CSecTor Newsletter #2

Elevating OT cybersecurity through specialized online training and resources.

@Csector

1 Strengthening SMEs: CSecTOR's Cybersecurity Training

Boost Your Business's Cybersecurity with CSecTOR's Tailored OT-Cybersecurity Course for SMEs

In response to the rising cyber threats, the European Erasmus project CSecTOR introduces a specialized digital OT-Cybersecurity course for SMEs. This course, adaptable to different skill levels through a preliminary self-assessment test, offers nine key modules. These include Cybersecurity Basics, Network Security Tools, OT Asset Protection, and Ethical Hacking, among others. SMEs can choose modules based on their needs, ensuring targeted and efficient learning. Join this initiative to elevate your company's cybersecurity resilience.

Virtual Partner Meeting

Benefits of the CSecTOR OT-Cybersecurity Course for SMEs:

The CSecTOR OT-Cybersecurity Course offers significant benefits for SMEs. It allows businesses to tailor their learning experience to their specific needs, as determined by an initial self-assessment test. The course covers a wide range of topics, from basic security concepts to advanced techniques, enabling companies to focus on relevant areas for effective cyber resilience enhancement. Additionally, the practical content directly addresses the digital challenges and threats faced by SMEs.

2022-1-AT01-KA220-VET-000087608
Funded by the European Union. Views and opinions expressed are however those of the author(s) only and do not necessarily reflect those of the European Union or OeAD-GmbH. Neither the European Union nor the granting authority can be held responsible for them.

2 Objectives of the CSecTOR OT-Cybersecurity Course:

Introduction to OT Cybersecurity:
The course is designed to thoroughly acquaint employees and specialists in the public sector with the intricate aspects of cybersecurity, specifically focusing on Operational Technologies. This foundational module is crucial for building a comprehensive understanding of the cybersecurity landscape as it pertains to OT.

1

2

Broad Framework Education:
Participants will delve into the expansive realm of information and operational security. This includes learning about cutting-edge information systems and emerging technologies that are pivotal in enhancing the safety and security of operational processes. The course aims to broaden the understanding of security beyond conventional IT protocols, integrating the latest advancements and best practices in the field.

Practical Tools for Secure Operations:
The course offers practical training on how to plan, organize, and execute sustainable and secure solutions within operational environments. This objective is geared towards equipping employees with the necessary tools and strategic approaches to address and mitigate potential security vulnerabilities within their operations, ensuring a robust and secure operational framework.

3

4

Training in Assessment Methods: This part of the course focuses on empowering employees with sophisticated assessment methods. These methods are designed to facilitate the development of critical decision-making skills, enabling participants to craft and implement resilient business models that consider a multitude of factors such as human elements, information integrity, environmental impact, economic viability, and societal implications.

Application of Modern Methods and Techniques:
The course culminates in training participants to apply modern and advanced methods and techniques. These are specifically chosen to contribute significantly to the improvement of operational security. The methods covered range from innovative cybersecurity technologies to advanced analytical techniques, all aimed at equipping participants with the skills to not only respond to but also proactively manage and improve their operational security infrastructure.

5

2022-1-AT01-KA220-VET-000087608
Funded by the European Union. Views and opinions expressed are however those of the author(s) only and do not necessarily reflect those of the European Union or OeAD-GmbH. Neither the European Union nor the granting authority can be held responsible for them.