Updated on 22/08/2025

Sign up

Threat Intelligence Training

3 days (21 hours)

Presentation

Our "Threat Intelligence" training course will enable you to understand how a cyber intelligence program works, identify relevant sources, process indicators of compromise (IOCs) and automate processes using Artificial Intelligence.

You will be able to set up and integrate a CTI cell into an SOC, use OSINT tools, structure an intelligence flow, or produce reports for analysts, IT teams or decision-makers. The focus will be on transforming raw data into actionable intelligence for detection, incident response and strategic decision-making.

Threat Intelligence integrates with existing security architecture, strengthening threat detection, incident response and proactive threat hunting. Thanks to AI, you can automate monitoring, prioritize alerts and improve response time. You'll also learn how to define CTI governance (workflow, roles, responsibilities) to ensure effective and appropriate dissemination of intelligence throughout the organization.

Following our training, you will be able to set up a threat intelligence service, exploit the data in your business environment, and use the appropriate tools (MISP, MITRE frameworks, OSINT flows, etc.).

Objectives

- Understand the fundamentals of Cyber Threat Intelligence
- Know how to collect and analyze threat information
- Use artificial intelligence to automate the collection, analysis and correlation of threat-related information
- Transform data into actionable intelligence
- Integrate CTI tools and methods into your organization's security process

Target audience

- CISOS
- SOC Manager
- SOC Analyst
- Cybersecurity consultant
- Anyone in charge of the security of a corporate information system

Prerequisites

- Basic knowledge of information systems and cybersecurity.

Cyber Threat Intelligence (CTI) Training - Collection, Analysis & Automation OSINT

[Day 1 - Morning]

CTI fundamentals & framework

- Intelligence cycle: planning ? collection ? analysis ? dissemination ? feedback
- CTI typology: strategic, tactical, operational, technical
- Organizational stakes of CTI (place in a cybersecurity strategy, RSSI/DPO/DIRCOM relations).
- Use cases by target profile: CISO (management), SOC (detection), IR (response).
- Threats, motivations and attack surfaces (APT, cybercrime, hacktivism, etc.).
- Formats & vocabulary: IOC/IOA, TTP, MITRE ATT&CK, kill chain, STIX/TAXII (intro)
- Practical workshop: Analysis of a recent cyberattack ? extraction of useful CTI elements

[Day 1 - Afternoon]

Information gathering - Conventional methods

- Source mapping: open (official sites, CERT, blogs, RSS), industry communities, editor reports, internal logs
- Manual monitoring techniques: query plan, advanced operators, RSS/newsletter monitoring, authenticity check
- Quality criteria: reliability, freshness, relevance, bias, sector coverage
- Collection log & traceability (chain of custody, source citation)
- Practical workshop: Building a collection plan + source evaluation grid (quality score)

[Day 2 - Morning]

Collect, sort & qualify (conventional approach)

- Manual multi-format ingestion (CSV/JSON/PDF/web) and basic normalization
- Cleansing: deduplication, entity disambiguation, simple enrichments (WHOIS, GeoIP, ASN, public reputation)
- Qualification: source & indicator scoring (trust, context, sector, temporality)
- Pre-structuring to STIX "light" (simple objects: indicator, malware, relationship)
- Practical workshop: Cleaning and qualifying a batch of IOCs from several streams

[Day 2 - Afternoon]

Analyze & correlate (conventional approach)

- Pivoting & links: domains ? IP ? hash ? infra, timeline construction
- MITRE ATT&CK & kill chain mapping to identify dominant TTPs
- Detection of recurring patterns (campaigns, infra providers, hours of activity)
- Restitution: analyst report (technical) vs. executive brief (decision-making)
- AI applied to correlation and detection of recurring patterns (clustering, automatic scoring of IOCs with LLM/ML).
- Demonstration of an open source tool or AI sandbox applied to CTI.
- Practical workshop: Multi-source correlation + drafting of an actionable one-pager.

[Day 3 - Morning]

AI-enhanced collection & analysis (OSINT + automated correlation)

- Automated OSINT pipelines: enriched RSS, compliant crawlers/scrapers, public APIs
- Reasoned use of AI/LLM: thematic classification, deduplication, IOC extraction, summarization and contextual correlation (no predictive analysis)
- STIX/TAXII connectors: standardized packaging & exchange of collected indicators
- Governance & compliance: legal limits, RGPD, TOU, bias reduction, human validation
- Practical workshop: Setting up a mini-pipeline (public streams) ? extraction, deduplication, summarization & "light" STIX export

[Day 3 - Afternoon]

Operational integration

- TIP/MISP: import, deconfliction, scoring, controlled sharing
- SIEM/SOAR: transforming intelligence into use cases (rules, alerts, playbooks)
- CTI-guided threat hunting & enrichment of IR investigations
- Measurement & monitoring: CTI KPI/KRI (false positive rate, MTTD/MTTR, ATT&CK coverage), improvement loop
- Setting up a complete CTI service
- Practical workshop: Designing a CTI mini-service (workflow collection ? validation ? dissemination ? action, RACI matrix, internal/external dissemination plan)

Deliverables & assets

- Conventional collection plan + source scoring grid
- Set of cleaned & qualified IOCs + "light" STIX mini-taxonomy
- Executive one-pager and analyst report
- OSINT auto pipeline (AI collection + sorting + summarization + correlation) + STIX export
- SIEM/SOAR use cases, response playbook, CTI management KPIs
- CTI usage charter, RACI matrix and CTI service implementation plan (end-of-training summary document)

Companies concerned

This course is aimed at both individuals and companies, large or small, wishing to train their teams in a new advanced IT technology, or to acquire specific business knowledge or modern methods.

Positioning on entry to training

Positioning at the start of training complies with Qualiopi quality criteria. As soon as registration is finalized, the learner receives a self-assessment questionnaire enabling us to assess his or her estimated level of proficiency in different types of technology, as well as his or her expectations and personal objectives for the forthcoming course, within the limits imposed by the selected format. This questionnaire also enables us to anticipate any connection or security difficulties within the company (intra-company or virtual classroom) which could be problematic for the follow-up and smooth running of the training session.

Teaching methods

Practical training: 60% hands-on, 40% theory. Training material distributed in digital format to all participants.

Organization

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

Validation

At the end of the session, a multiple-choice questionnaire verifies the correct acquisition of skills.

Certification

A certificate will be awarded to each trainee who has completed the entire course.