CA303: Cyber Threat Intelligence

25 Instructional Hours 38 CPEs 13 Labs

LIVE ONLINE OR ON-DEMAND ACCESS OR IN PERSON

INTERMEDIATE

This course provides a comprehensive exploration of Threat Intelligence (CTI) and Open-Source Intelligence (OSINT), focusing on how organizations collect, analyze, and operationalize intelligence to defend against evolving cyber threats. It covers the full intelligence lifecycle, threat actor profiling, malware analysis, and the integration of intelligence into security operations. Learners will gain both foundational knowledge and advanced insights into frameworks such as MITRE ATT&CK and the Cyber Kill Chain, along with practical techniques for intelligence-driven defense, threat hunting, and OSINT investigations. The course emphasizes actionable intelligence, real-world use cases, and the importance of context, relevance, and operational application in modern cybersecurity environments.

You Will Be Able To

- Apply the threat intelligence lifecycle to transform raw data into actionable intelligence
- Analyze and profile threat actors based on motivations, tactics, and behavior
- Conduct malware analysis using static, dynamic, and behavioral techniques
- Integrate threat intelligence into SOC workflows, SIEM, and incident response processes
- Perform OSINT investigations using structured methodologies and validated sources
- Develop intelligence-driven detection and response strategies aligned with real-world threats

Who Should Attend

This course is designed for cybersecurity professionals, analysts, and students who want to build or enhance their skills in threat intelligence and OSINT. It is suitable for individuals working in security operations, incident response, or threat hunting, as well as those interested in digital investigations and cyber defense. The course is also valuable for professionals seeking to transition into intelligence-focused roles, as it combines both technical and analytical perspectives with practical applications.

Relevant Combat Roles

- Threat Intelligence Analyst
- Incident Responder / DFIR Specialist
- Threat Hunter
- Cybersecurity Analyst
- Vulnerability Management Specialist

Topics Covered

Threat intelligence fundamentals – lifecycle, workflows, and types (tactical, operational, strategic)

Threat actors & context – motivations, categories, and real-world case studies

Malware analysis basics – common types and intro to analysis techniques

Applying intelligence in security – SIEM/SOAR use, MITRE ATT&CK, and threat hunting

OSINT methods & tools – data collection, verification, and online investigations

Labs

Malware Analysis & Sandbox Investigation (static/dynamic malware analysis, sandbox behavior analysis, and IOC identification)

Threat Detection & MITRE ATT&CK Mapping (MITRE ATT&CK mapping, SIEM detection rules, and threat behavior analysis)

OSINT Investigation & Digital Footprint Analysis (social media investigations, public data analysis, and digital footprint validation)

Threat Intelligence Operations & SOC Enrichment (alert enrichment, intelligence-driven incident prioritization, and SOC threat analysis)