Certified Cyber Threat Analyst (CCTA) – Advanced Threat Hunting Training Course

11 – 15 April 2027
Johannesburg

AGILE LEADERS
Training Center

AGILE LEADERS
Training Center

Certified Cyber Threat Analyst (CCTA) – Advanced Threat Hunting Training Course

Ref: 103600315_99653 **Date:** 11 – 15 April 2027 **Location:** Johannesburg **Fees:** 6000 Euro

Course Overview

In today's cyber landscape, organizations face constant threats that require skilled cybersecurity professionals to identify, analyze, and mitigate risks effectively. The Certified Cyber Threat Analyst CCTA Training - Advanced Threat Hunting Course is designed to equip participants with cutting-edge threat hunting techniques, cyber intelligence frameworks, and incident response strategies.

This comprehensive cybersecurity threat analyst course blends theoretical knowledge with hands-on labs, providing real-world threat hunting experience. Participants will learn how to implement cyber threat intelligence frameworks, develop risk assessment methodologies, and enhance their organization's security posture.

By earning the PECB Cyber Threat Analyst certification, professionals validate their expertise in cybersecurity risk management, advanced threat hunting, and cyber threat detection. Whether you're an SOC analyst, incident responder, or penetration tester, this course offers the skills and knowledge needed to excel in cybersecurity defense strategies.

Target Audience

- Cybersecurity professionals SOC analysts, incident responders, security engineers
- IT infrastructure managers
- Security managers and director
- Ethical hackers and penetration testers
- Risk management professionals
- Aspiring cybersecurity professionals

Targeted Organizational Departments

- Security Operations Center SOC teams
- Incident response and forensic investigation teams
- IT security and compliance departments
- Threat intelligence and cybersecurity governance teams
- Risk management and auditing departments

AGILE LEADERS
Training Center

Targeted Industries

- Financial institutions and banking
- Healthcare and pharmaceuticals
- Government and defense
- Telecommunications and IT services
- E-commerce and retail
- Energy and critical infrastructure

Course Offerings

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

- Identify cyber threats and attack frameworks to assess organizational risks
- Develop cyber threat intelligence strategies to predict and mitigate attacks
- Implement advanced threat hunting techniques for proactive security measures
- Execute incident response and management plans to minimize cyber incidents
- Utilize cybersecurity monitoring techniques to enhance threat detection
- Formulate and validate threat hunting hypotheses using data-driven approaches
- Conduct cyber forensic investigations to analyze attack patterns
- Apply cybersecurity continual improvement strategies to fortify defenses

Training Methodology

This interactive cybersecurity training combines:

- Live expert-led sessions with real-world case studies
- Hands-on cyber threat analysis training with advanced tools
- Simulated cyber attack scenarios to test incident response readiness
- Industry best practices for cybersecurity compliance and governance

Course Toolbox

- Cyber attack framework templates for real-world application
- Access to online cybersecurity resources for continuous learning
- Threat intelligence case studies to understand adversary tactics

AGILE LEADERS
Training Center

Course Agenda

Day 1: Foundations of Cyber Threat Analysis and Intelligence

- **Topic 1:** Introduction to Cyber Threat Analysis and Training Course Objectives
- **Topic 2:** Cyber Threat Overview - Types, Characteristics, and Attack Vectors
- **Topic 3:** Cyber Threat Intelligence - Fundamentals and Key Sources
- **Topic 4:** Cyber Threat and Attack Frameworks MITRE ATT&CK, Lockheed Martin Cyber Kill Chain
- **Topic 5:** Threat Modeling - Identifying and Assessing Potential Risks
- **Topic 6:** Understanding the Role of Cyber Threat Analysts in Security Operations
- **Reflection & Review:** Key takeaways from cyber threat intelligence and frameworks

Day 2: Threat Hunting Strategies and Incident Response Planning

- **Topic 1:** Fundamentals of Incident Response and Management Plans
- **Topic 2:** Threat Hunting Fundamentals - Proactive Security Strategies
- **Topic 3:** Preparing a Threat Hunting Program - Setting Objectives and Goals
- **Topic 4:** Executing the Threat Hunting Process - Techniques and Methodologies
- **Topic 5:** Incident Detection and Response - Integrating SOC Operations
- **Topic 6:** Cybersecurity Risk Management - Identifying and Addressing Vulnerabilities
- **Reflection & Review:** Best practices for incident response and threat hunting execution

Day 3: Advanced Threat Hunting and Threat Intelligence Utilization

- **Topic 1:** Data Collection and Analysis for Threat Hunting
- **Topic 2:** Formulating and Validating Threat Hunting Hypotheses
- **Topic 3:** Cyber Threat Hunt Reporting and Documentation Techniques
- **Topic 4:** Threat Intelligence Frameworks - Practical Implementation in Organizations
- **Topic 5:** Cybersecurity Monitoring Techniques - Enhancing Continuous Threat Detection
- **Topic 6:** Security Operations Center SOC Training - Optimizing Threat Response Efficiency
- **Reflection & Review:** Lessons learned from hands-on threat hunting and intelligence utilization

AGILE LEADERS
Training Center

Day 4: Cybersecurity Culture, Compliance, and Continuous Improvement

- **Topic 1:** Threat Hunting Metrics - Measuring Performance and Effectiveness
- **Topic 2:** Cybersecurity Awareness and Training Programs - Strengthening Organizational Defense
- **Topic 3:** Cybersecurity Compliance and Governance - Frameworks and Regulations
- **Topic 4:** Cybersecurity Forensic Investigation - Tracing and Analyzing Cyber Incidents
- **Topic 5:** Continual Improvement in Cyber Threat Hunting - Adaptive Security Strategies
- **Topic 6:** Cyber Threat Mitigation Strategies - Strengthening Defense Mechanisms
- **Reflection & Review:** Strategies for developing a resilient cybersecurity culture

Day 5: Practical Assessment & Course recap

- **Topic 1:** Cybersecurity Professional Certification - Exam Overview and Preparation
- **Topic 2:** Final Cyber Threat Hunting Simulation - Real-World Case Studies
- **Topic 3:** Ethical Hacking and Threat Hunting - Understanding the Adversary's Perspective
- **Topic 4:** Network Security Threat Detection Training - Identifying Hidden Threats
- **Topic 5:** Best Practices for Cybersecurity Defense Strategies - Lessons from Industry Experts
- **Topic 6:** Career Development in Cyber Threat Analysis - Next Steps for Certified Analysts
- **Reflection & Review:** Course recap, key takeaways, and certification readiness

FAQ

What specific qualifications or prerequisites are needed for participants before enrolling in the course?

Participants should have basic cybersecurity knowledge and familiarity with network security principles. While prior experience in threat analysis, SOC operations, or incident response is beneficial, it is not mandatory.

How long is each day's session, and what is the total number of hours for the course?

Each day's session runs 4-5 hours, including interactive labs, discussions, and hands-on exercises. The total course duration is 20-25 hours over five days.

What tools will participants use during the hands-on threat hunting exercises?

Participants will explore open-source cybersecurity tools for threat detection, forensic investigation, and cyber intelligence analysis. While no proprietary software is provided, the course offers insights into industry-leading security tools.

How This Course is Different from Other Cyber Threat Analyst Courses

The Certified Cyber Threat Analyst CCTA Training - Advanced Threat Hunting Course stands out by:

- Integrating real-world cyber threat analysis frameworks with hands-on labs
- Focusing on proactive threat hunting techniques, not just reactive security measures
- Offering advanced cybersecurity monitoring techniques for continuous threat detection
- Providing expert-led training from cybersecurity professionals with industry experience
- Aligning with global cybersecurity compliance and governance standards