PECB Where Excellence Meets Recognition



PECB Certified Cyber Threat Analyst

Gain expertise in identifying, analyzing, and mitigating cyber threats.

Why should you attend?

In today's rapidly evolving cyber landscape, the need for skilled professionals to effectively identify and mitigate cyber threats is more critical than ever. By attending the Certified Cyber Threat Analyst (CCTA) training course, participants will be taking a significant step toward enhancing their cybersecurity expertise. This course is designed to provide advanced skills and knowledge required to stay ahead of emerging threats and protect organization's valuable assets.

Besides the theoretical part, this training course includes hands-on practical labs focused on threat hunting, which allows participants to not only understand the latest threat analysis techniques, but also know how to implement them effectively. Furthermore, attaining the CCTA certification demonstrates an individual's commitment to professional development and dedication to maintaining the highest standards in cybersecurity. This industry-recognized certification will enhance credibility and career prospects, making everyone who attends a valuable asset to any organization.

The attainment of PECB Certified Cyber Threat Analyst (CCTA) certificate signifies that an individual has acquired the essential expertise and knowledge to proficiently identify, analyze, and mitigate cyber threats. This certification demonstrates the individual's ability to implement advanced threat hunting techniques and establish streamlined processes that enhance an organization's security posture.

By becoming a certified CTA, professionals validate their commitment to maintaining the highest standards of cybersecurity, ensuring they are well-equipped to safeguard their organization's information assets in an increasingly hostile cyber environment.



Who should attend?

This course is particularly advantageous and intended for:

- Cybersecurity professionals such as incident responders and security operations center (SOC)
- IT professionals who are involved in managing and security IT infrastructure
- Security managers and directors who are responsible for an organization's security strategy
- Professionals involved in penetration testing and ethical hacking in order to gain insights into the latest threats and defensive techniques
- Individuals responsible for risk management, compliance, and governance
- Aspiring cybersecurity professionals who want to gain foundational knowledge and skills in threat analysis

Course agenda

Duration: 5 days

Day 1 | Fundamentals of cyber threat analysis and threat hunting frameworks

- Training course objectives and structure
- Cyber threats overview
- Cyber threat intelligence
- Cyber threat and attack frameworks
- Threat modeling

Day 2 | Prepare, execute phase of threat hunting program and incident management plan

- Fundamentals of incident response and management plan
- Prepare stage
- Execute stage

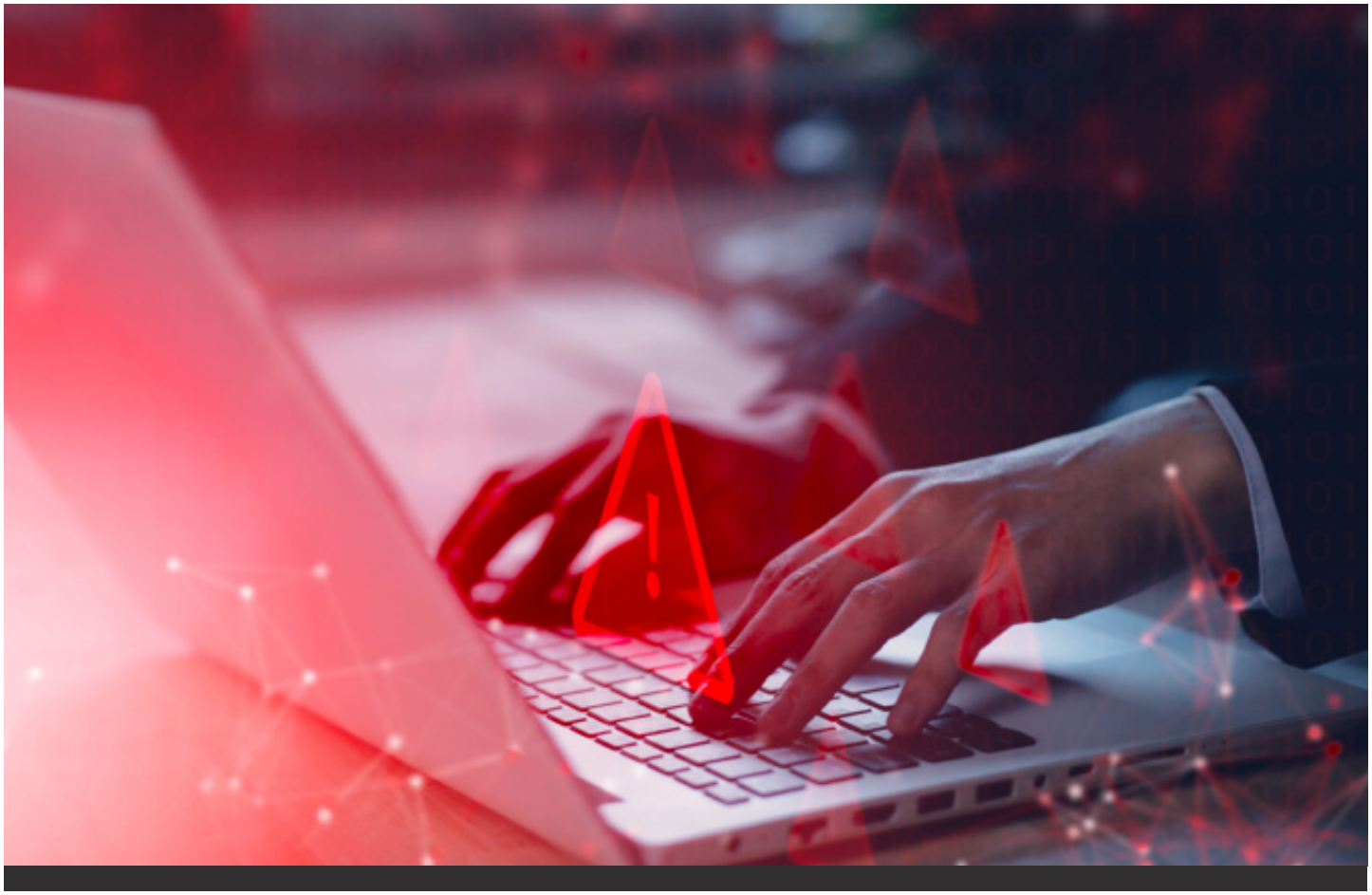
Day 3 | Analyze and knowledge phase of threat hunting framework

- Analyze stage
- Knowledge stage
- Threat hunting deliverables
- Cyber threat hunt reporting

Day 4 | Building a cybersecurity culture, monitoring and measurement, and continual improvement

- Threat hunting metrics
- Awareness and training programs
- Monitoring and measurement
- Continual improvement
- Closing of the training course

Day 5 | Certification Exam



Learning objectives

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

- Identify various types of cyber threats, understand their characteristics, and analyze their potential impact on organizational security
- Establish robust incident response plans to effectively manage and mitigate security breaches and cyberattacks
- Utilize advanced threat hunting techniques and tools to proactively search for and identify security threats within an organization's network
- Formulate and validate threat hunting hypothesis using data-driven approaches and identify potential threats by leveraging
- Design, implement, and continuously improve threat hunting programs within organizations

Examination

Duration: 3 hours

The "PECB Certified Cyber Threat Analyst" exam meets the requirements of the PECB Examination and Certification Program (ECP). It covers the following competency domains:

Domain 1	Fundamental concepts of cyber threat analyst and threat hunting
Domain 2	Preparation and execution phase of threat hunting programs and incident management plans
Domain 3	Analysis and knowledge phase of threat hunting frameworks
Domain 4	Operational aspects of information security controls, incident management, and change management
Domain 5	Building a cybersecurity culture, monitoring and measurement, and continual improvement

For specific information about exam type, languages available, and other details, please visit the List of PECB Exams and the Examination Rules and Policies.



Certification

After successfully passing the exam, you can apply for one of the credentials shown below. You will receive the certificate once you comply with all the requirements related to the selected credential.

The requirements for PECB Certified Cyber Threat Analyst certifications are as follows:

Credential	Exam	Professional experience	Project experience	Other requirements
PECB Certified Provisional Cyber Threat Analyst	PECB Certified Cyber Threat Analyst exam or equivalent	None	None	Signing the PECB Code of Ethics
PECB Certified Cyber Threat Analyst (CCTA)	PECB Certified Cyber Threat Analyst exam or equivalent	Five years: two years of work experience in threat hunting, threat analysis, and cybersecurity	300 hours	Signing the PECB Code of Ethics

General information

- Certification and examination fees are included in the price of the training course
- Participants will be provided with the training course material containing over 400 pages of explanatory information, examples, best practices, exercises, and quizzes
- An attestation of course completion worth 31 CPD (Continuing Professional Development) credits will be issued to the participants who have attended the training course
- In case candidates fail the exam, they can retake it within 12 months following the initial attempt for free