+33 (0)1 48 10 09 46
formation@ambient-it.net
140 Avenue Jean Lolive 93500 Pantin - France

Updated on 03/03/2026

Sign up

Ec-council CTIA™ Certification Training

3 days (21 hours)

Overview

The EC-Council CTIA™ training teaches you how to conduct an end-to-end cyber threat investigation: collection, analysis, correlation, and reporting. It is designed for SOC, incident response, and threat hunting environments to accelerate detection and reduce remediation time.

You will work through a structured process: scoping a case, defining hypotheses, acquiring data (logs, endpoints, network), and evidence-driven analysis. Emphasis is placed on traceability, the quality of indicators, and prioritizing actions.

This training prioritizes a hands-on approach through workshops and demos: investigating alerts, OSINT enrichment, MITRE ATT&CK mapping, and report writing. Deliverables: investigation playbooks, data collection checklists, report templates, and indicator dashboards.

Objectives

- Qualify an alert and formulate attack hypotheses.
- Collect and preserve relevant evidence (logs, memory, disk).
- Correlate multi-source events to reconstruct a timeline.
- Enrich and validate IOCs/TTPs using threat intelligence sources.
- Produce an actionable report and remediation recommendations.

Target Audience

- SOC analysts (Level 1 to Level 3)
- CERT/CSIRT Teams and Incident Response
- Security administrators / security engineers
- Technical auditors looking to enhance their investigative capabilities

Prerequisites

- Basic knowledge of TCP/IP, DNS, and HTTP/TLS networks
- Understanding of Windows and Linux logs
- Security fundamentals: authentication, privileges, malware
- Ability to read simple commands and scripts (PowerShell/Bash)

Technical prerequisites

- PC with 16 GB RAM recommended (8 GB minimum) and 40 GB of free disk space
- OS: Windows 10/11 or recent Linux (or Windows with WSL2)
- Tools: modern browser, terminal, text editor, Wireshark, Sysinternals
- Local admin access to install tools and run captures

Our EC-Council CTIA Training Program

[Day 1 - Morning]

CTIA Fundamentals and Investigation Framework

- Roles and responsibilities of the Threat Intelligence Analyst (CTI vs. SOC vs. DFIR)
- Intelligence cycle: planning, collection, processing, analysis, dissemination
- Types of threats: cybercriminals, APTs, hacktivism, insiders
- Defining the scope: objectives, constraints, classification levels, rules of engagement
- Hands-on workshop: Formalizing a CTI request (PIR) and a collection plan.

[Day 1 - Afternoon]

OSINT collection and operational hygiene

- OSINT sources: search engines, social media, code repositories, registries, forums, paste sites
- Search techniques: advanced operators, pivoting, enrichment through cross-referencing
- Identity management and compartmentalization: dedicated accounts, isolated browsing, traces, and metadata
- Validation and reliability: bias, corroboration, timestamping, evidence preservation
- Hands-on workshop: Building an OSINT checklist and collecting artifacts on a fictitious target.

[Day 2 - Morning]

Indicator analysis and standardization (IOC/TTP)

- Distinguishing between IOCs, IOAs, and TTPs and choosing the right level of granularity
- Extracting artifacts: domains, URLs, IPs, hashes, certificates, user agents, patterns
- Enrichment: WHOIS/DNS, ASN, reputation, passive DNS, infrastructure relationships
- Deduplication, scoring, and prioritization: relevance, recency, impact, confidence
- Hands-on workshop: Enrich an IOC list and produce an actionable summary.

[Day 2 - Afternoon]

Adversary modeling and attribution

- Mapping TTPs with MITRE ATT&CK (tactics, techniques, sub-techniques)
- Building an actor profile: motivations, capabilities, targeted sectors, geographies, tools
- Attribution: levels of evidence, limitations, false flags, assumptions, and uncertainties
- Producing a report: timeline, infrastructure, malware, campaigns, recommendations
- Hands-on workshop: Mapping a campaign to ATT&CK and drafting a reasoned attribution report.

[Day 3 - Morning]

CTI Standardization and Interoperability (STIX/TAXII)

- Structuring Information: Entities, Relationships, and Best Practices for Description
- Introduction to STIX 2.x: indicators, malware, threat-actor, intrusion-set, sightings
- Transport and distribution via TAXII: collections, subscriptions, access control
- Integration into the ecosystem: TIP, SIEM, SOAR, EDR (use cases and limitations)
- Hands-on workshop: Modeling a campaign in STIX and preparing a sharing package.

[Day 3 - Afternoon]

Reporting, detection, and action plan

- Deliverable formats: bulletin, alert, strategic report, actor profile, executive summary
- Translating CTI into detection: SIEM rules, queries, watchlists, YARA/Suricata (principles)
- Measuring effectiveness: KPIs/KRIs, ATT&CK coverage, false positive rates, team feedback
- Governance: source management, IOC lifecycle, retention, compliance, and confidentiality
- Hands-on workshop: Produce a comprehensive CTI report and a prioritized detection plan.

FAQ – QUESTIONS & ANSWERS

In what language is the CTIA™ training delivered?

The training is in French.

Is the exam included in the training price?

Yes, the certification fee is included in the training cost ($450 as a rough estimate). You will be able to take the exam at the end of the session.

How is the CTIA™ certification exam administered?

The exam consists of a performance-based multiple-choice test with a maximum of 50 **questions**.

It is taken online at a Pearson Vue-approved testing center.

The exam lasts **120 minutes**; the available languages are English

Relevant companies

This training is designed for both individuals and businesses—large or small—that wish to train their teams in new, advanced IT technologies or to acquire specific industry knowledge or modern methodologies.

Placement Assessment

The pre-training assessment complies with Qualiopi quality standards. Upon final registration, the learner receives a self-assessment questionnaire that allows us to evaluate their estimated proficiency in various types of technologies, as well as their expectations and personal goals for the upcoming training, within the limits imposed by the selected format. This questionnaire also allows us to anticipate certain connection or internal security issues within the company (intra-company or virtual classroom) that could pose challenges for monitoring and ensuring the smooth running of the training session.

Teaching Methods

Practical Course: 60% Practical, 40% Theory. Training materials distributed in digital format to all participants.

Organization

The course alternates between theoretical input from the trainer, supported by examples and reflection sessions, and group work.

Certification

At the end of the session, a multiple-choice quiz is used to verify that the skills have been properly acquired.

Certification

A certificate will be issued to each trainee who has completed the entire training program.