Certified CTI Analyst Program

The objective of this program is to prepare learners to work in cyber threat intelligence by building practical skills in threat research, malware analysis, infrastructure hunting, and AI-driven threat detection. Through hands-on labs and real-world case studies, participants learn how to identify threat actors, analyze indicators of compromise, and produce actionable intelligence to support security operations and decision-making.

100 HOURS | <DATE> | FULLY ONLINE

- Provides practical training in cyber threat intelligence and threat hunting.
- Covers threat intelligence, malware analysis, and infrastructure investigation.
- Includes hands-on labs, case studies, and applied certification exams.
- Explores threat hunting in on-premises and cloud environments.
- Introduces AI automation for intelligence and threat hunting.
- Designed to build job-ready skills for cyber threat intelligence roles.

TARGET AUDIENCE

- SOC Analysts and Cybersecurity Analysts
- Threat Hunters and Incident Responders
- Security professionals moving into CTI roles
- Professionals with SOC or threat analysis experience
- Anyone interested in cyber threat intelligence

THE INSTRUCTOR

This program is delivered through a dedicated learning platform and supported by experienced instructors with strong backgrounds in cybersecurity, IT systems, and digital technologies.

The training combines guided instruction, hands-on labs, case studies, and applied assessments to help participants build practical skills and prepare for certification.

ABOUT ECS ETHIOPIA

ECS Ethiopia is a technology-driven company working with government bodies, municipalities, and large corporations to bring advanced global solutions to Ethiopia. As part of the ECS Group (UK), we help finance and execute major projects while fostering strong partnerships and innovation across the country.

GLOBAL TRAINING PARTNERSHIPS

Our training programs and learning platform were developed in close collaboration with leading international training organisations. Thousands of professionals worldwide have successfully completed these programs using this training content and learning system.

THREAT INTELLIGENCE FOUNDATIONS COURSE

This course provides a practical foundation in cybersecurity defense covering network security, operating system protection and SOC operations. You will explore how modern organizations detect and respond to threats using industry frameworks, secure architectures and endpoint defense.

MODULE 1

INTRODUCTIONS TO CYBERSECURITY THREAT INTELLIGENCE (CTI)

This module introduces learners to the foundational principles and purpose of Cyber Threat Intelligence (CTI). Learners explore how intelligence supports proactive defense by examining the CTI lifecycle, threat actor behaviors, and attribution techniques. Through applied examples, they learn how intelligence gathering transforms raw data into actionable insights for anticipating and mitigating cyber threats.

Topics Covered:

- Cyber Threat Intelligence
- Introduction to Threat Intelligence
- Threat Intelligence Lifecycle
- Threat Actor Profiling and Attribution

MODULE 2

THREAT INTEL PLATFORMS

Learners are introduced to the key tools, feeds, and frameworks used to collect, organize, and analyze threat intelligence. The module explores CTI platforms, structured analytical models, and industry frameworks such as MITRE ATT&CK and MITRE D3FEND. Through practical exercises, learners gain experience in mapping adversary behaviors, developing threat profiles, and leveraging intelligence data to support security operations.

Topics Covered:

- CTI Feeds and Platforms
- Analytical Models & Frameworks
- MITRE ATT&CK Framework
- MITRE D3FEND Framework
- Threat Actor Profiling (APT Intelligence)

MODULE 3

MALWARE AND INFRASTRUCTURE ANALYSIS

This module focuses on analyzing indicators of compromise (IOCs), malware behavior, and adversary infrastructure to strengthen intelligence-driven defense strategies. Learners dive deeper into YARA rule creation, malware investigation workflows, and intelligence reporting techniques. Hands-on labs reinforce how to identify, classify, and interpret threat artifacts to support attribution and inform defensive actions.

Topics Covered:

- IOC Fundamentals Recap
- YARA Deep Dive
- YARA in Intelligence Workflows
- Malware Investigation & Analysis

MODULE 04

CLOSURE & CERTIFICATION

Course wrap-up and exam readiness.

LABS

- Building a Profile using OSINT
- Creating a Profile from a Case Study
- Collecting Cyber Threat Intelligence
- Creating an APT Research
- Creating YARA Rules
- Malware Sample Analysis

CASE STUDY

Case Study: Volt Typhoon

INFRASTRUCTURE THREAT HUNTING COURSE

This course provides practical training in infrastructure threat hunting, covering threat hunting methods, advanced persistent threats, and cloud-based detection strategies. You will learn how to collect and analyze data, investigate attacker techniques, and uncover hidden threats across on-premises and cloud environments.

MODULE 1

THREAT HUNTING METHODS

This module introduces the core concepts, frameworks, and methodologies that define modern threat hunting. Learners explore how to form hypotheses, collect and manage hunt data, and leverage analytical tools to identify anomalies and adversary activity. Through applied exercises, learners gain a structured understanding of how proactive threat hunting complements traditional SOC monitoring and strengthens organizational defense.

Topics Covered:

- Introduction to Threat Hunting
- Threat Hunting Team and Process
- Hypotheses for Threat Hunting
- Data Collection and Management
- Tools for Threat Hunting

MODULE 2

THREAT INTELLIGENCE AND APTS

Learners examine how threat intelligence informs and enhances hunting operations, with a focus on identifying advanced persistent threats (APTs) and complex attack patterns. The module covers endpoint hunting, command-and-control (C2) detection, honeypot utilization, and behavioral analytics through UEBA. Learners develop the ability to detect, analyze, and correlate indicators of compromise across diverse infrastructure environments.

Topics Covered:

- Endpoint Threat Hunting
- Threat Hunting and Detection Strategies
- C2 Communication
- Honeypots
- User and Entity Behavior Analytics (UEBA)

MODULE 3

CLOUD HUNTING AND DETECTION STRATEGIES

This module expands threat hunting practices into cloud-based ecosystems. Learners explore tools and visualization techniques for identifying malicious activity across virtualized and hybrid environments. Through hands-on scenarios, learners apply cloud-specific detection strategies to uncover hidden threats, monitor behavioral anomalies, and enhance visibility within cloud infrastructure.

Topics Covered:

- Threat Hunting and the Cloud
- Cloud Threat Hunting Tools
- The Power of Visualization

MODULE 04

CLOSURE & CERTIFICATION

Course wrap-up and exam readiness.

LABS

- Setting Up ELK for Data Collection
- Elastic Investigation
- Persistency Techniques Investigation
- Endpoint Hunt with Velociraptor
- Command and Control with Mythic
- DNS Tunneling Investigation
- Setting Up a Honeypot

CASE STUDY

- Case Study: Microsoft Teams Phishing and Quick Assist Abuse (2024)
- Case Study: Hunting Using Honeypots

STRATEGIC THREAT HUNTING AI AUTOMATION COURSE

This course provides practical training in strategic threat hunting with AI automation, covering the threat hunting maturity model, AI-driven threat intelligence, and AI-powered hunting techniques. You will learn to assess organizational maturity, integrate automation into intelligence workflows, and apply AI to scale detection and accelerate threat response.

MODULE 1

THREAT HUNTING MATURITY MODEL

This module explores the frameworks and stages that define an organization's threat hunting maturity. Learners examine how hunting capabilities evolve from reactive detection to proactive intelligence-led operations. Through adversary simulation exercises, learners gain insight into how mature hunting programs anticipate attacker behavior, refine detection strategies, and continuously improve through feedback and iteration.

Topics Covered:

- The Maturity Model and Stages
- Advancing in the Maturity Model
- Adversary Simulation

MODULE 2

AI AUTOMATION FOR THREAT INTELLIGENCE

Learners are introduced to how artificial intelligence transforms the collection, enrichment, and analysis of threat intelligence. The module covers AI foundations, automated data aggregation, and IOC enrichment to enhance decision-making speed and accuracy. Learners apply AI-driven workflows to streamline intelligence processes and improve visibility across dynamic threat landscapes.

Topics Covered:

- AI Foundations for TI
- Automated Data Collection & IOC Enrichment
- AI-Enabled TI Workflows

MODULE 3

AI AUTOMATION FOR THREAT HUNTING

This module focuses on the integration of AI and machine learning into proactive threat hunting operations. Learners explore techniques for anomaly detection, UEBA, and orchestration through AI-enhanced workflows. Emphasis is placed on the collaboration between human analysts and AI systems, enabling scalable, adaptive, and continuous hunting practices that strengthen organizational defense maturity.

Topics Covered:

- AI's Role in Proactive Hunting
- Baselines & Anomaly Detection
- UEBA
- AI-Enhanced Hunting Workflows
- Orchestration & Human–AI Collaboration

MODULE 4

CLOSURE & CERTIFICATION

Course wrap-up and exam readiness.

LABS

- Understanding THMM
- Risk Framework and Treatment Concepts
- Adversary Simulation Using Caldera

CASE STUDY

Case Studies: Endpoint & Network Anomalies