Reference: EN2/2CTD

Claroty CTD Training Course

Active Monitoring and Threat Detection for Industrial Systems

---

Duration: 5 Days | Hours: 35 h

Remote · Sessions guaranteed from 1 registrant · 60% hands-on practice

DESCRIPTION

OT (Operational Technology) environments are becoming prime targets for cyberattacks. Industrial systems, often isolated or poorly protected, require continuous monitoring to identify anomalies and limit intrusions. Companies must equip themselves with tools designed specifically for these constraints: long lifecycles, specific protocols and zero tolerance for downtime.

Claroty Continuous Threat Detection (CTD) addresses these challenges by mapping industrial assets, monitoring network traffic in real time and detecting suspicious behaviour. This training course teaches you how to detect threats, analyse abnormal behaviour and respond quickly in an industrial environment, with a hands-on approach focused on real OT and ICS infrastructures.

LEARNING OBJECTIVES

By the end of this training course, participants will be able to:

- Understand cybersecurity issues specific to industrial OT environments
- Get started with the Claroty CTD interface and its key features
- Automatically map and inventory connected assets
- Detect threats, abnormal behaviour and network intrusions
- Understand generated alerts and refine detection rules
- Integrate CTD into a SOC, SIEM or defence-in-depth strategy

PREREQUISITES

- Basic knowledge of industrial OT architectures (SCADA, PLC)
- Basic understanding of network security (firewalls, VLANs, industrial protocols)
- Experience with a monitoring tool or SIEM is appreciated

> *Because each participant is unique, a personalised interview is systematically organised in advance with our expert to design a training programme perfectly aligned with their objectives, level and professional challenges.*

TARGET AUDIENCE

OT engineers, security managers, industrial CISOs, SOC analysts and anyone involved in the cybersecurity of SCADA, PLC or DCS systems.

DETAILED PROGRAMME

> The training alternates between theoretical input and hands-on practice (approximately 60% of the time). Modules are built around practical exercises based on real-world business use cases.

Module 1 – Cybersecurity Challenges in OT Environments

- Specific characteristics of industrial threats
- OT and ICS attack surfaces
- Feedback from critical incidents and lessons learned

Module 2 – Introduction to Claroty CTD

- Architecture and network positioning
- Components and dashboard overview
- Initial indicators and operational metrics

Module 3 – Asset Discovery and Mapping

- Passive detection and automatic inventory
- Equipment classification and grouping
- Supported industrial protocols (Modbus, OPC-UA, EtherNet/IP)

Module 4 – Threat Detection and Alerts

- Behavioural analysis and signature-based alerts
- Typical scenarios: unauthorised changes, network scanning, anomalous flows
- Tuning detection rules for industrial environments

Module 5 – Response, Investigation and SIEM Integration

- Incident handling and forensic data collection
- Logging, log export and correlation with a SOC
- Custom dashboards and reporting

Module 6 – Best Practices and Feedback

- Concrete use cases from industrial deployments
- Security performance indicators
- Preparation for an inspection or cyber-industrial audit

TEACHING METHODS

Format and Delivery

The training is delivered remotely via an interactive virtual classroom. It can also be delivered on-site, with content customised to match the needs of your professional project. The theory/practice split is approximately 40%/60%.

MFE-IT Ultra-Personalised Format

Each session accommodates between 1 and 3 participants, ensuring highly individualised support. A preliminary interview allows us to tailor the content to each participant's profile. Inter-company sessions are guaranteed from just 1 registrant (except in cases of force majeure).

Skills Assessment

Throughout the training, the trainer assesses participant progress through multiple-choice questions, role-playing exercises and hands-on work. At the end, a certificate of achievement is issued to each participant.

Post-Training Support

For one month following the training, each participant can contact MFE-IT trainers with questions about implementing acquired knowledge. A response is provided by email or telephone within 48 working hours.

Accessibility

MFE-IT is committed to welcoming people with disabilities. Contact: contact@mfe-it.com.

PRACTICAL INFORMATION

Trainer Resources

- Structured demonstrations aligned with the detailed programme
- Exercise briefs and solutions throughout the training
- A ready-to-use technical environment for practical workshops
- Trainer validation of acquired knowledge at the end of each workshop
- Digital reference documents

Certification and Validation

At the end of the training, a certificate is sent by email specifying the objectives, nature, duration and assessment results. A completion certificate can also be provided on request.

Benefits for Participants

- Train from your workplace or home, with no travel required
- Benefit from an expert trainer-consultant on the subject
- Enjoy an ultra-personalised format (1 to 3 participants)
- Continue training even in the event of unforeseen circumstances

Benefits for the Organisation

- Optimise the training budget by reducing travel and accommodation costs
- Offer quality training to all employees, regardless of location
- Reduce absence time linked to travel
- Support team upskilling in all contexts