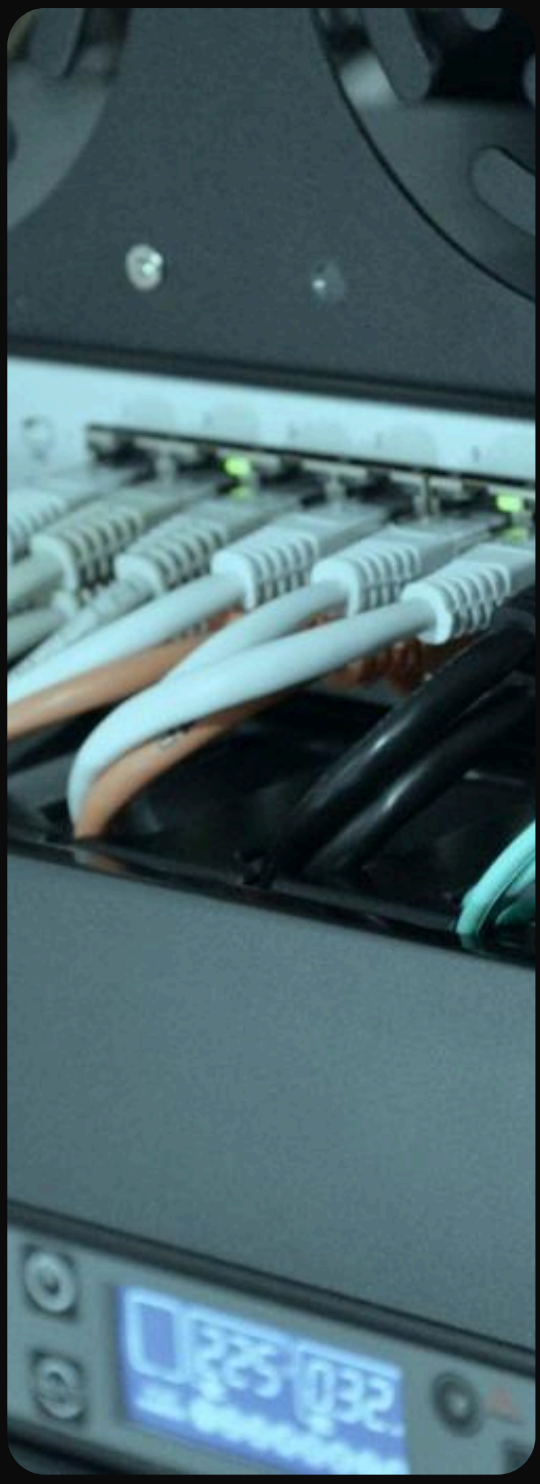
7

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	**Expert**
Duration	**48 Hours**
Modules	**7**
Certificate	**SAM-ZTNA**

Program overview

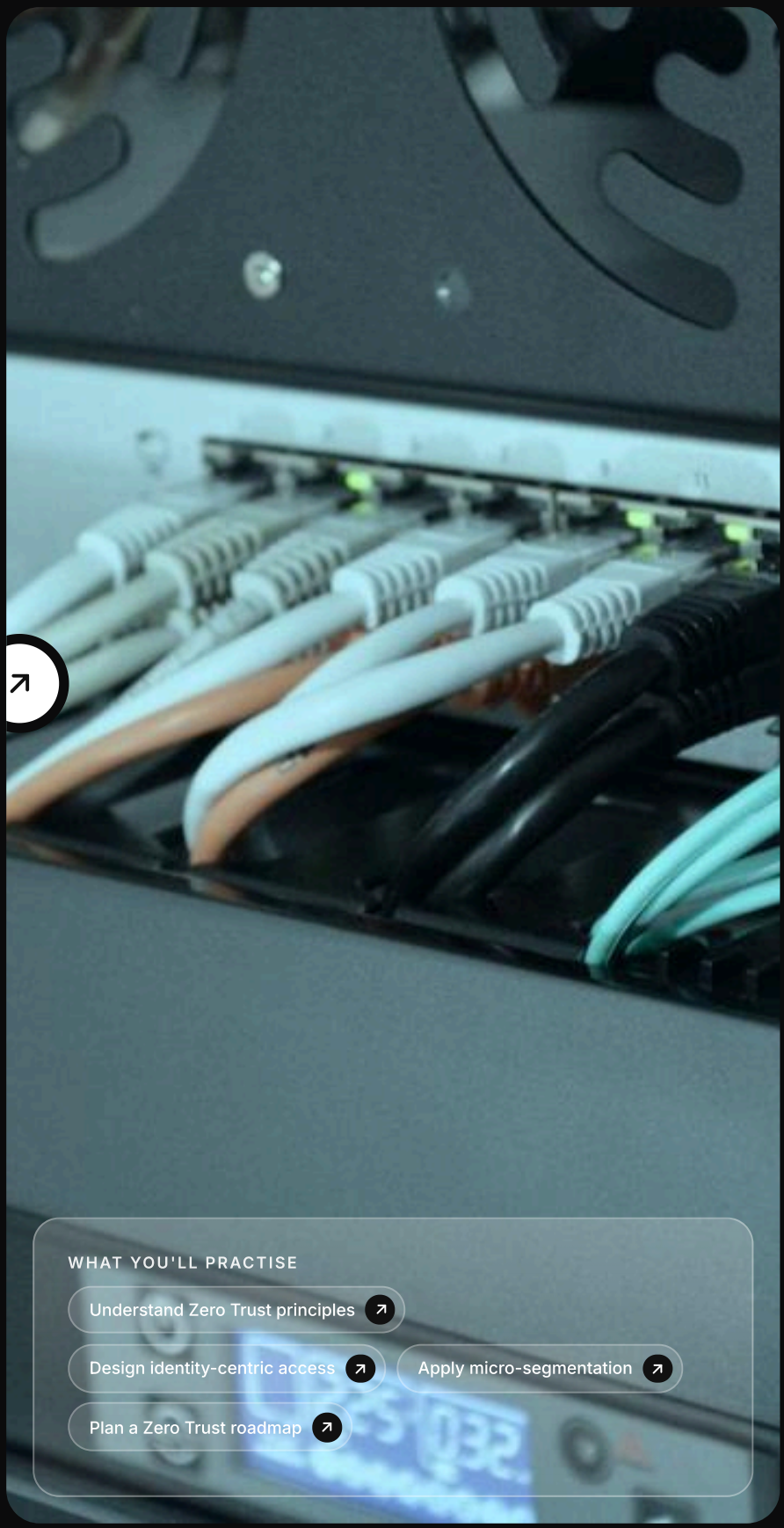
Never trust. Always verify.

Design identity-centric, least-privilege network architectures.

Perimeter-based security no longer fits a world of cloud services, remote work and connected devices. Zero Trust replaces implicit trust with continuous verification of every user, device and workload. This expert program covers NIST SP 800-207 and CISA maturity guidance, identity-centric access, micro-segmentation and practical roadmaps for adopting Zero Trust across enterprise networks.

DELIVERY

ILT · VILT · Blended

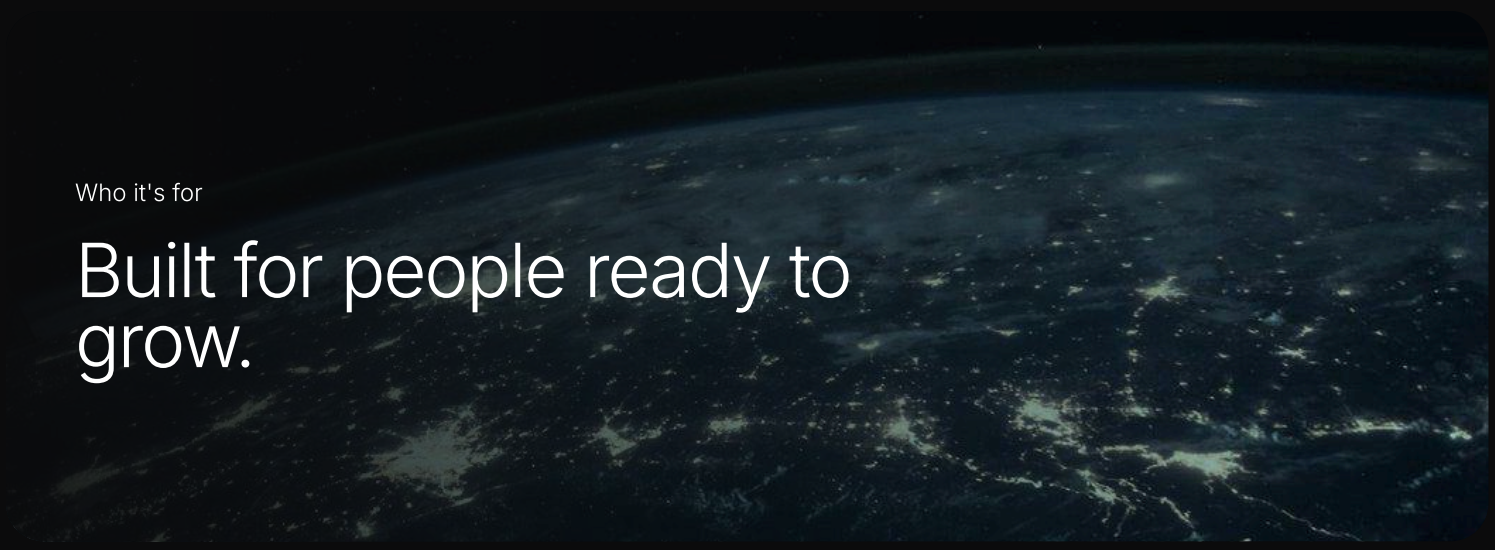


LEVEL
Expert

DURATION
48 Hours

CERTIFICATION
SAM-ZTNA

TRACK
Networking & Infrastructure



Who it's for

Built for people ready to grow.

01

Beginners

Network+ and CCNA foundations

02

Network engineers

CCNP Enterprise, SD-WAN, automation

03

Security engineers

Palo Alto, Fortinet, network security

04

Architects

CCIE prep, Zero Trust, SASE / SSE

PREREQUISITES

Strong networking and security architecture experience	01
Familiarity with identity and access management	02
Understanding of cloud and hybrid environments	03

ROLES THIS PREPARES YOU FOR

- Security Architect ↗
- Network Security Architect ↗
- Zero Trust Program Lead ↗
- Infrastructure Security Manager ↗
- Cloud Security Architect ↗

Learning outcomes

What you'll be able to do.



01	Apply NIST SP 800-207 Zero Trust principles and components
02	Assess organisational maturity using the CISA Zero Trust model
03	Design identity-centric access with MFA and conditional policies
04	Plan micro-segmentation for data centre and cloud workloads
05	Integrate device posture, ZTNA and continuous monitoring signals
06	Build a phased, business-aligned Zero Trust adoption roadmap

Program runway

Module by module.

7
modules · 48 hours

01	**Zero Trust Principles and Frameworks** Limitations of perimeter security, NIST SP 800-207 tenets, Policy engine and enforcement points	6 hrs
02	**Identity as the New Perimeter** Identity providers and federation, Phishing-resistant MFA and passkeys, Conditional and risk-based access	8 hrs
03	**Device Trust and Posture** Device inventory and health signals, Endpoint management and EDR integration, Certificate-based device identity	6 hrs
04	**Micro-segmentation** Segmentation models and granularity, Application dependency mapping, Host-based and network-based enforcement	8 hrs
05	**ZTNA and Secure Access** ZTNA vs traditional VPN, Agent and agentless ZTNA models, Application connectors and brokers	6 hrs
06	**Visibility, Analytics and Automation** Telemetry and logging requirements, SIEM and UEBA integration, Continuous trust evaluation	6 hrs
07	**Zero Trust Roadmap and Governance** Maturity assessment methods, Prioritising protect surfaces, Phased migration planning	8 hrs
★	**Capstone · Enterprise Zero Trust Architecture** Assessment, capstone review and certification	

The syllabus.

Modules 01–03

Module 01

Zero Trust Principles and Frameworks

6 hours

Hands-on lab
Map an existing architecture to NIST 800-207 logical components.

TOPICS COVERED

- Limitations of perimeter security
- NIST SP 800-207 tenets
- Policy engine and enforcement points
- CISA Zero Trust Maturity Model
- Common Zero Trust misconceptions

Module 02

Identity as the New Perimeter

8 hours

Hands-on lab
Design conditional access policies for employees, contractors and admins.

TOPICS COVERED

- Identity providers and federation
- Phishing-resistant MFA and passkeys
- Conditional and risk-based access
- Privileged access management
- Workload and machine identities

Module 03

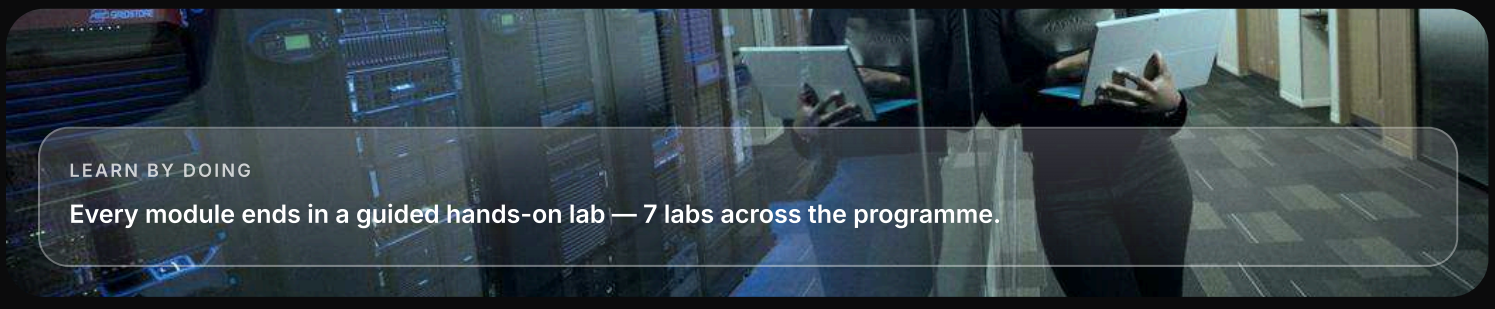
Device Trust and Posture

6 hours

Hands-on lab
Define device posture rules gating access to sensitive applications.

TOPICS COVERED

- Device inventory and health signals
- Endpoint management and EDR integration
- Certificate-based device identity
- Unmanaged and BYOD strategies
- Continuous posture reassessment



LEARN BY DOING

Every module ends in a guided hands-on lab — 7 labs across the programme.

Syllabus, continued.

Modules 04–05

Module 04

Micro-segmentation

8 hours

Hands-on lab
Create a segmentation policy from an application dependency map.

TOPICS COVERED

- Segmentation models and granularity
- Application dependency mapping
- Host-based and network-based enforcement
- Cloud security groups and policies
- Kubernetes network policies

Kubernetes

Module 05

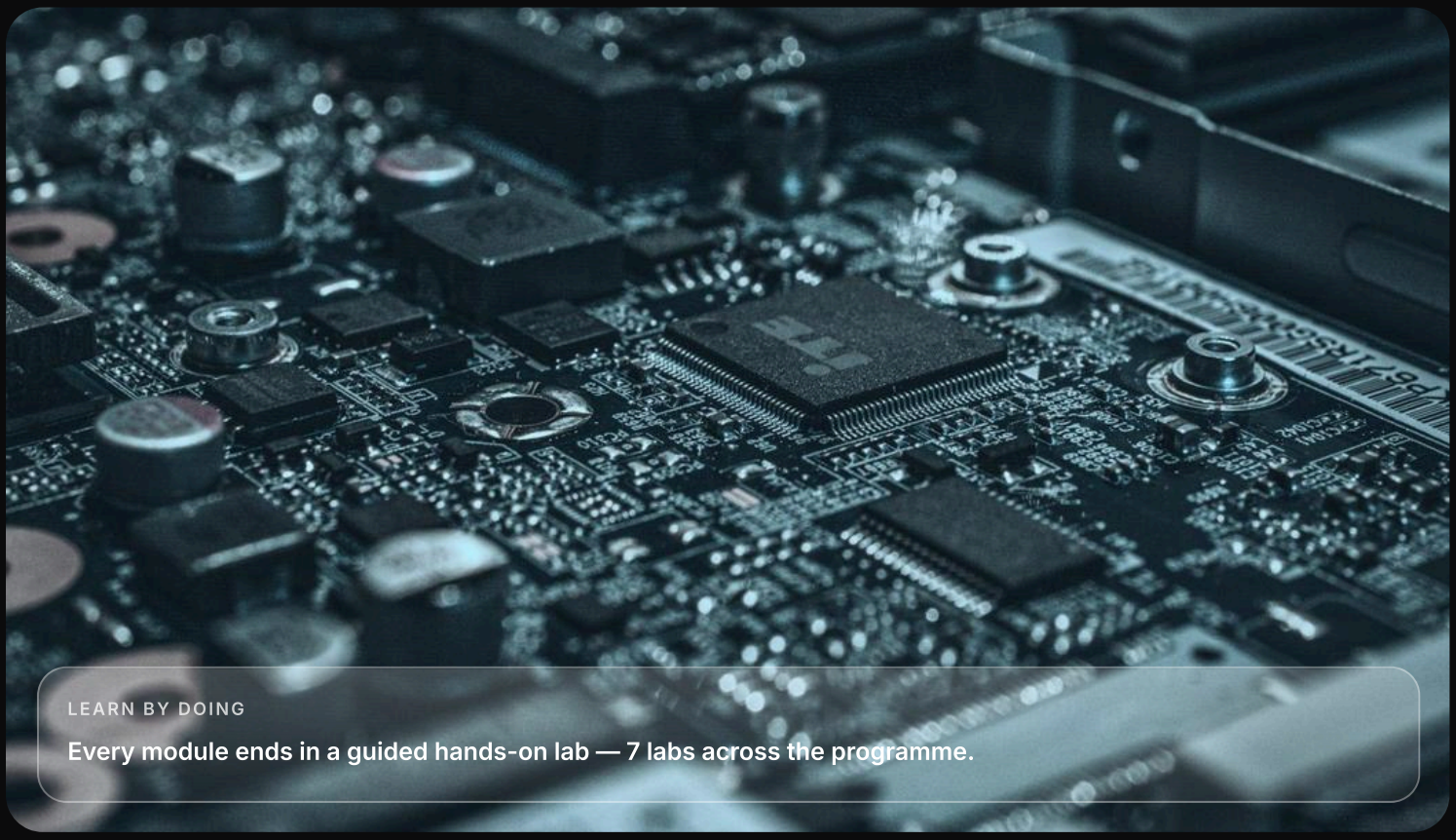
ZTNA and Secure Access

6 hours

Hands-on lab
Design a ZTNA rollout replacing VPN access for three applications.

TOPICS COVERED

- ZTNA vs traditional VPN
- Agent and agentless ZTNA models
- Application connectors and brokers
- Integration with SASE platforms
- Application access policy design



LEARN BY DOING

Every module ends in a guided hands-on lab — 7 labs across the programme.

Syllabus, continued.

Modules 06–07

Module 06

Visibility, Analytics and Automation

6 hours

Hands-on lab
Define telemetry sources and detections supporting continuous verification.

TOPICS COVERED

- Telemetry and logging requirements
- SIEM and UEBA integration
- Continuous trust evaluation
- Automated response and orchestration
- Zero Trust metrics and reporting

Module 07

Zero Trust Roadmap and Governance

8 hours

Hands-on lab
Produce a phased Zero Trust roadmap for a sample enterprise.

TOPICS COVERED

- Maturity assessment methods
- Prioritising protect surfaces
- Phased migration planning
- Metrics and governance
- Stakeholder communication and change



CAPSTONE

Enterprise Zero Trust Architecture



Kubernetes

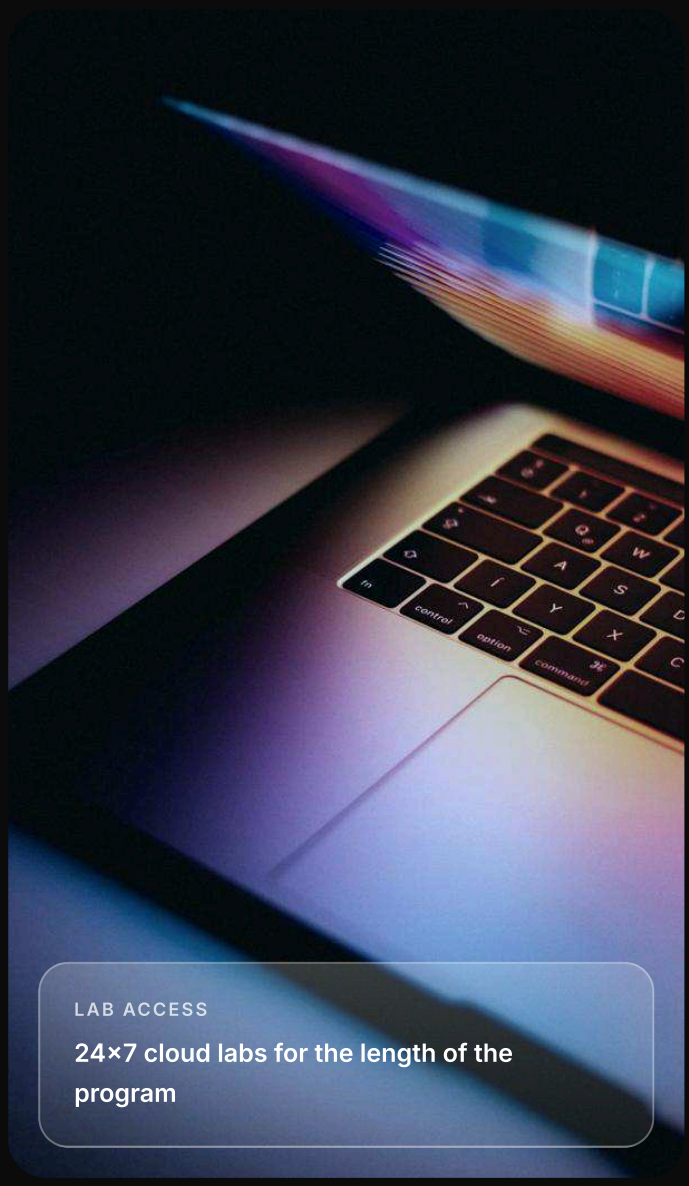
Container orchestration

Frameworks & standards

Zero Trust

FOCUS AREAS

Understand Zero Trust principles	01
Design identity-centric access	02
Apply micro-segmentation	03
Plan a Zero Trust roadmap	04



01

Zero Trust Maturity Assessment

Assess a case-study organisation against the CISA maturity model and identify priority gaps across each pillar.

02

Identity Access Policy Set

Design conditional access, phishing-resistant MFA and privileged access policies for a hybrid workforce, with clear justification for each control.

03

Segmentation Blueprint

Create a micro-segmentation blueprint for a three-tier application spanning on-premises and cloud environments, including enforcement points and rule sets.



Capstone project

Enterprise Zero Trust Architecture

Develop a complete Zero Trust target architecture and phased roadmap for a case-study enterprise, covering identity, devices, networks, applications and data, with governance metrics, and present it to a review panel.

Certification

SAM-ZTNA

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 · Networking & Infrastructure

Where this program fits.

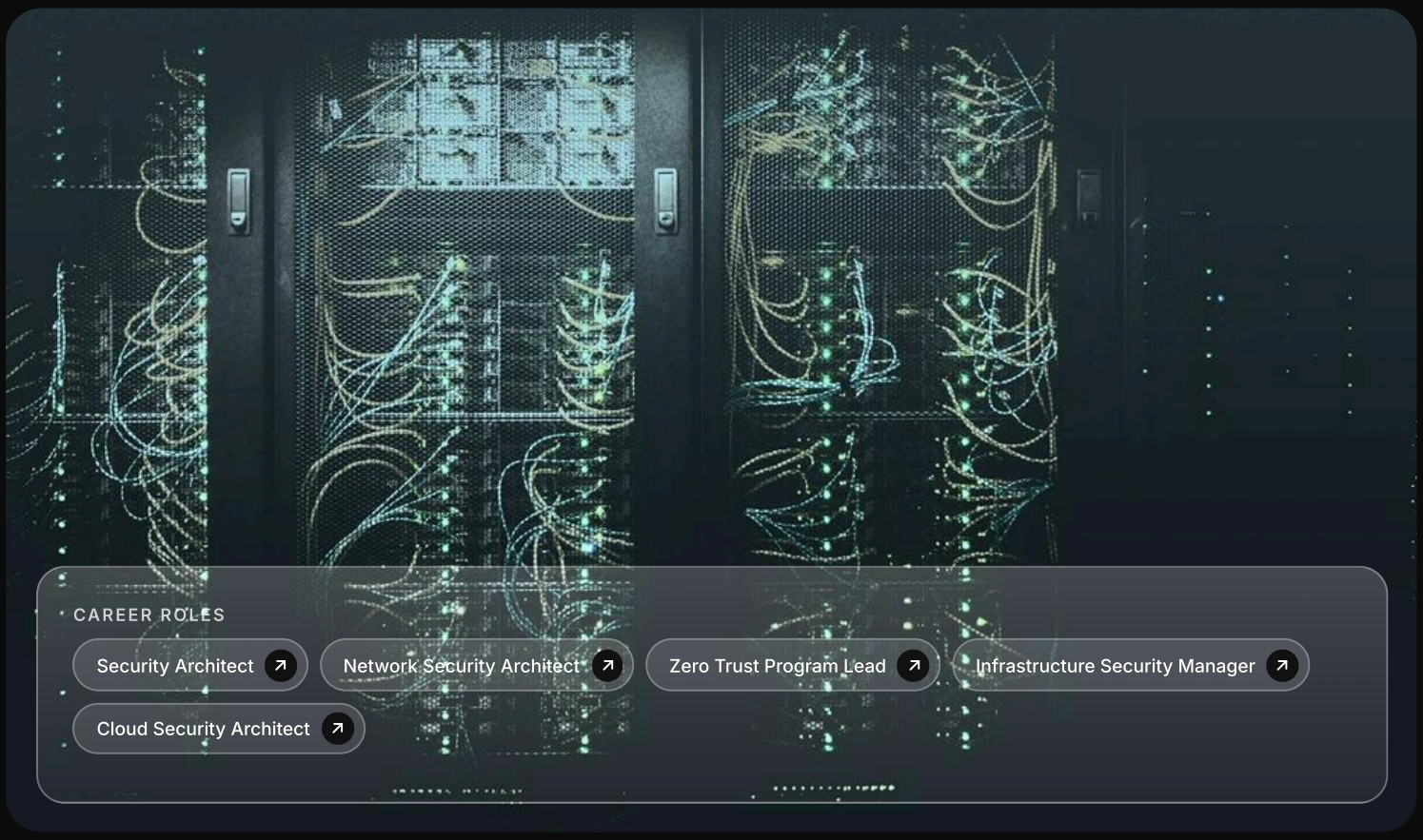
Beginner	Intermediate	Advanced	Expert
2 programs	3 programs	3 programs	You are here

Before this

Cisco CCIE Enterprise (Prep)	200 Hours
Palo Alto PCNSE Prep	72 Hours
Fortinet NSE 4–7 Track	96 Hours

Up next

The top of this pathway — explore related tracks.



CAREER ROLES

- Security Architect
- Network Security Architect
- Zero Trust Program Lead
- Infrastructure Security Manager
- Cloud Security Architect

Questions, answered.

Q01

Do I need prior experience to join?

Yes. This expert program assumes several years of networking or security experience and familiarity with identity, cloud and enterprise architecture. It focuses on architecture and strategy rather than introducing basic networking or security concepts.

Q02

How is the program delivered and scheduled?

The 48 hours program is instructor-led and delivered live virtual or blended, combining concept sessions, demonstrations and guided hands-on work. Batch timings and session frequency are confirmed with the academy team at enrollment.

Q03

Will I receive a certificate?

Yes. Participants who attend the required sessions and pass the program assessments, including practical tasks and a capstone review, receive the Samcommunity Academy SAM-ZTNA certificate for Zero Trust Network Architecture.

Q04

What labs and tools will I have access to?

Exercises use architecture case studies, design workshops and vendor-neutral tooling, with demonstrations of identity, ZTNA and segmentation platforms where available. Any required lab access or templates are shared during the program.

Q05

Is career support provided?

Yes. You receive guidance on building a portfolio from your projects, presenting skills on your resume and preparing for interviews. Career support helps you present yourself well, but job placement, interviews and salaries are not guaranteed.



Let's talk

START ZERO TRUST NETWORK ARCHITECTURE.

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