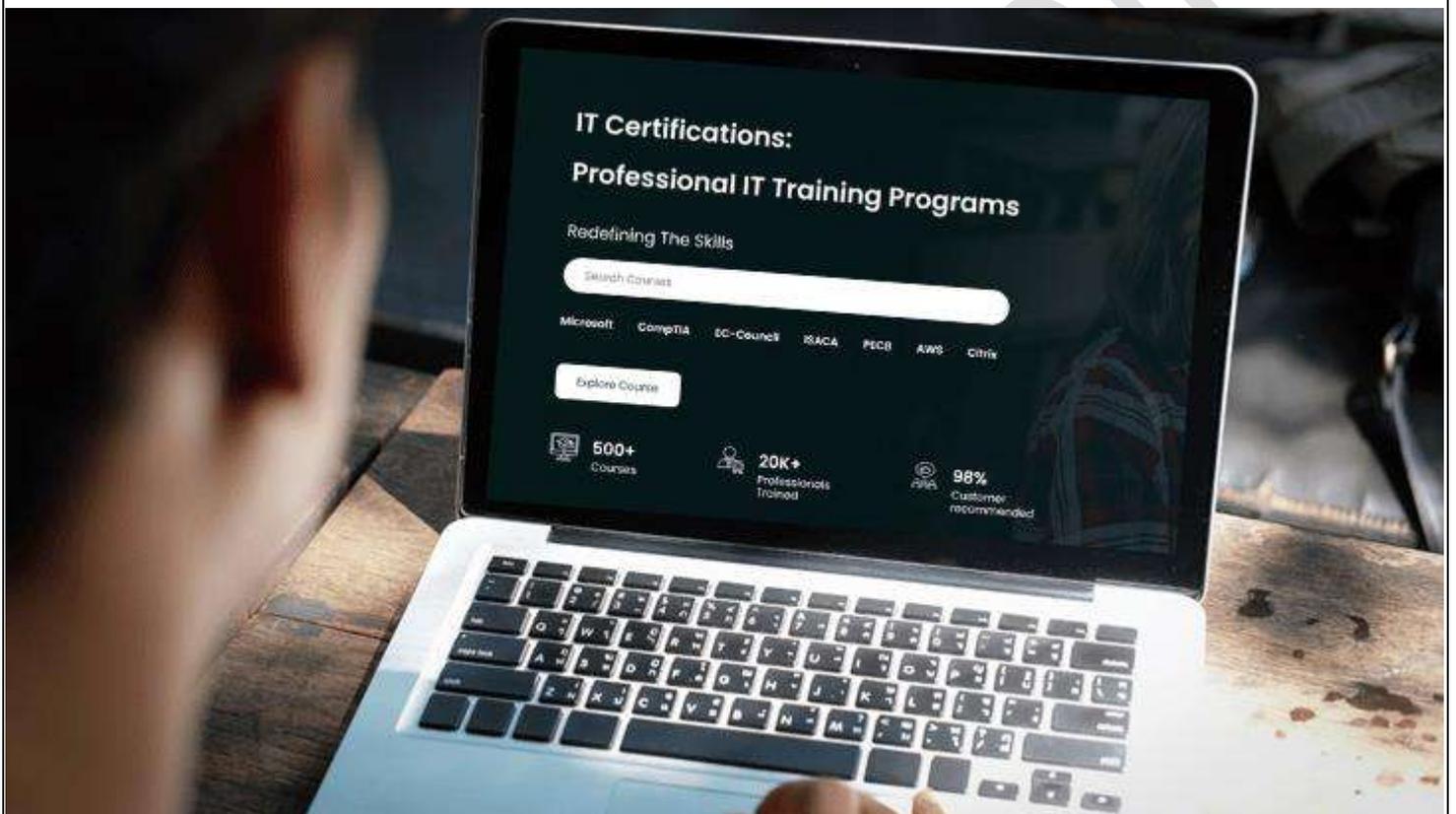




Redefining The Skills



CTIA: CERTIFIED THREAT INTELLIGENCE ANALYST TRAINING

Duration: 3 Days

Course Description

Certified Threat Intelligence Analyst (CTIA) from EC-Council is a credentialing certification and training program. This highly valued certification has been exclusively devised in collaboration with threat intelligence and cybersecurity experts worldwide to empower organizations effectively to identify and mitigate security risks with extensive processing and analysis of available threat information.

The CTIA is a specialist level training and certification that demonstrates security professionals the structured approach to acquiring threat intelligence. The CTIA certified candidates attain a competitive edge over other information security professionals. This threat intelligence certification course delivers standards-based, intensive practical skills to the most essentially required threat intelligence across information security.

Why Certified Threat Intelligence Analyst (CTIA)?

The CTIA certification training course from Microtek Learning helps you acquire a far-reaching understanding of:

- Threat intelligence and core concepts
- Various types of cyber threats
- Kill chain methodology
- Requirements of threat intelligence
- How to planning, direction, and review
- Collecting data and processing
- Data analysis
- Creating intelligence reports and disseminating

Who should attend this course?

This certification is designed to upskill:

- Security professionals and ethical hackers
- Security Analysts and architects
- SOC professionals, cybersecurity forensic experts and malware analysts
- Security consultants and threat hunters

What you will learn

- Primary issues threatening the information security world
- Role of threat intelligence
- Implementing threat intelligence in risk management, incident response, and SIEM
- Cyber threats and threat factors
- Objectives of diverse cybersecurity attacks
- Basics of threat intelligence including types, capabilities, strategy, lifecycle, maturity model, and frameworks
- Implementing the cyber kill chain methodology
- Advanced Persistent Threat (APT) lifecycle
- Tactics, Techniques, and Procedures (TTPs)
- Indicators of Compromise (IOS) and the pyramid of pain
- Steps to Planning a threat intelligence program including taking requirements, planning, directing, and review

- Types of data feeds and methods to collect data
- Threat intelligence data collection by using Cyber Counterintelligence (CCI), Open Source Intelligence (OSINT), Human Intelligence (HUMINT), and Indicators of Compromise (IOS)
- Bulk data collection, data structuring, processing, normalizing, sampling, storing, and creating visualizations
- Types of data analysis techniques such as Statistical Data Analysis, Analysis Structured Analysis of Competing Hypotheses (SACH), and of Competing Hypotheses (ACH)
- Threat analysis process including threat modeling, evaluation, fine-tuning, creating a knowledge base and runbook
- Threat intelligence dissemination, dissemination preferences
- Intelligence collaboration and Malware analysis
- Types of TI exchange and threat intelligence sharing formats
- Tools for threat intelligence, threat modeling, data analysis
- Disseminating threat intelligence and sharing protocols, dissemination preferences, sharing rules and models, intelligence collaboration
- TI exchange architecture and types, sharing relationships
- threat intelligence standards and formats for sharing
- Threat intelligence reporting
- Platforms and regulations to share operational, strategic, tactical, and technical intelligence

Prerequisites

- Working experience of minimum 2 years in information security

Curriculum

Module 01: Introduction to Threat Intelligence

Understand Intelligence

- Definition of Intelligence and its Essential Terminology
- Intelligence vs. Information vs. Data
- Intelligence-led Security Testing (Background and Reasons)

Summarize Cyber Threat Intelligence Concepts

- Cyber Threat Intelligence
- Threat Intelligence vs. Threat Data
- Stages of Cyber Threat Intelligence
- Characteristics of Threat Intelligence
- Benefits of Cyber Threat Intelligence
- Enterprise Objectives for Threat Intelligence Programs
- How Can Threat Intelligence Help Organizations?
- Threat Intelligence vs. Traditional Cybersecurity Approaches
- Threat Intelligence Metrics and Key Performance Indicators
- Types of Threat Intelligence
 - Strategic Threat Intelligence
 - Tactical Threat Intelligence
 - Operational Threat Intelligence
 - Technical Threat Intelligence
- Threat Intelligence Generation
- Predictive and Proactive Threat Intelligence
- Threat Intelligence Informed Risk Management

- Integration of Threat Intelligence into SIEM
- Leverage Threat Intelligence for Enhanced Incident Response
- Real-time Threat Detection and Response using Threat Intelligence
- Enhancing Incident Response by Establishing SOPs for Threat Intelligence
- Intelligence Preparation of the Environment (IPE) for Cyber Threat Intelligence
- Organizational Scenarios Using Threat Intelligence
- What Do Organizations and Analysts Expect?
- Common Information Security Organization Structure
- Responsibilities of Cyber Threat Analysts
- Threat Intelligence Use Cases
- Geopolitical Threat Intelligence
- Legal and Ethical Considerations in Threat Intelligence

Explain Threat Intelligence Lifecycle and Frameworks

- Threat Intelligence Lifecycle
- Role of Threat Analyst in Threat Intelligence Lifecycle
- Threat Intelligence Strategy
- Threat Intelligence Capabilities
- Capabilities to Look for in Threat Intelligence Solutions
- Threat Intelligence Maturity Model
- Threat Intelligence Frameworks
 - ThreatStream
 - ThreatConnect TIP
 - MISP-Open-Source Threat Intelligence Platform
 - CrowdStrike Falcon Intelligence Solution
 - Collective Intelligence Framework (CIF)
- Additional Threat Intelligence Frameworks

Understand Threat Intelligence Platforms (TIPs)

- Introduction to Threat Intelligence Platforms (TIPs)
- Role of TIPs in Cyber Security
- Types of TIPs
- Selecting the Right TIP
- Challenges in Selecting TIPs

Understand Threat Intelligence in the Cloud Environment

- Understanding the Role of Threat Intelligence in Cloud Security
- Necessity of Threat Intelligence for Proactive Cloud Security
- Threat Intelligence Integration into Cloud Security Architecture
- Cloud Security Automation using Threat Intelligence
 - Automating Cloud Security Processes using Threat Intelligence
 - Building Automated Responses to Cloud-based Threats
 - Integration of Threat Intelligence with Cloud-native Security Tools
- Cloud-specific Threat Intelligence Challenges
 - Mitigating Cloud-Specific Threat Intelligence Challenges
 - Mitigating Vendor-specific risks using Threat Intelligence

Understand Future Trends and Continuous Learning

- Emerging Technologies and Their Impact on Threat Intelligence
- Artificial Intelligence and Machine Learning in Threat Intelligence
 - Use of AI in CTI

- Career Paths and Opportunities in the Threat Intelligence Field
- Engaging with Threat Intelligence Community
- Ethical Considerations in Threat Intelligence Research and Reporting
- Role of Threat Intelligence in National Security and Defense

Module 02: Cyber Threats and Attack Frameworks

Understand Cyber Threats

- Overview of Cyber Threats
- Cyber Security Threat Categories
- Cyber Security Threats Associated with Specialized Technology
 - Industrial Control System (ICS)
 - Internet of Things (IoT)
 - Mobile Devices
 - Supervisory Control and Data Acquisition (SCADA)
 - Real-time operating system (RTOS)
 - Controller Area Network (CAN) Bus
- Threat Actors/Profiling the Attacker
- Threat: Intent, Capability, Opportunity Triad
- Motives, Goals, and Objectives of Cyber Security Attacks
- Hacking Forums
- Impact of Geopolitics and Economic Factors on Threats

Explain Advanced Persistent Threats

- Definition of Advanced Persistent Threats
- Characteristics of Advanced Persistent Threats
- Advanced Persistent Threat Lifecycle

Explain Cyber Kill Chain

- Cyber Kill Chain Methodology
- Tactics, Techniques, and Procedures
- Adversary Behavioral Identification
- Kill Chain Deep-Dive Scenario - Spear Phishing

Explain MITRE ATT&CK and Diamond Model

- MITRE ATT&CK Framework
- Use of ATT&CK Framework in Threat Intelligence and Red Teaming
- Diamond Model of Intrusion Analysis
- Extended Diamond Model of Intrusion Analysis

Understand Indicators of Compromise

- Indicators of Compromise
- Why Indicators of Compromise Important?
- Categories of Indicators of Compromise
- Key Indicators of Compromise
- Pyramid of Pain

Module 03: Requirements, Planning, Direction, and Review

Understand the Organization's Current Threat Landscape

- Identify Critical Threats to the Organization
- Assess Organization's Current Security Pressure Posture

- Assess Current Security Team's Structure and Competencies
- Understand Organization's Current Security Infrastructure and Operations
- Identifying Gaps and Vulnerabilities
- Assess Risks for Identified Threats

Understand Requirements Analysis

- Map Out Organization's Ideal Target State
- Identify Intelligence Requirements
- Define Threat Intelligence Requirements
 - Threat Intelligence Requirement Categories
- Business Requirements
 - Business Units Needs, Internal Stakeholders Needs, Third-Party Needs, and Other

Team's Needs

- Intelligence Consumer Requirements
- Priority Intelligence Requirements
- Factors for Prioritizing Requirements
- MoSCoW Method for Prioritizing Requirements
- Prioritize Organizational Assets
- Scope of Threat Intelligence Program
- Rules of Engagement
- Nondisclosure Agreements
- Avoid Common Threat Intelligence Pitfalls

Plan a Threat Intelligence Program

- Prepare People, Processes, and Technology
- Develop a Collection Plan
- Schedule a Threat Intelligence Program
- Plan a Budget
- Develop a Communication Plan to Update Progress to Stakeholders
- Aggregate Threat Intelligence
- Select a Threat Intelligence Platform
- Consuming Intelligence for Different Goals
- Track Metrics to Keep Stakeholders Informed

Establish Management Support

- Prepare Project Charter and Policy to Formalize the Initiative
 - Establish Your Case to Management for a Threat Intelligence Program
 - Apply a Strategic Lens to Threat Intelligence Program

Build a Threat Intelligence Team

- Satisfy Organizational Gaps with the Appropriate Threat Intelligence Team
- Understand different Threat Intelligence Roles and Responsibilities
 - Intelligence Analysts
 - Malware Analysts
 - Incident Responders
 - E-discovery and Forensics Examiners
 - Security Operators
 - Vulnerability Management Analysts
 - System/Data Architects
- Identify Core Competencies and Skills

- Define Talent Acquisition Strategy
- Building and Positioning an Intelligence Team
- How to Prepare an Effective Threat Intelligence Team

Understand Threat Intelligence Sharing

- Importance of Threat Intelligence Sharing
- Ways of Threat Intelligence Sharing
- Establishing Threat Intelligence Sharing Capabilities
- Considerations for Sharing Threat Intelligence
- Sharing Intelligence with Various Organizations
- Types of Sharing Partners
- Important Selection Criteria for Partners
- Sharing Intelligence Securely

Review Threat Intelligence Program

- Threat Intelligence-led Engagement Review
- Considerations for Reviewing Threat Intelligence Program
- Assessing Success and Failure of Threat Intelligence Program

Module 04: Data Collection and Processing

Understand Threat Intelligence Data Collection

- Introduction to Threat Intelligence Data Collection
- Data Collection Methods
- Types of Data
- Types of Threat Intelligence Data Collection
 - Strategic Threat Intelligence Data Collection
 - Operational Threat Intelligence Data Collection
 - Tactical Threat Intelligence Data Collection
 - Technical Threat Intelligence Data Collection

Summarize Threat Intelligence Collection Management

- Understanding Operational Security for Data Collection
- Understanding Data Reliability
- Ensuring Intelligence Collection Methods to Produce Actionable Data
- Validating the Quality and Reliability of Third-Party Intelligence Sources
- Establishing Collection Criteria for Prioritization of Intelligence Needs and Requirements
- Building a Threat Intelligence Collection Plan

Explain Threat Intelligence Feeds and Sources

- Threat Intelligence Feeds
- Threat Intelligence Sources
 - Open-Source Intelligence (OSINT)
 - Human Intelligence (HUMINT)
 - Signals Intelligence (SIGINT)
 - Technical Intelligence (TECHINT)
 - Geo-spatial Intelligence (GEOINT)
 - Imagery Intelligence (IMINT)
 - Measurement and Signature Intelligence (MASINT)
 - Covert Human Intelligence Sources (CHIS)
 - Financial Intelligence (FININT)
 - Social Media Intelligence (SOCMINT)

- Cyber Counterintelligence (CCI)
- Indicators of Compromise (IoCs)
- Industry Association and Vertical Communities
- Commercial Sources
- Government and Law Enforcement Sources

Explain Threat Intelligence Data Collection and Acquisition

- Threat Intelligence Data Collection and Acquisition
- Data Collection through Open-Source Intelligence (OSINT)
 - Data Collection through Search Engines
- Data Collection through Advanced Google Search
- Data Collection through Google Hacking Database
- Data Collection through Pulsedive
- Data Collection through Deep and Dark Web Searching
 - Data Collection through Web Services
- Finding Top-Level Domains (TLDs) and Subdomains
- Data Collection through Job Sites
- Data Collection through Groups, Forums, and Blogs
- Data Collection through Social Networking Sites
 - Data Collection through Website Footprinting
- Data Collection through Monitoring Website Traffic
- Data Collection through Website Mirroring
- Extracting Website Information from <https://archive.org>
- Extracting Metadata of Public Documents
 - Data Collection through Emails
- Data Collection by Tracking Email Communications
- Data Collection from Email Header
- Data Collection through Emails: eMailTrackerPro
 - Data Collection through Whois Lookup
 - Data Collection through DNS Interrogation
- Data Collection through DNS Lookup and Reverse DNS Lookup
- Fast-Flux DNS Information Gathering
- Dynamic DNS (DDNS) Information Gathering
- DNS Zone Transfer Information Gathering
 - Automating OSINT Effort Using Tools/Frameworks/Scripts
- Maltego
- TheHive
- OSINT Framework
- FOCA
- Data Collection through Human Intelligence (HUMINT)
 - Data Collection through Human-based Social Engineering Techniques
 - Data Collection through Interviewing and Interrogation
 - Social Engineering Tools
- Data Collection through Cyber Counterintelligence (CCI)
 - Data Collection through Honeypots
 - Data Collection through Passive DNS Monitoring
 - Data Collection through Pivoting Off Adversary's Infrastructure
 - Data Collection through Malware Sinkholes
 - Data Collection through YARA Rules
- Data Collection through Indicators of Compromise (IoCs)
 - IoC Data Collection through External Sources

- Commercial and Industry IoC Sources
 - IT-ISAC
- Free IoC Sources
 - AlienVault OTX
 - ThreatQ Data Exchange
 - MISP
 - Threatnote
 - GREYNOISE
- Tools for IoC Data Collection through External Sources
 - IoC Data Collection through Internal Sources
 - Tools for IoC Data Collection through Internal Sources
- Splunk Enterprise
- Valkyrie Unknown File Hunter
 - Data Collection through Building Custom IoCs
 - Tools for Building Custom IoCs
- IOC Editor
 - Steps for Effective Usage of Indicators of Compromise (IoCs) for Threat Intelligence
- Data Collection through Malware Analysis
 - Preparing Testbed for Malware Analysis
 - Data Collection through Static Malware Analysis
 - Data Collection through Dynamic Malware Analysis
 - Malware Analysis Tools
- Valkyrie
- Data Collection through Python Scripting
 - Threat Data Collection Techniques using Python Scripting: Web Scraping, API

Scraping, and Database Scraping

- Storing and Organizing Threat Data with Python
- Setting Up a Threat Intelligence Database in SQLite using Python
- Produce Own Threat Intelligence through Binary Classification
 - Importance of Producing Own Threat Intelligence through Binary Classification
 - Factors to Consider While Developing Threat Intelligence through Binary Classification

Understand Bulk Data Collection

- Introduction to Bulk Data Collection
- Forms of Bulk Data Collection
- Benefits and Challenges of Bulk Data Collection
- Bulk Data Management and Integration Tools
 - Talend Data Fabric

Explain Data Processing and Exploitation

- Threat Intelligence Data Collection and Acquisition
- Introduction to Data Processing and Exploitation
- Assessing Data Quality
- Data Dimensions
- Improving Data Quality
- Structuring/Normalization of Collected Data

- Data Sampling
 - Types of Data Sampling
- Storing and Data Visualization
 - Tableau
 - QlikView
- Sharing Threat Information

Understand Threat Data Collection and Enrichment in Cloud Environments

- Threat Data Collection and Enrichment in Cloud Environments
- Threat Data Sources in Cloud Environments
- Data Collection in Cloud Environments
- Enrichment Techniques: Contextualizing Threat Data For Cloud Security

Module 05: Data Analysis

Summarize Data Analysis

- Introduction to Data Analysis
- Contextualization of Data
- Types of Data Analysis

Explain Data Analysis Techniques

- Statistical Data Analysis
 - Data Preparation
 - Data Classification
 - Data Validation
 - Data Correlation
 - Data Scoring
 - Statistical Data Analysis Tools
- SAS/STAT Software
- IBM SPSS
- Analysis of Competing Hypotheses
 - Hypothesis
 - Evidence
 - Diagnostics
 - Refinement
 - Inconsistency
 - Sensitivity
 - Conclusions and Evaluation
- ACH Tool
 - PARC ACH
- Structured Analysis of Competing Hypotheses
- Other Data Analysis Methodologies

Understand Threat Analysis

- Introduction to Threat Analysis
- Types of Threat Intelligence Analysis
 - Strategic Threat Intelligence Analysis
 - Operational Threat Intelligence Analysis
 - Tactical Threat Intelligence Analysis
 - Technical Threat Intelligence Analysis

Demonstrate Threat Analysis Process

- Threat Analysis Process and Responsibilities
- Threat Analysis based on Cyber Kill Chain Methodology
- Aligning Defensive Strategies with Phases of Cyber Kill Chain Methodology
- Perform Threat Modeling
 - Asset Identification
 - System Characterization
 - System Modeling
 - Threat Determination and Identification
 - Threat Profiling and Attribution
 - Threat Ranking
 - Threat Information Documentation
- Threat Modeling Methodologies
 - STRIDE
 - PASTA
 - TRIKE
 - VAST
 - DREAD
 - OCTAVE
 - Common Vulnerability Scoring System (CVSS)
 - Attack Tree
- Threat Modeling Tools
 - Microsoft Threat Modelling Tool
 - ThreatModeler
 - OWASP Threat Dragon
 - IriusRisk
- Enhance Threat Analysis Process with Diamond Model Framework
- Enrich Indicators with Context
- Validating and Prioritizing Threat Indicators

Explain Fine-tuning Threat Analysis

- Fine-tuning Threat Analysis
- Identifying and Removing Noise
- Identifying and Removing Logical Fallacies
- Identifying and Removing Cognitive Biases
- Automate Threat Analysis Processes
- Develop Criteria for Threat Analysis Software
- Employ Advanced Threat Analysis Techniques
 - Machine Learning-based Threat Analysis
 - Cognitive-based Threat Analysis

Understand Threat Intelligence Evaluation

- Threat Intelligence Evaluation
- Threat Attribution

Create Runbooks and Knowledge Base

- Developing Runbooks
- Create Accessible Threat Knowledge Base
- Organize and Store Cyber Threat Information in Knowledge Base

Use Threat Intelligence Tools

- Threat Intelligence Tools

- AlienVault® USM® Anywhere
- IBM X-Force Exchange
- AutoFocus
- Docguard
- Additional Threat Intelligence Tools

Module 06: Intelligence Reporting and Dissemination

Understand Threat Intelligence Reports

- Threat Intelligence Reports
- Types of Cyber Threat Intelligence Reports
 - Threat Analysis Reports
 - Threat Landscape Reports
- Generating Concise Reports
- Threat Intelligence Report Template
- How to Maximize the Return from Threat Intelligence Report
- Continuous Improvement via Feedback Loop
- Report Writing Tools
 - MagicTree
 - KeepNote

Understand Dissemination

- Overview of Dissemination
- Preferences for Dissemination
- Benefits of Sharing Intelligence
- Challenges to Intelligence Sharing
- Legal and Privacy Implications of Sharing Threat Intelligence
- Disseminating Threat Intelligence Internally
- Building Blocks for Threat Intelligence Sharing
- Begin Intelligence Collaboration
- Establish Information Sharing Rules
- Information Sharing Model
- Information Exchange Types
- Threat Intelligence Exchange Architectures
- Threat Intelligence Sharing Quality
- Access Control on Intelligence Sharing
- Intelligence Sharing Best Practices

Participate in Sharing Relationships

- Why Sharing Communities are Formed?
- Join a Sharing Community
- Factors to be Considered When Joining a Community
- Engage in Ongoing Communication
- Consume and Respond to Security Alerts
- Consume and Use Indicators
- Produce and Publish Indicators
- External Intelligence Sharing
- Establishing Trust
- Organizational Trust Models

Understand Sharing Threat Intelligence

- Sharing Strategic Threat Intelligence

- Sharing Tactical Threat Intelligence
- Sharing Operational Threat Intelligence
- Sharing Technical Threat Intelligence
- Sharing Intelligence using YARA Rules
- Information Technology – Information Security and Analysis Center

Explain Delivery Mechanisms

- Forms of Delivery
- Machine-readable Threat Intelligence
- Standards and Formats for Sharing Threat Intelligence
 - Traffic Light Protocol (TLP)
 - MITRE Standards
 - Managed Incident Lightweight Exchange
 - VERIS
 - IDMEF
 - AFII4-133 Tradecraft Standard for CTI

Use Threat Intelligence Sharing Platforms

- Information Sharing and Collaboration Platforms
 - Continuous Threat Exposure Management (CTEM)
 - Anomali STAXX
 - MISP (Malware Information Sharing Platform)
 - Intel Exchange (CTIX)
 - Other Information Sharing and Collaboration Platforms

Understand Intelligence Sharing Acts and Regulations

- Cyber Intelligence Sharing and Protection Act (CISPA)
- Cybersecurity Information Sharing Act (CISA)
- General Data Protection Regulation (GDPR)

Explain Threat Intelligence Integration

- Integrating Threat Intelligence
- How to Integrate CTI into Environment
- Acting on Gathered Intelligence
- Tactical Intelligence Supports IT Operations: Blocking, Patching, and Triage
- Operational Intelligence Supports Incident Response: Fast Reaction and Remediation
- Strategic Intelligence Supports Management: Strategic Investment and Communications

Understand Intelligence Sharing and Collaboration using Python Scripting

- Collaborative Threat Intelligence Projects using Python
- Python Libraries and Frameworks to Share Threat Intelligence
- Interacting with Threat Intelligence Platforms
 - TAXII
 - MISP
- Secure Data Exchange with Python Script

Module 07: Threat Hunting and Detection

Summarize Threat Hunting Concepts

- Introduction to Threat Hunting
- Importance of Threat Hunting
- Types of Threat Hunting

- Threat Hunting Maturity Model (HMM)
- Threat Hunter Skillset
- Threat Hunting Process
- Threat Hunting Loop
- Developing Intelligence-driven Threat Hunting Methodology
- Targeted Hunting Integrating Threat Intelligence (TaHiTI)

Understand Threat Hunting Automation

- Threat Hunting Automation using EDR, XDR and SIEM
- ChatGPT for Threat Hunting Automation
- Threat Hunting Automation using Python Scripting
- Developing Python Scripts for Targeted Threat Hunting
 - Brute-force Detection with Python
 - Analyze Network Logs and Traffic with Python
 - Behavior-based Threat Detection using Python
- Threat Hunting Tools
 - IBM Security QRadar Suite
 - Sophos XDR
 - Swimlane Turbine
 - Additional Threat Hunting Tools

Module 08: Threat Intelligence in SOC Operations, Incident Response, and Risk Management

Understand Threat Intelligence in SOC Operations

- Overview of SOC Operations
- Challenges for SOC Investigation
- Threat Intelligence in SOC Operations
- Expectations of SOC Team from CTI
- Building SOC Threat Intelligence
- Next-Gen Intelligent SOC
- Role of Threat Intelligence Platform (TIP) in SOC
- SOC Threat Intelligence Platforms (TIP)
 - SOCRadar
 - EclecticIQ TIP

Understand Threat Intelligence in Risk Management

- Overview of Risk Management
- Challenges in Risk Management
- Role of Threat Intelligence in Risk Management Process
- Collaboration between Threat Intelligence and Risk Management
- Integrating Threat Intelligence into Risk Management Process
- Challenges of Integrating Threat Intelligence in Risk Management

Understand Threat Intelligence in Incident Response

- Overview of Incident Response (IR)
- Challenges Involved in Incident Response (IR)
- Integrating Threat Intelligence into Incident Response Process
- Measuring the Effectiveness of Threat intelligence in Incident Response
- Post-incident Analysis and Lessons Learned from Threat Intelligence
- Continuous Improvement of Incident Response using Threat Intelligence
- Threat Intelligence in Incident Recovery and Resilience