



Threat Intelligence Requirements and Production Practice Course

Threat Intelligence Requirements and Production Practice Course

Overview

Cyber Threat Intelligence Operations and Analysis Training Course is a ten-day intermediate course for intelligence analysts, SOC teams, threat hunters, incident responders, security researchers, and intelligence coordinators who leave with a Cyber Threat Intelligence Operations Portfolio. Participants connect intelligence requirements, collection planning, source evaluation, structured analysis, operational use, dissemination, feedback, and lifecycle improvement. Agile Leaders Training Center develops cyber threat intelligence operations and analysis practice.

Who Should Attend

- Intelligence functions responsible for requirements, collection, analysis, and production
- Security operations functions responsible for consuming and applying threat intelligence
- Threat hunting functions responsible for hypothesis development and evidence searches
- Incident response functions responsible for adversary context and investigative support
- Security research functions responsible for evaluating sources and adversary activity

The course assumes participants work with security events, threat reports, investigations, or intelligence requests, and leaves out platform administration, malware reverse engineering, offensive exploitation, certification preparation, and exam coaching.

Departments and Industries

The course supports departments and industries that produce or use cyber threat intelligence.

- Cyber threat intelligence and security operations
- Incident response and threat hunting
- Risk management and security architecture
- Financial services and telecommunications
- Healthcare, energy, industrial operations, and digital services

Learning Objectives

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



- Apply intelligence requirements and collection planning to stakeholder needs
- Evaluate source reliability, information credibility, and handling constraints
- Analyze indicators, adversary behavior, and competing hypotheses
- Build intelligence products for SOC, threat hunting, and incident response
- Prioritize dissemination, feedback, and lifecycle improvement actions
- Build a Cyber Threat Intelligence Operations Portfolio

Course Agenda

Day 1: Frame Intelligence Operations

- Cyber Threat Intelligence Lifecycle Operating Model
- Strategic, Operational, Tactical, and Technical Intelligence Map
- Stakeholder Decision and Intelligence Consumer Register
- Intelligence Requirement Statement Template
- Priority Intelligence Requirements Governance Board

Day 2: Plan Collection

- Collection Requirement and Gap Matrix
- Internal Telemetry and External Source Inventory
- Collection Source Selection Decision Tree
- Legal, Ethical, and Handling Constraint Checklist
- Collection Plan Coverage Dashboard

Day 3: Evaluate Sources

- Source Reliability and Information Credibility Matrix
- Indicator Provenance and Confidence Record
- Duplicate, Stale, and Conflicting Data Filter
- Threat Feed Relevance Scoring Method
- Collection Bias and Blind-Spot Review

Day 4: Process Threat Data

- Indicator Normalization and Enrichment Worksheet
- Adversary Entity and Infrastructure Relationship Map
- Tactic, Technique, and Procedure Extraction Method
- Event Timeline and Campaign Clustering Board
- Evidence Traceability and Analytic Notebook



Day 5: Apply Structured Analysis

- Analysis of Competing Hypotheses Matrix
- Key Assumptions Check and Challenge Session
- Indicators, Signposts, and Warning Register
- Confidence Language and Judgment Calibration Guide
- Alternative Futures and Scenario Comparison

Day 6: Analyze Adversaries

- MITRE ATT&CK Behavior Mapping Worksheet
- Diamond Model Intrusion Analysis Canvas
- Adversary Motivation, Capability, and Opportunity Profile
- Campaign Pattern and Infrastructure Pivot Map
- Threat Actor Assessment and Confidence Statement

Day 7: Operationalize Intelligence

- SOC Detection Use-Case Translation Sheet
- Threat Hunting Hypothesis and Query Brief
- Incident Response Intelligence Support Card
- Risk Scenario and Control Decision Linkage
- Operational Intelligence Action Tracker

Day 8: Produce Intelligence

- Intelligence Product Type Selection Matrix
- Executive Threat Brief Structure
- Analyst Report Evidence and Judgment Pattern
- Visual Threat Narrative and Relationship Diagram
- Peer Review and Analytic Tradecraft Checklist

Day 9: Disseminate and Improve

- Audience, Channel, and Handling Distribution Matrix
- Stakeholder Briefing and Question Log
- Intelligence Feedback and Utility Scorecard
- Requirement Closure and Reprioritization Method
- CTI Capability Maturity Improvement Backlog



Day 10: Practice CTI Operations

- Exercise: Convert Stakeholder Needs into Intelligence Requirements
- Exercise: Evaluate Sources and Correlate Threat Evidence
- Exercise: Test Competing Hypotheses and State Confidence
- Exercise: Brief SOC and Threat Hunting Consumers
- Capstone: Cyber Threat Intelligence Operations Portfolio

Practical Exercises

The course uses suggested activities based on financial services, telecommunications, healthcare, energy, and digital services.

- Suggested activity: convert a stakeholder decision into priority intelligence requirements and a collection plan.
- Suggested activity: evaluate conflicting sources, normalize indicators, and document confidence and provenance.
- Suggested activity: map adversary behavior, compare hypotheses, and prepare intelligence for SOC and threat hunting use.
- Suggested activity: deliver a stakeholder briefing, capture feedback, and update the lifecycle improvement backlog.

FAQs

Who suits cyber threat intelligence operations training, and what does it assume?

Intelligence, SOC, threat hunting, incident response, security research, and coordination functions suit the course; it assumes work with security events, threat reports, investigations, or intelligence requests.

How does cyber threat intelligence analysis differ from threat hunting training?

Cyber threat intelligence analysis develops requirements, evaluates sources, produces judgments, and disseminates products, while threat hunting training searches environments for evidence of suspected adversary behavior.

How should cyber threat intelligence requirements be written?

Cyber threat intelligence requirements should connect a stakeholder decision to a defined question, scope, priority, collection need, delivery timing, handling rule, and success measure.

What makes a cyber threat intelligence product actionable?

An actionable product identifies the decision, evidence, judgment, confidence, affected context, implications, recommended action, handling constraints, and feedback route for its intended consumer.



How is cyber threat intelligence quality improved?

Quality improves through source evaluation, provenance, structured analysis, peer review, calibrated confidence, consumer feedback, utility measurement, and regular reprioritization of intelligence requirements.

Conclusion

Participants take back a Cyber Threat Intelligence Operations Portfolio connecting requirements, collection, analysis, production, dissemination, and feedback. It changes disconnected threat data into a governed intelligence workflow serving operational and management decisions. The portfolio supports traceable judgments, clearer consumer briefings, measured utility, and continual lifecycle improvement.



Training Course Categories

Agile PM and Project Management Training Courses

Agribusiness & Food Security Training Courses

Certified Courses By International Bodies

Communication and Public Relations Training Courses

Crisis Management and Business Continuity Training Courses

Data Analytics Training and Data Science Courses

Digital Government & Public Service Training Courses

Education and Learning Development Training Courses

Environment & Sustainability Training Courses

Facilities and Real Estate Training Courses

Finance and Accounting Training Courses

Governance, Risk and Compliance Training Courses

Healthcare Management Training Courses

Heritage Conservation and Museum Management Training Courses

Hospitality and Tourism Training Courses

Human Resources Training and Development Courses

IT Security Training & IT Training Courses

Leadership and Management Training Courses

Legal Training, Procurement and Contracting Courses

Maintenance Training and Engineering Training Courses

Marketing, Customer Relations, and Sales Courses

NGO, Humanitarian and Development Management Training Courses

Occupational Health, Safety and Security Training Courses

Oil & Gas Training and Other Technical Courses

Personal & Self-Development Training Courses

Quality and Operations Management Training Courses



Training Course Categories

Secretarial and Administration Training Courses

Shipping, Maritime and Ports Training Courses



Training Cities

Abu Dhabi UAE	Accra Ghana	Amman Jordan
Amsterdam Netherlands	Athens Greece	Baku Azerbaijan
Bali Indonesia	Bangkok Thailand	Barcelona Spain
Berlin Germany	Cairo Egypt	Cape town South Africa
Casablanca Morocco	Chicago USA	Doha Qatar
Dubai UAE	Frankfurt Germany	Geneva Switzerland
Istanbul Turkey	Jakarta Indonesia	Johannesburg South Africa
Kuala Lumpur Malaysia	Kuwait Kuwait	Langkawi Malaysia
Lisbon Portugal	London UK	Madrid Spain
Manama Bahrain	Marbella Spain	Milan Italy
Montreux Switzerland	Munich Germany	Muscat Oman
Nairobi Kenya	New York USA	Nice France

Training Cities

Paris

France

Phuket

Thailand

Port Louis

Mauritius

Porto

Portugal

Prague

Czech Republic

Rome

Italy

San Diego

USA

Seoul

South Korea

Sharm El-Sheikh

Egypt

Singapore

Singapore

Tashkent

Uzbekistan

Tbilisi

Georgia

Tokyo

Japan

Toronto

Canada

Trabzon

Turkey

Vienna

Austria

Zanzibar

Tanzania

Zoom

Online Training

Zurich

Switzerland