



# **Advanced Cyber Threat Intelligence and Response Training Course**

8 – 12 August 2027  
Chicago



## Advanced Cyber Threat Intelligence and Response Training Course

**Ref:** 748\_157043 **Date:** 8 – 12 August 2027 **Location:** Chicago **Fees:** 12000 Euro

### Overview

Advanced Cyber Threat Intelligence and Response Training Course is a five-day advanced course for intelligence analysts, SOC teams, incident responders, security-operations leaders, risk specialists, and technical managers who leave with a Cyber Threat Intelligence Response Playbook. Participants apply intelligence requirements management, source reliability evaluation, MITRE ATT&CK adversary mapping, STIX and TAXII intelligence exchange, and TLP 2.0 sharing controls to prioritize detection and enrich incident decisions. Agile Leaders Training Center develops operational cyber threat intelligence.

### Who Should Attend

- Threat-intelligence functions responsible for collection, analysis, and production
- SOC teams responsible for detection priorities and alert enrichment
- Incident-response teams responsible for triage, scope, and defensive action
- Security-operations leaders responsible for intelligence platforms and workflows
- Risk and technical-management functions responsible for threat-informed decisions

The course assumes participants work with security alerts, threat reports, or incident cases and leaves out introductory cybersecurity, malware reverse engineering, forensic acquisition, penetration testing, and certification preparation.

### Departments and Industries

The course supports departments and industries that need evaluated threat information converted into timely defensive decisions.

- Security operations and threat intelligence
- Incident response and cyber-risk functions
- Financial services and telecommunications
- Healthcare and digital-service organizations
- Industrial, logistics, and professional-service operations

### Learning Objectives

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



- Build intelligence requirements and collection plans
- Evaluate source reliability and information credibility
- Analyze actors, campaigns, indicators, and observables
- Apply MITRE ATT&CK to detection and response priorities
- Use STIX, TAXII, and TLP 2.0 for controlled sharing
- Build a Cyber Threat Intelligence Response Playbook

## **Course Agenda**

### **Day 1: Intelligence Direction and Collection**

- Priority Intelligence Requirements Register
- Intelligence Consumer and Decision Map
- Collection Source Coverage Plan
- Source Reliability and Credibility Matrix
- Intelligence Gap and Collection Task Board

### **Day 2: Threat Analysis and Adversary Mapping**

- Threat Actor and Campaign Analysis Profile
- Indicator and Observable Validation Checklist
- MITRE ATT&CK Tactic and Technique Map
- Competing Hypotheses Analysis Matrix
- Intelligence Confidence and Assumption Record

### **Day 3: Structuring and Sharing Intelligence**

- STIX 2.1 Object and Relationship Model
- TAXII 2.1 Collection Exchange Workflow
- TLP 2.0 Information Handling Matrix
- Threat Intelligence Platform Data Quality Rules
- Intelligence Dissemination and Feedback Plan

### **Day 4: Detection and Incident Response Integration**

- Threat-Informed Detection Use-Case Backlog
- Alert Enrichment and Triage Worksheet
- Incident Scope and Attribution Evidence Map
- Response Priority and Action Matrix
- Operational and Executive Intelligence Report



## Day 5: Intelligence-to-Response Practice

- Exercise: Define Requirements and Evaluate Sources
- Exercise: Map a Campaign with MITRE ATT&CK
- Exercise: Structure and Mark Intelligence for Sharing
- Exercise: Enrich an Incident and Prioritize Response
- Capstone: Cyber Threat Intelligence Response Playbook

## Practical Exercises

The course uses suggested activities drawn from financial services, telecommunications, healthcare, industrial operations, logistics, and digital services.

- Suggested activity: define intelligence requirements and compare source reliability, credibility, and coverage.
- Suggested activity: analyze an adversary campaign and map observed behavior to MITRE ATT&CK.
- Suggested activity: structure intelligence relationships, apply handling markings, and design an exchange workflow.
- Suggested activity: enrich an incident case, prioritize detection actions, and prepare consumer-specific reporting.

## FAQs

### Who suits advanced cyber threat intelligence and response training, and what does it assume?

Threat-intelligence, SOC, incident-response, security-operations, risk, and technical-management functions suit the training; it assumes participants work with alerts, threat reports, or incident cases.

### How does cyber threat intelligence differ from general incident-response training?

Cyber threat intelligence focuses on requirements, collection, source evaluation, adversary analysis, structured exchange, and decision support, while incident-response training concentrates on managing the incident lifecycle.

### How should teams evaluate cyber threat intelligence sources?

Teams should separately assess source reliability, information credibility, relevance, timeliness, corroboration, collection bias, confidence, and the decision the intelligence must support.

### How can MITRE ATT&CK improve threat-informed response?

MITRE ATT&CK improves response by organizing observed adversary behavior into tactics and techniques that teams can connect to evidence, detection gaps, investigation priorities, and defensive actions.



## **What belongs in a Cyber Threat Intelligence Response Playbook?**

A Cyber Threat Intelligence Response Playbook includes requirements, consumers, sources, validation rules, analysis methods, ATT&CK mappings, sharing controls, detection use cases, enrichment steps, priorities, reports, feedback, and owners.

## **Conclusion**

Participants take back a Cyber Threat Intelligence Response Playbook supported by requirement registers, source matrices, ATT&CK maps, exchange workflows, sharing controls, enrichment worksheets, and reporting artifacts. It changes disconnected threat feeds into evaluated intelligence tied to detection and incident decisions. The playbook provides a repeatable basis for prioritization, controlled sharing, response coordination, and improvement.