CONCEPT

Cyber Threat Intelligence (CTI): Intelligence Requirements, Analysis and Operationalisation

Cyber Threat Intelligence (CTI): Intelligence Requirements, Analysis and Operationalisation

Introduction:

Cyber threat intelligence CTI teams often collect far more feeds, indicators and vendor reports than anyone uses, because no one has agreed which decisions the intelligence must support. Analysts then publish long reports that executives skim and detection engineers cannot act on. This Core Concept course builds a requirements-led CTI practice: stakeholder questions turned into priority intelligence requirements, adversary behaviour profiled and mapped to MITRE ATT&CK, judgements tested against analyst bias, and products written for each audience. Participants produce a Threat Intelligence Requirements and Reporting Pack for their own organisation.

Course Objectives:

- Define priority intelligence requirements with stakeholders and plan collection against them across the intelligence cycle
- Build threat actor profiles that record motivation, targeting, capability and observed behaviour mapped to MITRE ATT&CK
- Assess indicators and TTPs for relevance, confidence and shelf life before they are passed to detection teams
- Apply structured analytic techniques such as Analysis of Competing Hypotheses to test judgements and reduce analyst bias
- Share and receive intelligence through a threat intelligence platform using STIX, TAXII and TLP handling rules
- Write strategic, operational and tactical intelligence products and measure the value the CTI programme delivers

Target Audience:

- Analysts responsible for collecting, assessing and reporting cyber threat intelligence
- SOC analysts who turn intelligence into detection content and alert context
- Security risk analysts who feed threat likelihood into risk assessments
- Analysts who maintain threat intelligence platforms and sharing community memberships
- Vulnerability management analysts who prioritise remediation using threat activity

Course Outline:

Day 1: CTI Purpose, Levels and Programme Baseline

- Strategic, Operational and Tactical Intelligence: Audiences and Decisions Supported
- Data, Information and Intelligence Distinction with Worked Examples
- CTI Stakeholder Map: SOC, Risk, Vulnerability Management and Leadership Consumers
- Internal Telemetry, Vendor Feeds, Sharing Communities and Open Sources Inventory
- CTI Programme Baseline Self-Assessment Worksheet

Day 2: Intelligence Cycle, Requirements and Adversary Models

- Five-Phase Intelligence Cycle: Planning and Direction to Dissemination and Feedback
- Priority Intelligence Requirements and Stakeholder Interview Template
- Collection Management Plan Linking Requirements to Sources
- MITRE ATT&CK as a Common Language for Adversary Behaviour
- Diamond Model and Cyber Kill Chain for Structuring Intrusion Activity

Day 3: Threat Actor Profiling, Indicators and TTP Analysis

- Threat Actor Profile Template: Motivation, Targeting, Capability and Infrastructure
- ATT&CK Technique Mapping of Vendor and Community Threat Reports
- Indicator Assessment: Relevance, Confidence, Context and Expiry
- Source Reliability and Information Credibility Rating in Analytic Records
- Threat Landscape Heatmap for the Organisation's Sector and Technology Stack

Day 4: Analytic Rigour, Sharing Standards and Operationalisation

- Analysis of Competing Hypotheses Matrix and Sensitivity Check
- Cognitive Bias Checklist: Confirmation, Anchoring and Mirror Imaging
- Threat Intelligence Platform Functions: Ingestion, Deduplication, Enrichment and Scoring
- STIX 2.1 Objects, TAXII 2.1 Collections and TLP 2.0 Handling Labels at Overview
- ATT&CK Coverage Gap Analysis as an Input to Detection and Hunting Backlogs

Day 5: Intelligence Products and the Requirements and Reporting Pack

- Estimative Language and Confidence Statements in Written Assessments
- Guided Case: Sector-Targeting Campaign Assessment for Operational Consumers
- Executive Threat Briefing: One-Page Strategic Summary and Decision Points
- CTI Programme Value Measures: Requirement Coverage, Consumer Feedback and Action Taken
- Threat Intelligence Requirements and Reporting Pack Review Panel

Skills You Will Gain:

- Intelligence Requirements Management
- Collection Planning
- Threat Actor Profiling
- ATT&CK Technique Mapping
- Indicator Quality Assessment
- Structured Analytic Techniques
- Intelligence Report Writing
- CTI Programme Measurement

Why Attend This Course:

- Return with a Threat Intelligence Requirements and Reporting Pack built around the questions your own stakeholders ask
- Cut the volume of unused feeds by tying every collection source to a named requirement
- Give detection teams ATT&CK-mapped behaviour and gap lists they can act on, not raw indicator dumps
- Compare analytic and reporting practice with analysts from banking, energy, telecoms, government and healthcare

Conclusion:

Threat intelligence earns its budget only when it answers questions that defenders and decision makers actually have. The course moves from CTI levels and stakeholder needs, through the intelligence cycle, requirements and adversary models, to actor profiling, ATT&CK mapping and indicator assessment, then to structured analysis, sharing standards and detection inputs. The final day applies that method to case material and produces a Threat Intelligence Requirements and Reporting Pack with products for executive, operational and technical readers.