



TRAININGS CATALOG 2019

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 CHALLENGE

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 CATALOGUE SUBSET

● HACKING AND FORENSICS

Build your Csirt / 2 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 kinds 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 malware can 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 and 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.

● 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 day

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.

● DATA PRIVACY

Certified Data Protection Officer / 4 days / Partnership with Oxiane and 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

ISO 27001 Lead Implementer / 5 days / Partnership with Oxiane and 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.