EXCELLIUM

Your first call when it comes to IT and security

TRAININGS CATALOG 2021

We provide local training and certification on a range of Information Security areas, including Security Awareness, Secure Development, Hacking techniques, Forensic Analysis, Security Infrastructure and Products related competences, Information Security Governance…

> Real world attackers often target ordinary users as part of their strategy. User buy-in and awareness are essential elements in resisting these attacks.

CUSTOMER CHALLENGES

As Information Technology is a fast moving domain, criminals continue to discover endless new opportunities.

To address this challenge, an organization must keep itself updated in order to:

- Understand new threats,
- Define reaction capabilities,
- Detect malicious activities.

Effective information security management combines technical skill with management vision. And while securing technical infrastructure is rightly seen as crucial, equally important human factors are often neglected.

OUR APPROACH

We recognize that users are a key part of security countermeasures. Seeing how often hackers exploit users in their attacks, we see training users as essential in being able to resist such attacks.

- If you want to defend against cyber threats properly, the best advice is to know your enemy, his weapons and techniques.
- According to the learning pyramid, the student retention rate 24 hours after training is only 5% with passive listening to a lecture, but 75% with active practice. No prizes for guessing our preferred approach!
- Knowing a security standard is good, getting real examples and guidelines on how to apply it is better!
- These days, application security is paramount, and the only truly effective way to achieve it is by building security in, from the very beginning.

TRAINING CATALOG SUBSET

HACKING & FORENSICS

Build your Csirt / 4 days

This course will enable you to understand the needs and the global scope of what a Computer Security Incident is and Response Team (CSIRT). What are the roles in both incident prevention and incident response? And what skills and conduct are required for various different kind of incidents?

Malware : Reverse Engineering / 3 days

In this course, we address the issue of malware, a major societal concern. Nowadays, IT infrastructure requires security specialists to prevent attacks and analyze the damage caused by malware.

Office Document Analysis / 2 days

This training will enable you to understand how malwarecan use office documents as initial infection mechanism . It will enable your Incident response team to determine whether an office document is malicious. You will be able to extract the payload an determine the IOC for samples of malware.

Certified Ethical Hacker / 5 days / Partnership with Oxiane and EC Council

This training will immerse you in a hands-on environment where, using practical examples, you will learn about the approaches and techniques used by real-world hackers. Successful completion of the training and exam leads to an industry-recognized certification.

DATA PRIVACY

Certified Data Protection Officer / 4 days / Partnership with PECB

This course will prepare you become a certified DPO to manage the entire data life cycle applicable to the collection and processing personal data within your organization in the context of GDPR and ePrivacy.

SECURITY MANAGEMENT

Introduction ISO 27001 Foundation / 1 day / Partnership with PECB

ISO/IEC 27001 Introduction training course enables you to become familiar with the basic concepts of an Information Security Management System (ISMS). By attending the ISO/IEC 27001 Introduction training course, you will understand the importance of ISMS and the benefits that businesses, society and governments can obtain.

ISO 27001 Foundation / 2 days / Partnership with PECB

ISO/IEC 27001 Foundation training allows you to learn the basic elements to implement and manage an Information Security Management System as specified in ISO/IEC 27001.

ISO 27001 Lead Implementer / 5 days / Partnership with PECB

ISO 27001 Lead Implementer is a professional certification for those specializing in information security management systems (ISMS) based on the ISO/IEC 27001 standard.

ISO 27005 Risk Manager / 3 days / Partnership with PECB

This training enables you to develop the competence tmaster the risk management process related to all assets of relevance for Information Security using the ISO/IEC 27005 standard as a reference framework. During this training course, you will also gain a thorough understanding of best practices of risks assessment methods such as OCTAVEn EBIOS, MEHARI, and harmonized TRA. understanding of best practices of risks assessment methods such as OCTAVE, EBIOS, MEHARI, and harmonized TRA. This training course correspods to the implementation process of the IMS framework presented in the ISO/IEC27001 standard.

Using Mitre Att&ck / 1 day

Upon this training, you will be capable to understand how Att&Ck may be used in both detection and reporting in order to strengthen your security posture.

Information Security Governance / 2 days

The objective of the training is to address all the security topics that a CISO can be confronted with and to explain how and why different reference systems can be useful. In addition, the daily problems of a CISO will be addressed. The second day is dedicated to a free exchange around themes chosen by the participants according to their real needs.

APPLICATION SECURITY

Secure Development / 3 days

This training lets students discover the offensive side of Application Security, and learn how to develop secure Web Applications as well as Mobile Applications, including how to code securely through lab-based practical exercises.

SECURITY AWARENESS / 0,5

Real world attackers often target ordinary users as part of their strategy. User buy-in and awareness are essential elements in resisting these attacks. This training includes modules on: Email phishing, Social engineering, Traveling and mobility, and Password management.

Awareness on Infrasttructure Breaches/ 2.5 hours

Upon this training, you will be capable to understand how an intrusion may be realised and take away ideas and feedback to strengthen your security posture.

PECB EC-Council

OXiane