IoT Security

Secure connected devices, networks and IoT cloud platforms against real-world attacks.

DURATION	FORMAT	LEVEL	LABS
45 hours	Onsite, online or hybrid	Advanced	Cloud sandbox included

About this programme

An advanced IoT security course covering the full stack: device hardening, secure boot and firmware, cryptography and identity, network and protocol security, cloud platform controls and incident response — with threat-modelling and attack labs based on real incidents such as the Mirai botnet.

Who it is for: Security engineers, IoT developers and OT/ICS teams responsible for connected devices

What your team will be able to do

- Threat-model an IoT system across device, network and cloud layers
- Apply secure-by-design principles, secure boot and firmware update practices
- Implement cryptography, device identity and access management for IoT
- Secure MQTT/CoAP traffic and segment IoT networks
- Detect, respond to and recover from IoT security incidents

Before you start

- Networking and security fundamentals
- Some experience with embedded or connected devices

Course outline

We send the module-by-module outline with your proposal, adapted to your team's tools and goals.

Assessment and certification

How learning is checked

- A short knowledge check on day one and again at the end, so you can see each person's progress
- Graded hands-on labs in every module, reviewed by the trainer
- A final exercise that applies the programme to a problem like your team's own

Certificate and exams

- Participants who complete the programme receive a Cognitive Networks AI certificate of completion.

Formats and cohort size

- Onsite: At your office or a venue you choose, in full days.
- Online, live: Instructor-led over video, usually in half-day sessions so people can keep up with work.
- Hybrid: Some days in a room together, the rest online. Useful when a team works across cities.

Cohort size: 15 to 25 people per trainer. Larger teams run as parallel cohorts on the same outline, so everyone learns the same thing.

Pricing: We quote per cohort, based on duration, format and number of cohorts. There is no per-seat price list: tell us your team and we send a proposal within one business day.

Bring this programme to your team

Request a proposal at cognitivenetworks.ai/contact?programme=iot-security

reachus@cognitivenetworks.ai · Bangalore +91 72043 05303 · Dallas +1 (303) 827-7415