



EVIDEN

Catalogue

Cybersecurity Academy

Learn. Practice. Secure.

Edito

With a cyber-attack occurring every eleven seconds worldwide, no industry nor company is completely safe. Also, as the impact's magnitude can be such as it entirely disrupts the business continuity, corporate insurance policies now include terms regarding cybersecurity, and even cyber-specific insurance policies are gaining in importance.

In the meantime, employees serve as the first barrier against cybersecurity threats targeting your most valuable assets. Therefore, they must be aware of all the cyber risks they could encounter as users and be equipped with the right tools and knowledge to be your most efficient frontline defense. Consequently, all members of your staff should be trained regardless of their depth of knowledge in IT and cybersecurity. Nonetheless, ensuring knowledge accessibility and boosting motivation lies in training material with progressive complexity levels.

Pursuing the mission of making the world a cyber-safe place, Eviden has developed a complete cybersecurity training portfolio, with various complexity and technicality levels, to train as many staff members as possible, from non-cyber employees to cybersecurity experts, and from juniors to executives (V-, D- and C-suite).

This effort goes alongside the regulations enacted by global and local institutions to support raising cybersecurity awareness. Recently, some significant European and local regulations have updated the "company size" criteria and therefore widened the field of application of cybersecurity awareness training. Thereby, contributing to the effort of making all businesses cyber-safer, regardless of their size, the European NIS-2 regulation has widened the scope of cybersecurity awareness compliance to small companies.

Nevertheless, regulations are not the only factor that has contributed to what we consider being a "cyber wake-up call" for companies, the reality of the field plays a significant role. Indeed, according to Gartner more than 90% of breaches result from human error. And as the resulting loss of a cyber breach goes up to an average 4.45 million dollars (IBM Data Breach Cost), companies are not required to only train their staff but also to go to the next level to increase their cyber maturity. One of the most effective ways to achieve this goal is to get skilled by experts.



Barbara Thureau




Head of Eviden
Cybersecurity Academy

At Eviden, we believe that the path to a bolstered security is sharing knowledge. Thus, as a cybersecurity key player strengthened with over 6,500 top experts, our top subject-matter experts are the ones who deliver the training. We put the emphasis on methodology, combining theory and practice, with gamification, labs, and case studies.

To support your organizations and staff to keep up with the constantly evolving technological and threat landscape, we deliver exclusive training modules on the latest cybersecurity innovations with our world-class experts on such niche topics.

Start your journey to cyber safety the best way: with Eviden. Joining the Cybersecurity Academy, you will onboard to a path of learning infused with the values of expertise, excellence, and continuous improvement.

Table of contents

Edito	2
Eviden's cybersecurity academy at a glance	6
Our training methodology	6
Our educative team	6
All the courses you need for your staff	7
Training offers	8
 Cyber rise	9
Cybersecurity basics (e-learning)	10
Security awareness	11
Comproission awareness and demonstration	12
Anti-phishing campaigns	13
Anti-smishing campaigns	13
 Hyper-specialized training	14
Post quantum cryptography – introduction	15
Post-quantum cryptography - deep dive	16
Privacy-enhancing technologies – awareness	17
Awareness on security for AI / generative AI	18
Generative AI - fundamentals	19
Generative AI - the technical pentester perspective	20
Secure AI / generative AI development	21
Security for AI / generative AI – the DFIR perspective	22
 Cyber trek	24
Technical awareness on vulnerabilities	25
Certification ISO 27001 – certified lead implementer	26
Certification ISO 27001 – certified lead auditor	27
Certification ISO 22301 – Certified Lead Implementer	28
Certification ISO 27005 – Certified Risk Manager	29
Secure coding	30
Secure design threat modeling	31
SECDEV essentials	32
SECDEV technical	34
OT and IOT	36
IAM - technical	37
PKI basics modules	38

Cloud Security Basics	39
Cloud Security Risk and Governance Training	40
Devsecops for cloud	41
Securing cloud-native container workloads (advanced)	42
Microsoft security fundamentals	43
AWS security fundamentals	44
Security engineering on AWS	45
Google security	46
Initiation to digital footprint	47
Initiation to incident handling	48
Introduction to cybersecurity and is security awareness	49
Initiation to OSINT	51
Intrusion test implementation	52
Installing intrusion detection probes	53
Advanced reconnaissance (including social engineering)	54
Attack surface technical reconnaissance	56
Network security	57
Social engineering awareness	58
Hacking techniques initiation	59
Hacking techniques expertise	60



Security immersion

62

Security immersion – exclusive professional part-time program	63
---	----



Cyber crisis exercise

65

Incident response tabletop exercise	66
Crisis simulation	67



Cyber for executives

69

Cybersecurity awareness for executives	70
EU regulatory compliance: NIS-2/CER directive and DORA regulation for executives	71
EU regulatory compliance: NIS-2/CER directive and DORA regulation for cybersecurity, procurement, and sales teams	72
Holistic approach to ISO standards family	73
Selected techniques of qualitative and quantitative risk analysis	74

Contact us

76

About us

76



Eviden's Cybersecurity Academy briefly

Our training Methodology

As we strongly believe knowledge infuses better with practice, we have designed highly dynamic and interactive training modules.

Our trainers, as world-class subject-matter experts, will take care of challenging each trainee to ensure they fully understand the concepts and their practical implications.

Our methodology mixes theory and practice because we believe that cybersecurity training is the most successful only if the trainees can test their understanding, hesitate or fail, and learn from it by having the possibility to get answers and support from the subject matter expert, and finally try again and succeed.

To have the most compelling, successful, and complete technical training, we rely on senior trainers with a strong pedagogical approach, and the most relevant firsthand exercises and labs.

Pursuing a tailored-to-the-audience approach, our training track reserved to executives focuses on providing your top-management staff with the main keys to understand the most dominant or innovative cybersecurity threats, seize the potential risks and impacts to their business, and raise their awareness thanks to novice-friendly analogies.

Our educative team

To build a relevant curriculum, Eviden has gathered a pedagogical council composed of senior technical experts, CTOs and learning experts. They infused the values of excellence and innovation in the curriculum's courses and contents.

The other key group of contributors to the Eviden Cybersecurity Academy is the trainers. On the one hand, our subject-matter experts are senior professionals in their field, and most of them are already part-time or volunteer trainers in one or several Science and Technology Universities. On the other hand, Eviden leverages its rich network of partners and top providers to efficiently skill the trainees on their cybersecurity products or platforms.



All the courses you need for your staff

Our wide catalogue of cybersecurity training fits and adapts to every company's needs. The average module rolls out over 2 days. Though we offer some express modules of 2 hours, and up to a 6-month professional part-time apprenticeship, "Security Immersion".

To better match the needs of various groups of your staff, each of our modules is adapted to the audience it targets: from juniors and non-cybersecurity employees to executives, including security professionals and experts. Starting with cybersecurity awareness track, "Cyber Rise," we reinforce your workforce with solid knowledge basis of the cybersecurity ecosystem, the behaviors to adopt to both efficiently protect your IT environment and actively defend it against cyber threats, whenever they recognize a signal of attack. Each staff member being a key of your security chain, it is crucial to equip them with the right level of knowledge they must have to turn them into an effective first line of defense and protect your business.

In addition, Eviden selected a few innovative partners to enable your company to have a better success rate in your anti-phishing campaigns. We can deliver in two different formats: either short videos or a full Cyber Awareness Day.

Besides, our technical track, "**Cyber Trek**," is designed especially for your IT and cybersecurity teams to upskill in defensive or offensive security. From junior to senior, this track's courses and exercises are designed with various difficulty levels by the subject-matter experts. To complete the learning, we also offer internationally recognized cybersecurity certifications, including ISO ones.

To catch the technical-hype train, your experts can access our "**Hyper-specialized training**" on the most innovative cybersecurity topics. It offers a focus on the future game-changer technologies and trends that already affect our businesses, like AI, Generative AI, privacy-enhancing technologies (PET), post-quantum cryptography (PQC), etc.

For some areas of cybersecurity that are highly strategic to your organization, we offer a tailored and innovative module, "**Security Immersion**." It allows a defined group of staff to dive into the topics you select. For 6 months, they will alternate between training sessions with us and work time in your company. By learning both the theory and practice, and experience it in their daily job, the trainees have a unique opportunity to assimilate the knowledge while tailored to your company's environment, processes, and tools.

With sixteen SOC and a multi-year experience in securing major events – including the Olympics – Eviden experts have highly-accurate and up-to-date knowledge of the attack techniques and vectors. Their lessons from the battlefield fuel the design of the **Cyber Crisis Exercise** module, to ensure its realism.

Finally, as no link of your cybersecurity chain should ignore how attackers will target them specifically based on their elevated position in the hierarchy, we also designed an exclusive module "**Cyber for executives**" for your D-, V- and C-suite. As decision makers they must grasp the impacts a cyber-attack or weak security posture could have on their business activities and continuity, as well as their workforce, finances, and even reputation.

To make the most of the training and close mentorship, select the on-site option, and our trainers will come to your office locations. Otherwise, for international groups to train, we can also deliver with virtual classes.



Training offers



Cyber Rise – Awareness



Hyper-specialized – Technological trends



Cyber Trek – Technical training



Security Immersion – Professional part-time apprenticeship



Cyber Crisis Exercise



Cyber for Executives



Cyber Rise

Equip all your staff with the cybersecurity core knowledge to efficiently protect your organization and comply with regulations' requirement to run regular cybersecurity awareness training.



Cybersecurity Basics (e-learning)

Reference: CR241

📅 **Duration:** 2 hours, May vary according to your company's' needs

📺 **Delivery:** Online self-learning videos

🧑 **Level:** All

👥 **Audience:** All staff

🌐 Available in **36** languages

General cybersecurity awareness training on the core knowledge your employees need to know and cyber-secure behaviors they should adopt daily.

Objectives

- Strengthen the cyber-risk awareness of your teams.
- Easily and quickly deliver to the broadest audience.
- Provide the cybersecurity essential knowledge to safely work in digital environment.
- For Europe-based companies or entities for which the application of the NIS-2 regulation is effective, cybersecurity training has become necessary to be compliant.

Prerequisites

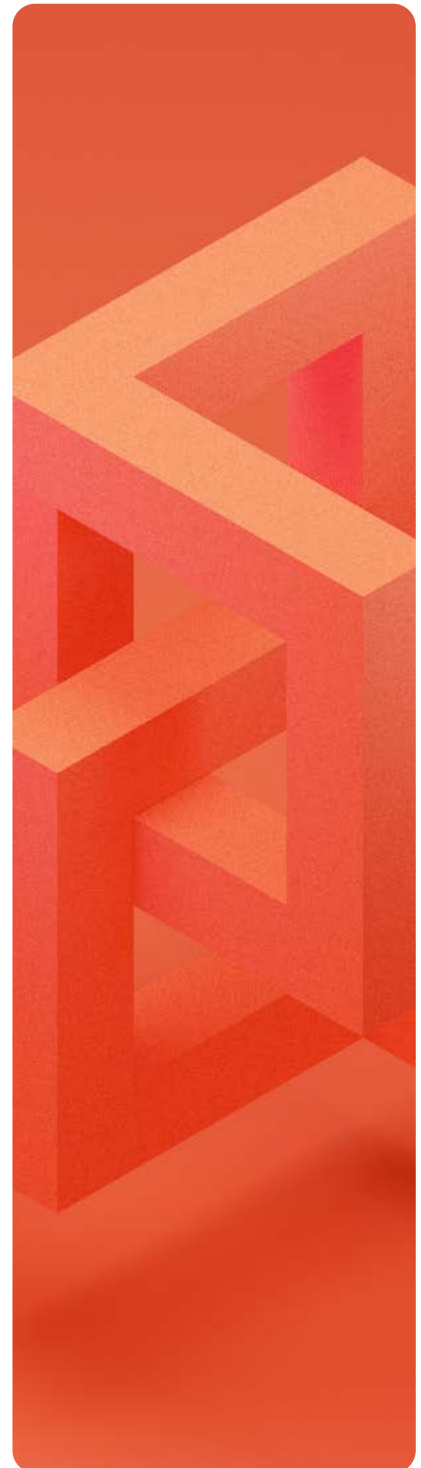
Workshops with the security team to adapt the content to your organization specific environment and existing security practices.

Program

Based on your company's specific needs, our Eviden team will select the most accurate videos that match your staff's maturity in terms of cybersecurity knowledge.


Each learning aims to make your staff more aware of the cyber risks and threats in common situations they encounter daily and adopt the right behavior to reduce the risks weighing on your organization.


Your staff will access short videos – from 5 to 7 minutes each - available in multiple languages and compliant with SCORM, as well as some written materials, on the security awareness basics (e.g., password policy, confidentiality, etc.).




Security Awareness


Reference: CR242

 **Duration:** 2 to 4 hours

 **Delivery:** On-site course / Virtual classroom course / Online course

 **Level:** All

 **Audience:** All staff

 Available in **36** languages

Give your teams a more detailed understanding of the cybersecurity trends, threats, and attack techniques. And tackle more daily-situation use cases.

Objectives

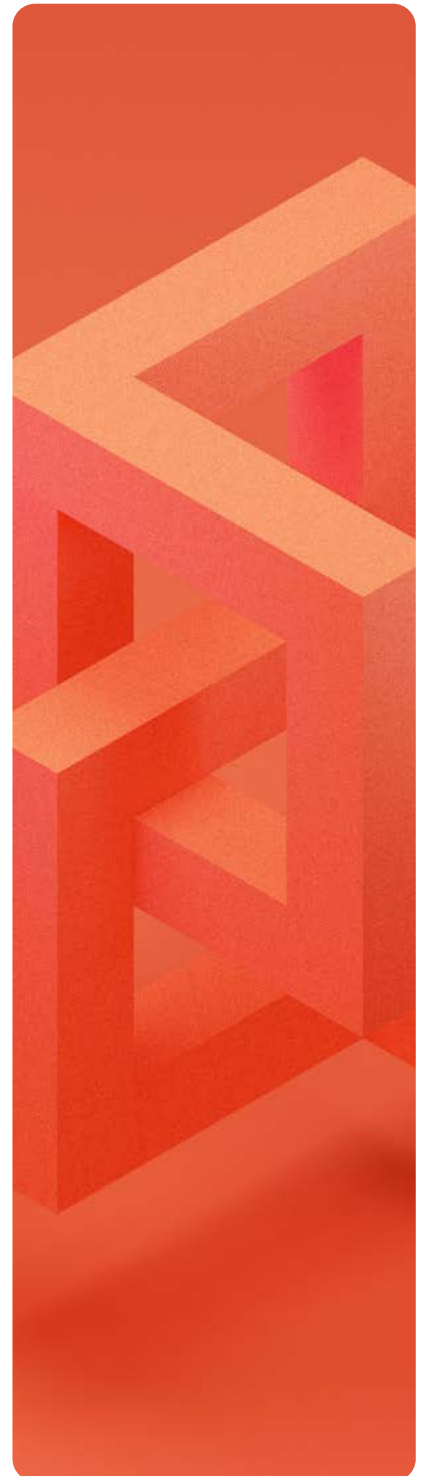
Strengthen the cybersecurity awareness and sharpen your staff's vigilance in usual situations at work.

Prerequisites

None

Program

- Overview of the current cyber threat landscape
- Secure handling of email and phishing
- Secure use of the Internet and malware risks
- Secure handling of data storage and accesses
- Secure handling of endpoints and devices
- Secure handling of confidential information
- Secure interaction with external people
- The conduct to adopt in the event of security incidents



Compromise awareness and demonstration

Reference: CR243

📅 **Duration:** 3 sessions of 25 minutes, all on the same day

🏠 **Delivery:** On-site

👤 **Level:** All

👥 **Audience:** All staff

🌐 **Language:** Only available in French

Objectives

- Understanding the cybersecurity challenges in the enterprise.
- Understand to what cyber-attacks users can be exposed.
- Learn how to detect suspicious behavior.
- Understand the concept of IT hygiene.
- Integrate your business processes with internal users.

Program

- Instant phishing: understanding what a phishing attack is, the risks it bears, how to detect it efficiently, spotting URL shorteners and how to handle them.
- Controlling your equipment: running regular updates (functionality vs. security) and managing non-catalog applications
- The USB moment: our expert will make rubber duckie demonstrations, and how to protect yourself?
- Cybersecurity in your company (customized part): what security behaviors to adopt when telecommuting and in mobility? How to communicate safely with internal contacts? Our experts will share some documentary resources as well.
- Compromise demonstration via USB key and cable



Anti-phishing campaigns

Reference: CR244

📅 **Duration:** Number of campaigns may vary according to your company's needs

📺 **Delivery:** On-site course / Online course

👤 **Level:** Beginner

👥 **Audience:** All staff

🌐 Available in **36** languages

Learning comes with practice, and there is no better option for your security teams to evaluate if your staff has adopted the right cyber-safe behavior, or if they still always need more practice so their awareness peaks.

Objectives

- Improve the phishing awareness of your teams.
- Building a relevant campaign according to your organizational and business context.
- Analyze the failure rate and identifying what element fooled people the most.
- Running an alternative test once again on the staff who failed spotting the phishing email.
- Several campaigns will be running to compare the results and improve the overall security of your company.

Anti-smishing campaigns

Reference: CR245

📅 **Duration:** Number of campaigns may vary according to your company's needs

📺 **Delivery:** On-site course / Online course

👤 **Level:** Beginner

👥 **Audience:** All employees

🌐 Available in **36** languages

This training aims to raise awareness and instill cyber-safe behaviors in your staff when it comes to smishing (i.e., phishing via SMS)

Objectives

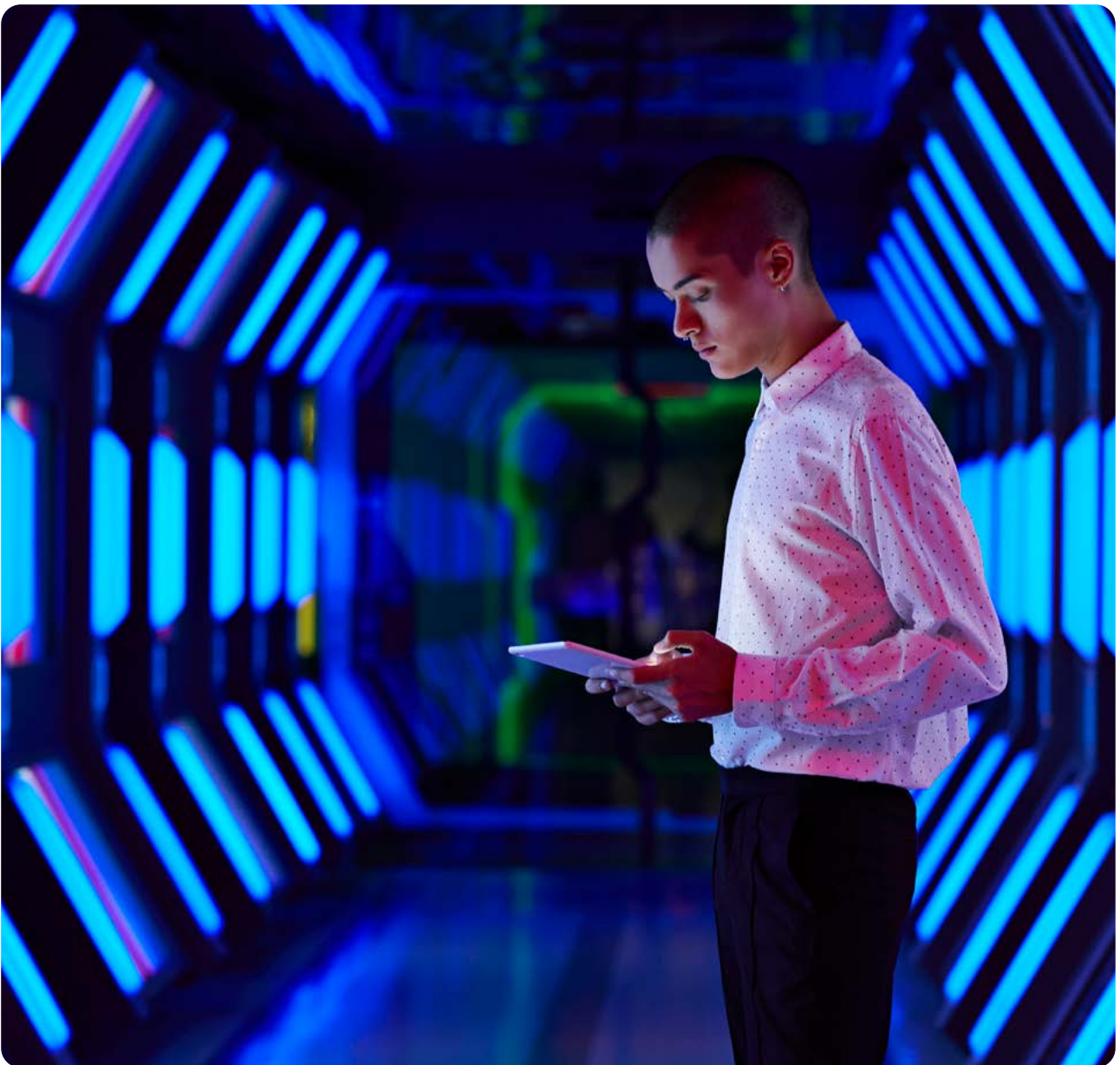
- Given your company's environment and business, your staff will be served with a highly accurate and compelling smishing campaign.
- Identify what elements of the malicious SMS triggered an unsafe behavior (e.g., clicking, sharing sensitive data or PII).





Hyper-specialized training

Broaden the cybersecurity perspectives of your teams with training modules on the latest technological trends.



Post Quantum Cryptography – Introduction

Reference: HS241

📅 **Duration:** 2 to 4 hours

📺 **Delivery:** On-site course / Online course

👥 **Audience:** depends on the modules (see below)

🌐 **Language:** English and French

Module 1: What is PQC, why it is important and how complex will the migration be?

Audience: All

Prerequisite: Basic knowledge in IT

Objective: Understand the impact of Quantum Computing on cybersecurity, both the critical importance and the complexity of the upcoming PQC migration program organizations.

Program:

- What is asymmetric cryptography and for what it is used.
- Why are Quantum computers a threat, and the new possible attacks they enable (i.e., “Store Now, Decrypt Later”), and the danger of leaving any copy encrypted with non-Quantum-safe algorithms.
- the possible responses to the Quantum risk.
- The status of the PQC schemes and then, of communication protocols, systems, and applications.
- The migration complexity (crypto agility, risk assessment, vendor management, skills scarcity, etc.).
- Main steps of the migration program (executive sponsorship, program setup, cryptographic inventory, technical tests, risk assessment, applications prioritization, etc.).

Module 2: PQC status and challenges

Audience: Technical staff, (IT and/or cybersecurity teams)

Prerequisite: Basic knowledge on cryptography

Objective: Understand the status of PQC schemes and dependent protocols and standards.

Program:

- Provide a brief history and status of the NIST competition and standardization.
- Address cryptanalysis (SIKE example...).
- Explain hybridization strategies (national security agencies' recommendations, why, ongoing work...) with a focus on X.509 hybrid certificates.

Zoom on the impact on network protocols (TLS/HTTPS/DoH, DNSSEC, IPSEC/IKE...) and 5G protocols (cf. ETSI work). As well as other protocols (SCEP, CMS, SSH, OCSP, JWT, OpenPGP, ACME, S/MIME, etc.).



Post-Quantum Cryptography - Deep dive

Reference: HS242

📅 **Duration:** 2h to 0.5 day

📺 **Delivery:** On-site course / Online course

🧑 **Level:** Beginner

👥 **Audience:** Encryption Security specialist (not Cryptographers but encryption implementer)

🌐 **Language:** English and French

Module 1: PQC algorithms families and implementations

Objective: Understand the status of PQC schemes and dependent protocols and standards

Program:

- Present some primitives: lattice-based, hash-based, code-based SHA3.
- Describe some algorithms for lattice-based schemes.
- Overview of existing libs for PQC, overview of existing competitions, impact on protocols, and latency.
- PKI Basic training.
- Impact of PQC in PKI: new algorithms PQC, impact on certificates format, CRL, link with HSMS.

Module 2: PQC status and challenges

Objective: Understand the arithmetic differences with RSA and have hand-on exercise on an open-source implementation.


Program:

- Show how to compile the Open Quantum Safe lib (OpenSSL compatible open-source implementation) and integrate it into OpenSSL3.
- Describe the arithmetic differences with RSA, introducing some Risc-V HW implementations.
- Theoretical presentation of the various operations needing acceleration and a few open-source HW and RISC-V implementation projects.




Privacy-enhancing technologies – Awareness

Reference: HS243

 **Duration:** 1 week (Five 90-minutes sessions on the platform, split over 5 days and an additional design thinking session with experts)

 **Delivery:** Online course + Virtual final session live

 **Level:** Beginner and Intermediate

 **Audience:** Cybersecurity or IT staff

 **Language:** English and French

Dive into the world of data privacy with an engaging escape game!

By 2025, **60% of large organizations** will be using PETs as they are essential to ensure data privacy throughout its entire lifecycle – **collection, processing, analysis, and sharing**. This includes protecting **sensitive data** even in untrusted environments, complying with regulations on personally identifiable information (PII), and enabling collaboration while safeguarding privacy. PETs offer a diverse toolbox, encompassing techniques like:

- **Data transformation** through data generation, data perturbation or data cryptography.
- **Data-in-use security** through encryption (including in use, with homomorphic encryption) or secure and private environments.
- **Privacy-preserving mechanisms** for sharing data, building analytics, and collaboratively leveraging the results.

While the **vast array of PET solutions** may seem overwhelming, this escape game equips you with the knowledge and skills to **confidently embark on your data privacy journey**.

Objective: Understand the impact of Quantum Computing on cybersecurity, both the critical importance and the complexity of the upcoming PQC migration program organizations.

Program:

- **Gain technical knowledge:** Learn about various PET technologies, identify best combinations for your specific needs, and make informed decisions about choosing the right ones.
- **Explore real-world applications:** Discover concrete examples of PETs used in diverse scenarios, sparking inspiration for your own organization.
- **Navigate the market:** Gain visibility into different PET categories and vendors, understanding the landscape and selecting the best fit for your needs.
- **Develop a roadmap:** Participate in a design thinking session with cybersecurity and PET experts to craft a personalized roadmap for implementing PETs in your organization.

Prerequisites:

- No prior knowledge of cryptography required. The game is designed to be understandable for all profiles, without having to code.
- Those working in the fields of data, cryptography, security, or AI/ML will find this game particularly valuable in building their awareness.



Program:

The game scenario

This escape game will enable your team to understand PET usage, potential benefits, underlying technologies through fun and insightful daily challenges that include:

- Lectures
- Guided demonstrations of vendor's solutions
- Quizzes

The design thinking session

During the live session, Eviden experts will answer questions submitted during the game and help your team determine the PET value specific to your domain and usage.

Awareness on Security for AI / Generative AI


Reference: HS244

 **Duration:** 1 hour

 **Delivery:** on site / online

 **Level:** Beginner / Intermediate / Advanced / Expert

 **Audience:** All staff

 **Language:** English, French and German

This training will provide your team with the definition of AI / generative AI and its use cases, as well as raise their awareness on the associated risks and regulations. Finally, your staff will understand what behaviors to adopt to safeguard your organization from AI-generated attacks.

Objectives:

- Provide an overview of AI / Generative AI security and its importance.
- Raise awareness of potential AI/Generative AI breaches.
- Encourage participants to take steps to improve their AI safety posture.

Program:


- Overview of AI and Generative AI, and its relationship with cybersecurity.
- Study of proven security incidents and their impacts.
- Solutions to guard against risks linked to technical and human vulnerabilities in AI and Generative AI.



Generative AI - Fundamentals


Reference: HS245

 **Duration:** 3 days

 **Delivery:** on site / online

 **Level:** Beginner / Intermediate / Advanced / Expert

 **Audience:** C-suite / VP / Directors / CISO / DPO

 **Language:** English, French and German

Gain knowledge on GRC topics related to AI and Generative AI

Objectives:

- Provide an overview of AI and Generative AI Fundamentals
- Acquire Vocabulary / Taxonomy / Glossary
- Understanding the Data Lifecycle
- Gaining understand of AI / Generative AI Specific risks.
- Expanding risks outside of cybersecurity

Prerequisites:

- Basic AI / Generative AI knowledge
- Experience in cybersecurity Governance

Program:

Generative AI Fundamentals

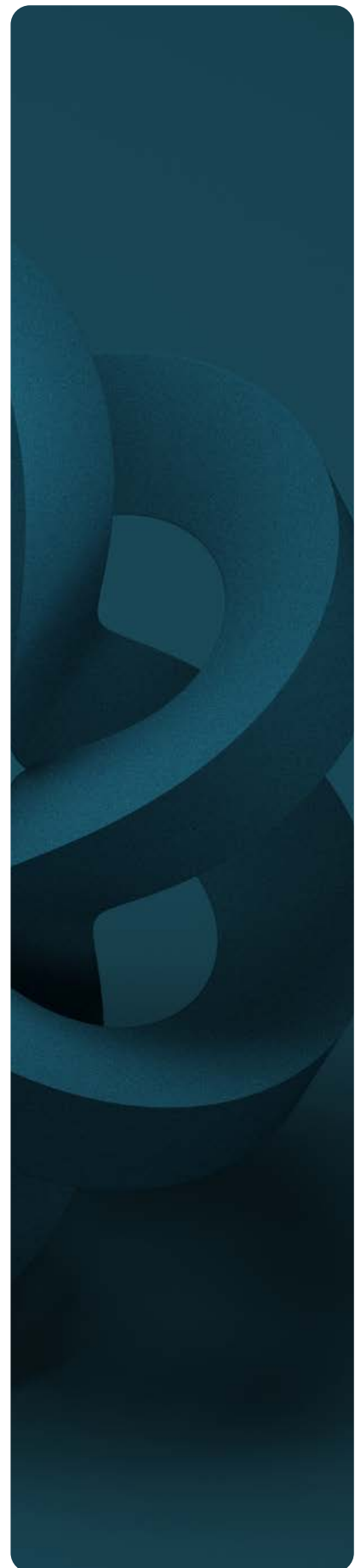
- AI Definition and Classification
- AI Project Lifecycle
- MLOps introduction
- Differences between AI and Generative AI
- AI place in Information System

CISO's perspectives

- AI risks & Opportunities
- Shadow AI
- Ethical Risks: On the road to AI Act
- MS Copilot CISO: AI as a tool

GRC Perspective

- Governance: ISO 42001
- Risk management: NIST AI RMF, Google SAIF
- Compliance: GDPR, AI Act, ENISA Certification



Generative AI - the Technical Pentester Perspective

Starting on September 2024

Reference: HS246

📅 **Duration:** 1 or 2 days

📺 **Delivery:** On-site course / Online course

👤 **Level:** Intermediate / Advanced / Expert

👥 **Audience:** Pentesters / Cybersecurity Staff / Offensive security / RED & Purple Teams

🌐 **Language:** English, French and German

Objectives:

- AI Definition and Classification
- Provide an overview of AI and Generative AI Fundamentals
- Acquire Vocabulary / Taxonomy / Glossary
- Understanding the Data Lifecycle
- Understanding how to pentest an AI model

Prerequisites:

- Basic AI / Generative AI knowledge
- Penetration Testing Experience

Program:

- Surface Attack
- OWASP Top 10 LLM & ML
- Attacks Examples
- AI Enabled Tools
- AI Project Lifecycle
- MIOps introduction
- Differences between AI and Generative AI
- AI place in Information System





Secure AI / Generative AI Development

Starting on September 2024


Reference: HS247

 **Duration:** 2 days

 **Delivery:** on site / online

 **Level:** Intermediate in Cybersecurity or Data

 **Audience:** Cybersecurity or Data scientist

 **Language:** English, French and German

Objectives:

- Operationalizing MLSecOps
- Provide an overview of AI and Generative AI Fundamentals
- Acquire Vocabulary / Taxonomy / Glossary
- Understanding the Data Lifecycle

Prerequisites:

- Basic AI / Generative AI knowledge
- Secure Software Development Lifecycle (SSDLC) / DevSecOps Experience

Program:

- MLOps Introduction
- MLSecOps
- Ethics By Design
- Open-Source Tools
- AI Definition and Classification
- AI Project Lifecycle
- MLOps introduction
- Differences between AI and Generative AI
- AI place in Information System



Security for AI / Generative AI – The DFIR perspective

Starting on September 2024

Reference: HS248

📅 **Duration:** 2 days

📺 **Delivery:** on site / online

🧠 **Level:** Beginner in AI or Cybersecurity

👥 **Audience:** Cybersecurity or IT staff

🌐 **Language:** English, French and German

Objectives:

- Gain knowledge on AI and Generative AI
- Provide an overview of AI and Generative AI Fundamentals
- Acquire Vocabulary / Taxonomy / Glossary
- Understanding the Data Lifecycle

Prerequisites:

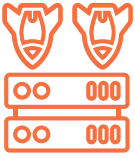
- Basic AI / Generative AI knowledge
- DFIR / CERT / SOC Experience

Program:

- MITRE ATLAS™ (Adversarial Threat Landscape for Artificial-Intelligence Systems)
- AI-enabled SOC / SOAR
- Examples of AI-enabled Attacks and how to protect from them
- AI Definition and Classification
- AI Project Lifecycle
- MIOps introduction
- Differences between AI and Generative AI
- AI place in Information System







Cyber Trek


A full range of technical training modules to ensure your cybersecurity teams to get world top certifications and hands-on practice with world-class experts.



Technical awareness on vulnerabilities


Reference: CT241

 **Duration:** 1 day

 **Delivery:** On-site course

 **Level:** Beginner / Intermediate / Advanced / Expert

 **Audience:** Software architects, software designers, and project managers

 **Language:** English, French and German

This training module covers the essentials to know when it comes to cybersecurity vulnerabilities and assets or vectors that could represent an entry point to your IT system for attackers.

Objectives:

- Understand the main technical cyber concepts.
- Adopt a secure way of working.

Program:

- Awareness/war stories
- Top vulnerabilities according to OWASP
 - » Cross site scripting XSS
 - » Same origin Policy
 - » Cross site request forgery
 - » SQL injection
 - » Remote command execution
 - » External Entity injection
 - » File upload
 - » Path traversal
 - » Authentication / session Management
- Management of Passwords
- Consequences of non-compliance, breaches, and relevant legislation



Certification ISO 27001 – Certified Lead Implementer

 **Reference:** CT242

 **Duration:** 5 days

 **Delivery:** On-site course / Virtual classroom course / Online course

 **Level:** All

- Audience: Managers or consultants involved in information security management.
- Information Security Management System (ISMS) team members.
- Specialized consultants handling the implementation of an ISMS.
- Staff members responsible for maintaining compliance with ISMS requirements.

 **Language:** Language: Available only in French

Once you have mastered the concepts of Information Security Management Systems, you can sit the exam and apply for the title of “PECB Certified ISO/IEC 27001 Lead Implementer”. With PECB certification, you will demonstrate that you have the practical knowledge and professional skills to implement ISO/IEC 27001 in an organization. This training course is based on both theory and best practices used for ISMS implementation. The lectures are illustrated by case study examples. Practical exercises are based on a case study which includes role-playing and oral presentations. Practical tests are like the certification exam.

Objectives:

- Understand the correlation between ISO/IEC 27001 and ISO/IEC 27002, as well as with other standards and regulatory frameworks.
- Master the concepts, approaches, methods, and techniques needed to effectively implement and manage an ISMS.
- Interpret the requirements of ISO/IEC 27001 in an organization’s specific context.
- Support an organization in planning, implementing, managing, monitoring, and maintaining an ISMS.
- Acquire the expertise needed to advise an organization on the implementation of Information Security Management System best practices.

Prerequisites:

- Good knowledge of ISO/IEC 27001 and in-depth understanding of the principles of implementation.

Program

- Day 1: Introduction to ISO/ IEC 27001 and ISMS initialization
- Day 2: ISMS implementation planning
- Day 3: ISMS implementation
- Day 4: Monitoring, measurement, continuous improvement, and preparation for the ISMS certification audit
- Day 5: Certification exam

Certification ISO 27001 – Certified Lead Auditor

 **Reference:** CT243

 **Duration:** 5 days

 **Delivery:** On-site course / Virtual classroom course / Online course

 **Level:** All

 **Audience:**

- Auditors wishing to carry out and lead Information Security Management System certification audits.
- Managers or consultants wishing to master the ISMS audit process.
- Staff members responsible for maintaining compliance with ISMS requirements.
- Technical experts wishing to prepare an Information Security Management System audit.
- Consultants specializing in information security management.

 **Language:** Available only in French

Once you have mastered the audit concepts demonstrated and passed the exam, you can apply for PECB Certified ISO/IEC 27701 Lead Auditor certification. This internationally recognized certification demonstrates that you have the expertise and skills to audit organizations based on best practice. - This training course is based on both theory and best practices used in ISMS auditing - Lectures are illustrated by case study examples - Practical exercises are based on a case study that includes role-playing and oral presentations - Practical tests are like the certification exam.

Objectives:

- Understand how an Information Security Management System (ISMS) compliant with ISO/IEC 27001 works.
- Explain the correlation between ISO/IEC 27001 and ISO/IEC 27002, as well as with other standards and regulatory frameworks.

Understand the role of an auditor:

- plan, conduct and follow up a management system audit in accordance with ISO 19011.
- lead an audit and an audit team.
- interpret the requirements of ISO/IEC 27001 in the context of an ISMS audit.
- acquire the skills of an auditor to plan an audit, conduct an audit, draft reports, and follow up an audit, in accordance with ISO 19011.

Prerequisites:

- Good knowledge of ISO/IEC 27001 and in-depth knowledge of auditing principles

Program

- Day 1: Introduction to the Information Security Management System and the ISO/CEI 27001 standard.
- Day 2: Audit principles, preparation, and initiation.
- Day 3: On-site audit activities.
- Day 4: Closing the audit.
- Day 5: Certification exam.

Certification ISO 22301 – Certified Lead Implementer

 **Reference:** CT244

 **Duration:** 5 days

 **Delivery:** On-site course / Virtual classroom course / Online course

 **Level:** All

 **Audience:**

- Managers or consultants involved in business continuity management.
- Specialized consultants wishing to master the implementation of a Business Continuity Management System.
- Staff members responsible for maintaining compliance with BCMS requirements.
- Members of a BCMS team.

 **Language:** Available only in French

Once you have mastered the concepts of Business Continuity Management Systems, you can sit the exam and apply for the title of “PECB Certified ISO 22301 Lead Implementer”. With PECB certification, you will demonstrate that you have the practical knowledge and professional skills to implement ISO 22301 in an organization. - This training course is based on both theory and best practices used in the implementation of SMCA - Lectures are illustrated by examples based on a case study. The practical exercises are based on a case study which includes role-playing and oral presentations. And the practical tests are like the certification exam.

Objectives:

- Understand the correlation between ISO 22301 and other standards and regulatory frameworks.
- Master the concepts, approaches, methods, and techniques needed to effectively implement and manage an SMCA.
- Interpret the requirements of ISO 22301 in an organization's specific context.
- Know how to support an organization in planning, implementing, managing, monitoring, and maintaining the SMCA.
- Acquire the expertise needed to advise an organization on the implementation of Business Continuity Management System best practices.

Prerequisites:

- A good knowledge of ISO 22301 and in-depth understanding of the principles behind its implementation.


Program

- Day 1: Introduction to ISO 22301 and SMCA initialization
- Day 2: SMCA implementation planning
- Day 3: SMCA implementation
- Day 4: Monitoring, measurement, continuous improvement, and preparation for the SMCA certification audit
- Day 5: Certification exam

Certification ISO 27005 – Certified Risk Manager

 **Reference:** CT245

 **Duration:** 3 days

 **Delivery:** On-site course / Virtual classroom course / Online course

 **Level:** All

 **Audience:**

- Information security managers or team members
- Staff members responsible for information security, compliance, and risk in an organization
- Staff members implementing ISO/IEC 27001, wishing to comply with ISO/IEC 27001 or involved in a risk management program.
- IT consultants or professionals
- Information Security or Data privacy officers

 **Language:** Available only in French

Once you have understood all the necessary concepts of information security risk management based on ISO/IEC 27005, you can sit the exam and apply for “PECB Certified ISO/IEC 27005 Risk Manager” certification. By holding a PECB Risk Manager certificate, you will be able to demonstrate that you have the skills and knowledge to carry out an optimal information security risk assessment and manage information security risks in a timely manner.

Objectives:

- Understand the relationship between information security risk management and security measures.
- Understand the concepts, approaches, methods, and techniques that enable an effective risk management process that complies with ISO/IEC 27005.
- Know how to interpret the requirements of ISO/IEC 27001 in the context of information security risk management.
- Acquire the skills to effectively advise organizations on best practices in information security risk management.

Prerequisites:

- A fundamental understanding of ISO/IEC 27005 and an in-depth knowledge of risk assessment and information security.


Program


- This course is based on both theory and best practices used in information security risk management.
- Course sessions illustrated by examples based on case studies.
- Practical exercises based on a case study that includes role-playing and discussions.
- Final practical mock exams to prepare for the certification exam.

Secure coding


Reference: CT246

 **Duration:** 2 days

 **Delivery:** On-site course / Virtual classroom course / Online course

 **Level:** Advanced / Expert

 **Audience:** Software developers and software testers

 **Language:** English, French and German

Defensive security training to embed security in every code development and protect from malicious injections.

Prerequisites:

- Knowing a programming language.


Program


- Awareness / War stories
- Input Validation / Output Sanitization
- BURP Proxy - Basic Security Testing Tool
- Top Vulnerability Classes / Security Concepts
 - » Cross-Site Scripting (XSS)
 - » Same Origin Policy (SOP)
 - » Cross-Site Request Forgery (CSRF)
 - » SQL Injection
 - » Remote Command Execution (RCE)
 - » External Entity Injection (XXE)
 - » File Uploads
 - » Path Traversal
 - » Authentication / Session Management
- Management of Passwords

Secure design threat modeling

Reference: CT247


 **Duration:** 1 day

 **Delivery:** On-site course / Virtual classroom course / Online course

 **Level:** Advanced / Expert

 **Audience:**

- Software architects and software developer
- Application owners
- Quality managers
- Pentesters
- Requirements engineers

 **Language:** English, French and German

Program


- Awareness - Why security matters
- Overview of the application security management process
- Goals and benefits of threat modeling
- Threat modeling in theory
- Threat modeling in practice using case studies



SECDEV Essentials


Reference: CT248

 **Duration:** 1 day

 **Delivery:** On-site course / Virtual classroom course / Online course

 **Level:** All

 **Audience:** Management/Project Manager/Tech Lead / Lead Dev/IT or security team

 Available only in French

In a context of increased usage of applications, security is nonetheless often forgotten in the DevSecOps project flow. This training module offers your staff members with an in-depth coverage of SEC DEV concepts.

Objectives:

- Understand the challenges of application security.
- Understand the most common application vulnerabilities.
- Determine an application's attack surface.
- Understand how security is integrated into the SDLC.
- Monitor the security level of an application.

Prerequisites:

- General computer literacy

Program

Background and objectives

- Why application security?
- Standards and regulations
- General ISS concepts
- Web application architectures

Vulnerabilities in applications

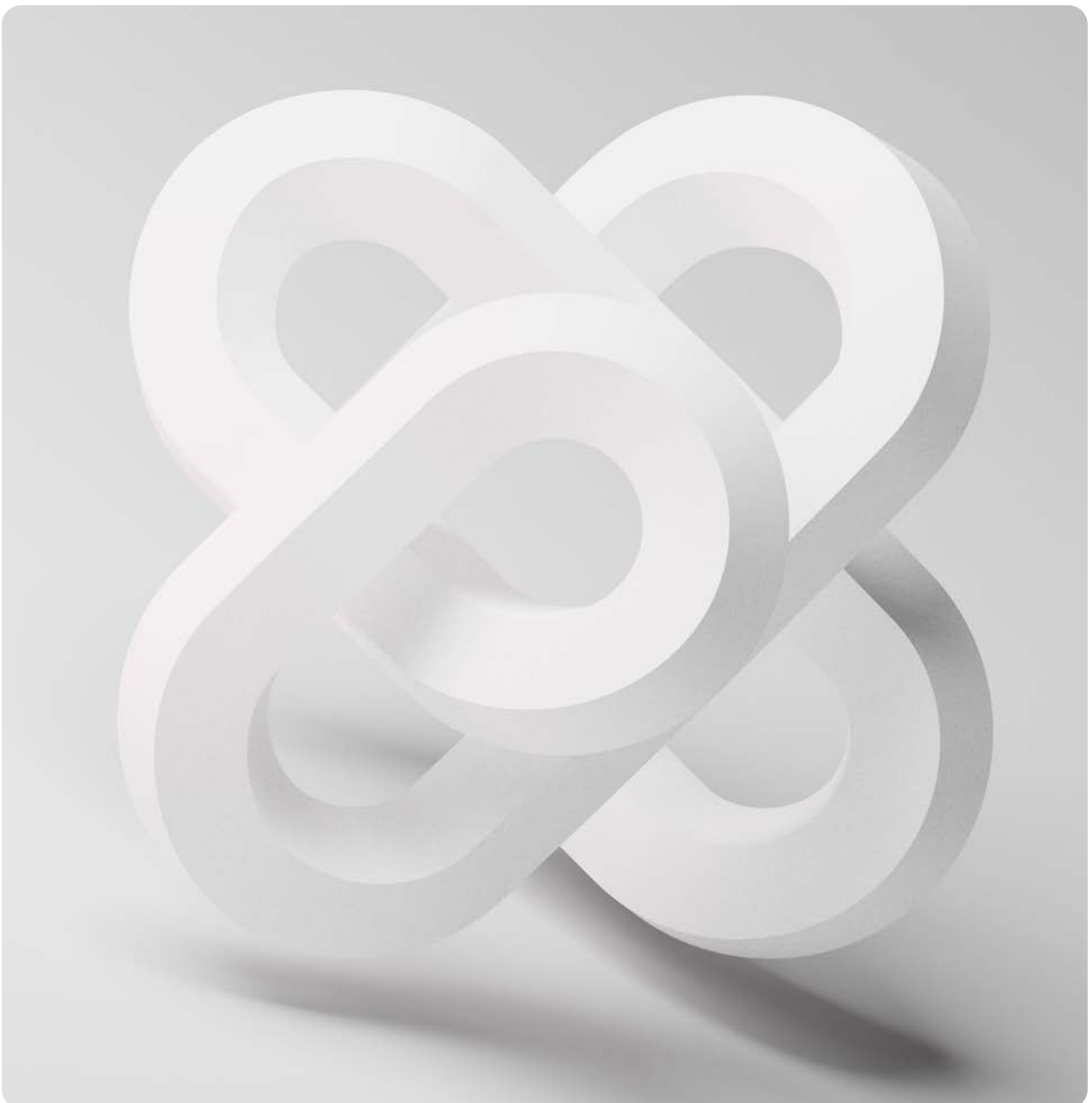
- Introduction to OWASP and the top 10
- New public vulnerabilities (CVE)
- Scaling systems (CVSS)
- How to analyze an application
- Presentation of vulnerability discovery tools
- Understanding the main application vulnerabilities
- Topics covered:
 - » Recognition and analysis
 - » Access and session management
 - » User input management
 - » Application logic
 - » Environment

Supporting project teams

- Understanding corrective and preventive measures
- How can we help developers secure their code?
- Presentation of development tools
- Guides to best development practices

Monitor the security level of your applications


- Application vulnerability management
- Static and dynamic code auditing
- SSI Dashboard
- Presentation of monitoring tools




SECDEV Technical

Reference: CT249

 **Duration:** 2 days

 **Delivery:** On-site course / Virtual classroom course / Online course

 **Audience:** Dev team / test team / Tech Lead / Lead Dev

 Available only in French

Objectives:

- Understand the challenges of application security in a web environment.
- Understand the most common application vulnerabilities.
- Determine the attack surface of a web application.
- Understand the means of correction, security, and prevention.
- Understand how to integrate security into the SDLC.

Prerequisites:

- Expert in the programming language to be covered in the session.
- Available languages: C++ / Java / Python / Node.js / .NET / PHP / Ruby / Go / Spring.

Program

Background and objectives

- Why application security?
- Standards and regulations
- General ISS concepts
- Web application architectures

Vulnerabilities in applications

- Introduction to OWASP and the top 10
- New public vulnerabilities (CVE)
- Scaling systems (CVSS)
- How to analyze an application
- Presentation of vulnerability discovery tools

Vulnerabilities and countermeasures

- Secure development exercises (corrections and tests on a platform dedicated to each participant)
- Technical demonstrations of vulnerability exploitation
- Recognition and analysis: identification of technologies used, technical information leaks, user enumeration, directory indexing, etc.
- Access and session management: client- and server-side access control, cryptographic callback, session token security, user self-registration, security event notification, user session logout...
- User input management: file upload, path traversal, injection (SQL, XML and HTTP headers), XSS, CSRF vulnerabilities, lack of client- and server-side data validation...
- Application logic: multi-stage process bypass, incomplete parameter handling, race condition, CORS...

Environment: Vulnerabilities in dependencies, resource allocation, local storage of sensitive data, clickjacking, use of HTTPS protocol, global variables, sensitive values and comments in code, logging, traces, and auditing.

Security resources

Guides to best development practices

Code reviews

Development tools presentation



OT and IOT

 **Reference:** CT2410

 **Duration:** 9 hours

 **Delivery:** Virtual classroom course / Online course

 **Level:** Beginner / Intermediate

 **Audience:** All staff

 **Language:** English

Objectives:

- Foundational Level knowledge about OT, IoT, and IIoT and their specifics

Prerequisites:

- Understanding of Cybersecurity, IT, and OT terminology
- Understanding IT and OT Business scope

Program

Module 1: IT, OT, IoT, & IIoT Explained

The module explains the similarities, differences & priorities of IT, OT, IoT, & IIoT

Module 2: Business Process within an OT environment

The module explains what a business process is, what it looks like in OT environments, and how is it influenced by the risk management process based on NIST CSF

Module 3: OT Best Practices & Regulatory Review

The module explains what the best practices, frameworks, standards, and regulations are applicable in OT (NIS2 Directive, NIST CSF, C2M2, ISA/IEC 62443, C2M2, NIST, ISO 27000)

Module 4: OT Network Deployment structures & The Purdue Model and Management Systems

The module focuses on network types, network security, and network communication protocols characteristic of OT.

The second part of the module explains what a Purdue Model is and what systems are part of it.

Module 5: Industry 4.0 and the Manufacturing Site within OT & Supply Chain and External Dependencies within OT

The module explains what the industry 4.0 is, and what the four industrial revolutions are.

The second part of the module explains how suppliers and their risks are being managed. It deep dives into the concept of ICS Supply Chain Risks.

Module 6: OT Common attacks, attack vectors, and threat agents & OT Incident Kill Chain & Security Management


The module explains common attack vectors, and threat actors and how to analyze security incidents in their distinct phases of the incident kill chain.


Module 7: OT E2E Security Landscape

The module explains how defense in depth can be delivered E2E in an OT environment with different OT security solutions to protect the OT assets from threats.

IAM - Technical

 **Reference:** CT2411

 **Duration:** 1 day – 8 hours

 **Delivery:** Virtual classroom course / Online course

 **Level:** Beginner / Intermediate

 **Audience:** All staff / Cybersecurity or IT staff / C-suite / VP / Directors

 **Language:** English

This training is designed to provide its audience general orientation on key aspects of Identity and Access Management layer, so that they could more effectively address their business needs in IT organization and understand potential dependencies for their processes.

Objectives:

- Theoretical overview on IT technical fundamentals.
- Understanding of basic IT/ Security terminology.
- Creation of general orientation regarding IAM role in IT systems.
- Definition of recommended best practices which are coming from IAM field, and which can support business processes.

Prerequisites:


- Not mandatory but nice to have basic knowledge related with IT: internet and networks, Active Directory, Cloud concepts, ITIL framework, etc.

Program


- Digital Identity and its function including their types.
- Access from security perspective which is including concepts like (RBAC, 2FA, MFA, PAM).
- Difference between on-premises (AD) and cloud environments.
- Basic concepts of network and internet applications.
- Managed security services – including ITIL processes.
- IAM as core element of security model.


PKI Basics Modules

 **Reference:** CT2412

 **Duration:** 1 day / 4 hours

 **Delivery:** Virtual classroom course / Online course

 **Level:** Beginner / Intermediate

 **Audience:** Staff members involved or interested in implementing a PKI solution (Security Managers, CISOs, Project Managers, Architects, System and Network Administrators)

 **Language:** English and French

Objectives:

- Discover certificates and their lifecycle.
- Understand technologies and cryptography norms.
- Understand PKI organization.

Prerequisites:

- Basic university training or computer engineer or equivalent through experience.


Program

- Basics of cryptography.
- Implement cryptography.
- Introduction to the PKI concepts.
- PKI and organization.
- The structure of the PKI.
- Hierarchy of authority.
- Certification authority.
- Legal and regulatory framework.

Cloud Security Basics

 **Reference:** CT2413

 **Duration:** 2 sessions of 4 hours (on two consecutive days)

 **Delivery:** Virtual classroom course

 **Level:** Beginner / Intermediate

 **Audience:** Cybersecurity or IT staff / C-suite

 **Language:** English and German

Attackers can reach 70% of essential assets in on-premises networks within merely three steps. The situation is even more dire in cloud environments, where 90% of critical assets are a single step away from an initial breach ((Source: XM Cyber 2023).

As part of the event, participants will be introduced to basic security requirements and security best practices in the use of cloud services, which automatically contributes to a reduction in the attack surface. By participating in the basic cloud security training course, participants will be given the necessary tools to understand the security requirements in the cloud. They will gain the knowledge to understand and address cloud security risks to create a secure environment for their environment for their data and services in the cloud.

Objectives:

- Learn the basics of cloud technology.
- Understand key cloud security principles.
- Discover various cloud security tools and technologies.
- Monitor and manage security incidents.
- Apply cloud security concepts through a case study.
- Explore encryption and key management in cloud settings.
- Discuss a real incident to learn from practical security scenarios.

Prerequisites:

- High-Level Cloud Know-How


Program

- Introduction to cloud technology
- Cloud security concepts
 - » CIA-Triade, Shared Responsibility Model, Defense in Depth, Zero Trust, IAM
- Cloud security tools and technologies
 - » CSPM, CWPP, CNAPP, network security, security incident monitoring
- Case study (Homework)
- Risk management, compliance, and legal aspects
 - » C5, Schrems, DSGVO
- Cloud encryption and key management
 - » BYOK, HYOK, BYOE
- Business continuity
- Discussion of a real incident

Cloud Security Risk and Governance Training

 **Reference:** CT2414

 **Duration:** 2 to 3 days

 **Delivery:** On-site course / Virtual classroom course / Online cour

 **Level:** Beginner

 **Audience:**

- Cybersecurity or IT staff
- Information security professionals
- Cloud security architects
- Risk management and GRC professionals

 **Language:** English and German

In-depth coverage of cloud security governance, including risk management, identity management, data security, and compliance.

Objectives:

- Mastering cloud security fundamentals, risk assessment methodologies, compliance controls, and designing effective cloud security architectures.

Prerequisites:

- Basic cloud computing and security knowledge, with experience in information security or risk management beneficial but not mandatory.


Program

- Cloud computing basics.
- Security fundamentals.
- Governance.
- Risk management.
- Identity and access management.
- Legal frameworks.


DevSecOps for Cloud

 **Reference:** CT2415

 **Duration:** 2-3 days

 **Delivery:** In-person or virtual classroom course

 **Level:** All

 **Audience:** Cybersecurity or IT staff interested in integrating security into DevOps practices, particularly suitable for multi-cloud and application security including CNAPP.

 **Language:** English and German

Implementation of DevSecOps processes, tools, techniques, and integration into CI/CD pipelines.

Objectives:

- To learn DevSecOps processes, creating and maintaining pipelines using various security tools and practices.

Prerequisites:

- Knowledge of basic Linux commands and understanding of application security practices like OWASP Top 10. No prior experience with DevOps tools is needed.

Program

- Covers DevOps principles, tools like Gitlab, Docker, Ansible, secure SDLC, software component analysis, static and dynamic analysis, and infrastructure as code.

Securing cloud-native container workloads (Advanced)

Reference: CT2416

📅 **Duration:** 2-3 days

🎓 **Delivery:** In-person or virtual classroom course

🧑 **Level:** All

👥 **Audience:** Cybersecurity or IT staff, Cloud security engineers and architects

🌐 **Language:** English and German

Best practices for securing container-based applications and Kubernetes platforms during build, deployment, and runtime.

Objectives

- Demonstrate competence in Kubernetes and cloud security in a real-world environment.

Prerequisites:

- Experience in containers and container orchestration, including and cloud security.

Program

- Covers cluster setup, hardening, system hardening, minimizing microservice vulnerabilities, supply chain security, and monitoring, logging, and runtime security.



Microsoft Security Fundamentals

Reference: CT2417

📅 **Duration:** 1 day

🖥️ **Delivery:** On-site course / Virtual classroom course / Online course

👤 **Level:** Beginner

👥 **Audience:** Cybersecurity or IT staff new to Microsoft cloud and security, including cloud and security engineers.

🌐 **Language:** English and German

Foundational knowledge on security, compliance, and identity concepts plus Microsoft solutions.

Objectives:

- Understanding of Microsoft security, compliance, and identity solutions across various solution areas.

Prerequisites:

- General understanding of networking, cloud computing, Microsoft Azure, and Microsoft 365.

Program

- Covers security, compliance, and identity concepts; Microsoft Entra capabilities; Microsoft Security solutions; and Microsoft compliance solutions.



AWS Security Fundamentals

Reference: CT2418

📅 **Duration:** 3 hours

📺 **Delivery:** On-site course / Virtual classroom course / Online course

👤 **Level:** Beginner

👥 **Audience:** Cybersecurity or IT staff experienced cloud and security engineers specializing in AWS environments.

🌐 **Language:** English and German

This training enables you to deepen your knowledge and skills to secure the AWS environment, understanding specialized data classifications, data protection mechanisms, encryption methods, and secure internet protocols.

Objectives:

- Validate expertise in creating and implementing security solutions in AWS, enhance understanding of AWS data protection mechanisms and secure internet protocols.

Prerequisites:

- Five years of IT security experience designing and implementing security solutions, with at least two years of hands-on experience securing AWS workloads.

Program

- Focuses on security engineering on AWS, including key services and tools.



Security Engineering on AWS

Reference: CT2419

📅 **Duration:** 3 days

🏠 **Delivery:** On-site course / Virtual classroom course

🧠 **Level:** Intermediate

👥 **Audience:** Security engineers, architects, cloud architects, and operators.

🌐 **Language:** English and German

Utilizing AWS security services to secure data and systems in the cloud.

Objectives:

- Enhancing skills in AWS security services like Amazon Security Lake, Amazon Detective, and AWS Control Tower; managing secrets, continuous monitoring, and responding to security incidents.

Prerequisites:

- Completion of AWS Security Fundamentals Workshop and Architecting on AWS courses; working knowledge of IT security practices and familiarity with AWS Cloud.


Program


- Focuses on the application of AWS security best practices; creating and analyzing authentication and authorizations with IAM; managing accounts; investigating threats and mitigation.




Google Security

Reference: CT2420

 **Duration:** The total course duration is variable, with individual courses and labs ranging from several hours to several days in total. The structured learning path includes activities like hands-on labs, introductory courses, and more detailed study in specific areas of cloud security.

 **Delivery:** On-site course / Virtual classroom course / Online course

 **Level:** Intermediate to Advanced

 **Audience:** Security engineers and professionals responsible for managing and ensuring the security of Google Cloud deployments. Ideal for those looking to solidify their understanding of Google Cloud's security features and best practices.

 **Language:** English and German

The focus is on designing and implementing secure infrastructure on the Google Cloud Platform. This includes a comprehensive understanding of Google Cloud's security services and features to maintain security and compliance.

Objectives:

- To validate your skills in configuring and managing security within Google Cloud environments. It covers areas like cloud access control, network security, data protection, managing cloud operations, and compliance standards.

Prerequisites:

- Designed for professionals who have practical experience with Google Cloud products and solutions. Candidates should have the ability to configure access within a cloud solution environment, configure network security, ensure data protection, manage operations within a cloud solution environment, and ensure compliance.

Program

- The training includes an extensive range of topics such as Resource Manager, Cloud IAM, Network Security, Encryption on Google Cloud, Data Protection, Compute and Storage Security, Managing Operations in a Cloud Environment, Cloud Monitoring, and Compliance. These areas are covered through hands-on labs, courses, and skill badges.

Initiation to digital footprint

Reference: CT2421

📅 **Duration:** 2 days

🏠 **Delivery:** On-site course

🧠 **Level:** Beginner

👥 **Audience:** All

🌐 **Language:** English and French

This training offers of better understanding of how to manage company's digital footprint, due diligence, company profile and personal information.

Objectives:


- Explore methods for understanding digital footprints, including in-depth online searches, and analyzing hidden data.
- Dedicate focused training sessions to comprehensively understanding and managing digital footprints.



Initiation to incident handling


 **Reference:** CT2422

 **Duration:** 1 day

 **Delivery:** On-site course

 **Level:** Beginner

 **Audience:** All staff

 Available only in French

Objectives:

- At the end of the course, the participant will have a good knowledge of the incident management process and will be able to adopt the right actions in the event of a cybersecurity incident.

Prerequisites:

- Basic knowledge of IT security

Program

1. Introduction to cybersecurity
2. Steps in incident management
3. Legal aspects
4. Evidence recovery and analysis

Introduction to cybersecurity and IS security awareness


 **Reference:** CT2423

 **Duration:** 2 days

 **Delivery:** On-site course or remote

 **Level:** Beginner

 **Audience:** All staff

 Available only in French

This training covers general cybersecurity, digital footprint & hygiene, and Google hacking.

Objectives:

- The training aims to provide participants with the knowledge and skills to understand and effectively manage their digital footprint, adopt safe online practices, comply with cybersecurity regulations, and be aware of the potential risks associated with using the Internet, while equipping them with basic ethical hacking skills to enhance the protection of their data and privacy.

Prerequisites:

- Basic computer and network skills

Program

Day 1: Information hygiene

Module 1: What traces do we leave on the Internet?

- Understanding the types of data we leave online.
- Raising awareness of the risks associated with disclosing personal information.
- Concrete examples of data collected and used by third parties.

Module 2: Knowing and managing your digital footprint

- Techniques for assessing and managing your digital footprint.
- Tools and resources for monitoring online information.
- Strategies for reducing exposure and protecting privacy online.

Module 3: Best practice guide

- Basic principles of data security and privacy protection.
- Practical tips for securing online accounts, devices, and social networks.
- Raising awareness of threats such as phishing, identity theft and malware.
- Promoting a culture of security within the organization.

Day 2: Introduction to cybersecurity

Module 4: Legislation and hacking

- Overview of laws and regulations relating to cybersecurity and data protection.
- Introduction to the main concepts of ethical hacking and computer hacking.
- Awareness of the legal and ethical implications of using hacking techniques.

Module 5: Google Hacking - theoretical

- Introduction to Google Hacking.
- Explanation of advanced search operators and how they can be used to gather sensitive information.
- Examples of Google Hacking techniques used to discover vulnerabilities and security holes.

Module 6: Google Hacking - practical exercises


- Practical exercises to put Google Hacking techniques into practice.
- Search for sensitive information on the Internet using advanced search operators.
- Analysis of results and identification of necessary corrective measures.



Initiation to OSINT


Reference: CT2424

 **Duration:** 2 days

 **Delivery:** On-site course

 **Level:** Beginner

 **Audience:** All staff / Cybersecurity or IT staff / C-suite / VP / Directors

 Available only in French

OSINT, investigation, dorking, search engines

Objectives:

- Initiation to OSINT aims to equip participants with the fundamental skills to effectively collect and analyze information from open sources, strengthen their understanding of OSINT technical and operational principles, while raising awareness of good security and ethical practices in data handling.

Program

Day 1

Module 1: Introduction to OSINT

- Importance of OSINT in information gathering

Module 2: Technical basics

Module 3: OPSEC (Operations Security)

Module 4: Google Dorking

Module 5: Practical exercise

Day 2

Module 6: Looking back at dorks

Module 7: Exercise corrections

Module 8: Personal investigation

Module 9: Website analysis


Module 10: Practical exercises

Conclusion and final evaluation

Intrusion test implementation


 **Reference:** CT2425

 **Duration:** 4 days

 **Delivery:** On-site course

 **Level:** Advanced

 **Audience:** All staff / Cybersecurity or IT staff / C-suite / VP / Directors

 Available only in French

Objectives:

- At the end of the course, participants will be able to carry out an intrusion test on a corporate information system and write an audit report.

Prerequisites:

- Theoretical and practical knowledge of the main cyber attacks
- Mastery of OSI and TCP/IP models
- Know how to use a Linux environment.


Program

1. Rules, constraints, and regulations relating to penetration testing.
2. Diverse types of penetration tests
3. Testing methodology
4. Reminder of common attack techniques
5. Performing an intrusion test on a real case study
6. Writing an audit report
7. Practical exercises


Installing intrusion detection probes


Reference: CT2426

 **Duration:** 3 days

 **Delivery:** On-site course

 **Level:** Advanced

 **Audience:** All staff / Cybersecurity or IT staff / C-suite / VP / Directors

 Available only in French

Objectives:

- At the end of the course, participants will be able to create their own detection rules based on recognized open-source tools and detect attacks targeting their information systems.

Prerequisites:

- Basic knowledge of IT security
- Master OSI and TCP/IP models
- Know how to use a Linux environment


Program


- Introduction to cybersecurity and intrusion detection methods
- Presentation of the diverse types of detection probes
- Setting up network and application attack detection rules with the Suricata probe
- Setting up system attack detection rules with the Wazuh probe
- Implementation of correlation rules with Wazuh
- Introduction to detection probe bypass techniques
- Hands-on exercises

Advanced reconnaissance (including social engineering)


 **Reference:** CT2427

 **Duration:** 3 days

 **Delivery:** On-site course

 **Level:** Intermediate

 **Audience:** Cybersecurity or IT staff

 Available only in French

Objectives:

- The objectives of this training are to provide participants with the advanced skills necessary to conduct thorough reconnaissance of the attack surface, using specialized tools such as Shodan and Censys, refining their website analysis techniques, and developing their understanding and practice of Social Engineering, in order to enhance the resilience and security of computer systems against potential threats.

Prerequisites:

- Computer and network knowledge, reading code can be a plus.

Program

Day 1: Shodan & Censys: Theory and Practical Exercises

Module 1: Introduction to Shodan and Censys

- Presentation of the features and capabilities of Shodan and Censys in reconnaissance of the attack surface.
- Explanation of key concepts and terms associated with these tools.

Module 2: Using Shodan and Censys

- Hands-on training in the practical use of Shodan and Censys to search for connected devices, exposed services, and vulnerabilities
- Exploration of advanced search and filtering features.

Module 3: Practical Exercises

- Guided practical exercises to apply the knowledge gained in the previous modules.
- Research and analysis of connected devices and exposed services using Shodan and Censys.
- Identification of vulnerabilities and potential risks.

Day 2: Advanced Website Analysis

Module 4: Advanced Website Analysis Techniques

- Exploration of advanced methods for analyzing website security.
- Use of specialized tools to discover vulnerabilities and potential entry points

Module 5: Advanced Reconnaissance Tools.

- Introduction to advanced tools for reconnaissance of the attack surface.
- Skill development in the use of tools such as Nmap, Nikto, DirBuster, etc.

Module 6: Practical Exercises

- Advanced practical exercises to apply website analysis techniques and reconnaissance tool usage.
- Real-world case studies to identify and exploit vulnerabilities.

Day 3: Social Engineering Content

Module 7: Introduction to Social Engineering

- Definition of Social Engineering and its various techniques.
- Understanding of human psychology and manipulation tactics used in Social Engineering.

Module 8: Social Engineering Techniques

- Exploration of phishing, social engineering, persuasion, and manipulation techniques.
- Case studies on successful Social Engineering attacks and their consequences.

Module 9: Practical Exercises


- Practical exercises on Social Engineering to simulate attack scenarios.
- Application of acquired skills to develop defense strategies against Social Engineering attacks.




Attack surface technical reconnaissance


 **Reference:** CT2428

 **Duration:** 3 days

 **Delivery:** On-site course

 **Level:** Intermediate

 **Audience:** Cybersecurity or IT staff

 Available only in French

This training will cover theory and practice for several reconnaissance techniques to evaluate your attack surface: reverse dns, whois, Shodan, dorking, Censys, and networks.

Objectives:

- The objectives of this training course are to equip participants with the skills needed to carry out effective technical reconnaissance of attack surfaces, using tools and techniques such as Google Hacking, website analysis, Shodan and Censys, to identify vulnerabilities and potential entry points for strengthening system security.

Prerequisites:

- General computer and network knowledge (server port, dns etc...).

Program

Day 1 - Google Hacking theory & practical exercises

Module 1: What is OSINT?

Module 2: Technical basics

Module 3: OPSEC (Operations Security)

Module 4: Google Dorking

Day 2 - Theoretical website analysis and practical exercises

Module 5: Definitions

Module 6: Website analysis

Day 3 - Shodan & Censys theory and practical exercises


Module 7: Legislation

Module 8: Shodan and practical exercises

Network security


 **Reference:** CT2429

 **Duration:** 3 days

 **Delivery:** On-site course

 **Level:** Advanced

 **Audience:** Cybersecurity or IT staff

 Available only in French

Objectives:

- At the end of the course, participants will have a good command of the attacks (Web, system, network, and application) used by attackers targeting corporate information systems.
- They will also be able to reproduce them manually or using specialized tools, and to bypass defense systems.

Prerequisites:

- Good knowledge of classic attacks (Web, system, and network)
- Mastery of OSI and TCP/IP models
- Know how to use a Linux environment


Program


- Advanced network attacks and tool development with Scapy
- Advanced Web attacks (blind SQL injection with application firewall, SSRF, XXE, JWT token attacks, etc.).
- System attacks and bypassing protection systems
- Theory and practice of buffer overflow (basics and introduction to Return Oriented Programming)
- Final challenge on a realistic case

Social engineering awareness

 **Reference:** CT2430

 **Duration:** 1 day

 **Delivery:** On-site course

 **Level:** Beginner

 **Audience:** All staff / Cybersecurity or IT staff / C-suite / VP / Directors

 Available only in French

Objectives:

- At the end of the course, the participant will be able to detect the signs of an attempted social engineering attack and adopt the right measures to deal with it.


Program


- Introduction to social engineering
- Open-source intelligence and social engineering
- The manipulator's tools.
- Case studies
- Audit feedback
- Media examples
- Good practice in dealing with manipulators.
- Quiz


Hacking techniques initiation


Reference: CT2431

 **Duration:** 5 days

 **Delivery:** On-site course

 **Level:** Intermediate

 **Audience:** All staff / Cybersecurity or IT staff / C-suite / VP / Directors

 Available only in French

Objectives:

- At the end of the course, participants will have a good understanding of the classic attacks used by attackers targeting corporate information systems.
- They will also be able to reproduce them manually or using specialized tools.

Prerequisites:

- Basic knowledge of IT security
- Knowledge of OSI and TCP/IP models
- Know how to use a Linux environment


Program

- Open-source intelligence by practice
- Network discovery with Nmap
- Network attacks (Man-In-The-Middle, denial of service, etc.)
- Web attacks (SQL code injection, XSS vulnerabilities, file inclusion, etc.)
- System attacks with the Metasploit tool
- Privilege elevation attacks
- Final challenge on a realistic case


Hacking techniques expertise


 **Reference:** CT2432

 **Duration:** 5 days

 **Delivery:** On-site course

 **Level:** Expert

 **Audience:** All staff / Cybersecurity or IT staff / C-suite / VP / Directors

 Available only in French

Objectives:

- At the end of the course, participants will have a good command of the attacks (Web, system, network, and application) used by attackers targeting corporate information systems.
- They will also be able to reproduce them manually or using specialized tools, and to circumvent defense systems.

Prerequisites:

- Good knowledge of classic attacks (Web, system, and network)
- Mastery of OSI and TCP/IP models
- Know how to use a Linux environment

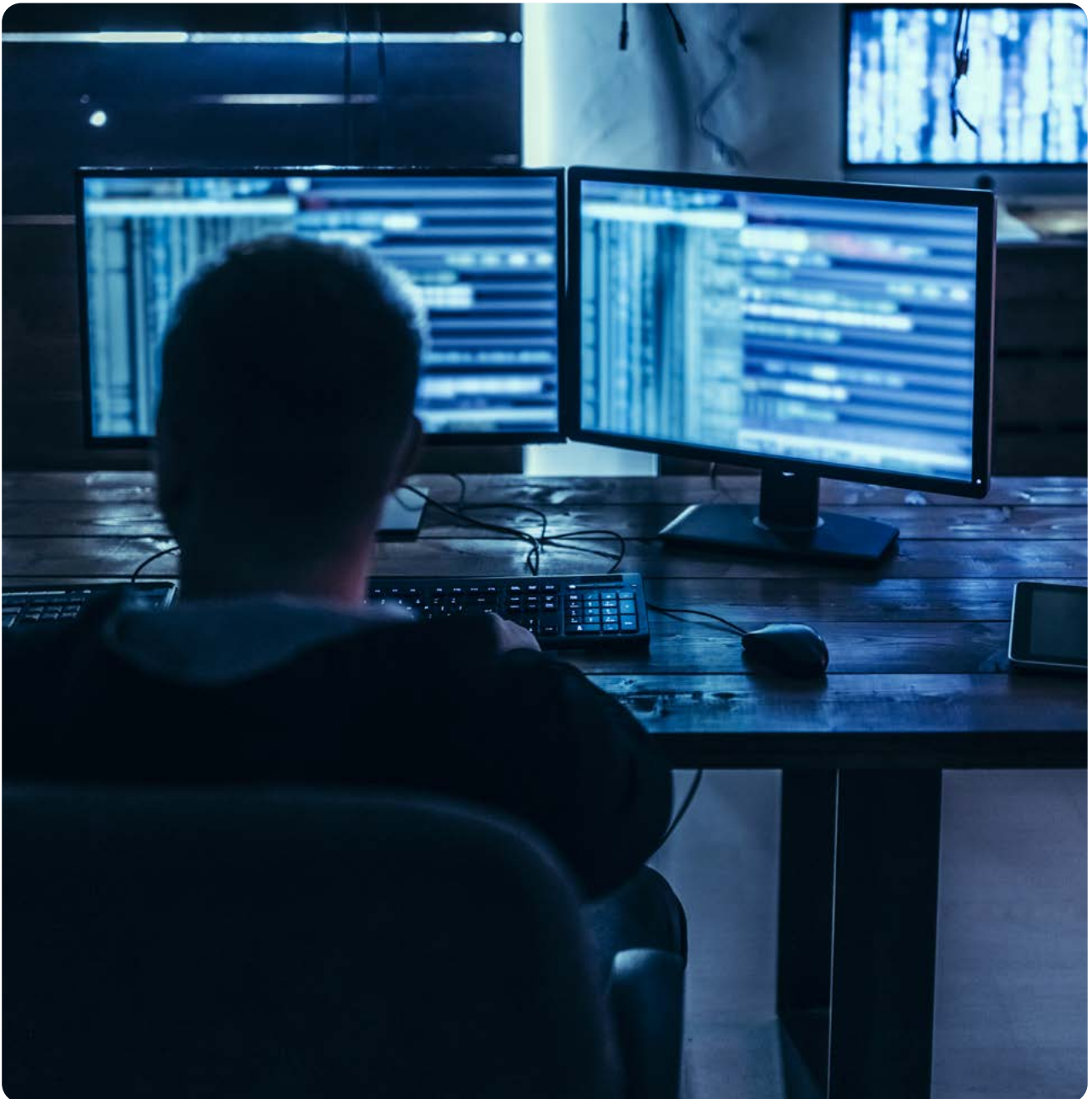
Program

- Advanced network attacks and tool development with Scapy
- Advanced Web attacks (blind SQL injection with application firewall, SSRF, XXE, JWT token attacks, etc.)
- System attacks and bypassing protection systems
- Theory and practice of buffer overflow (basics and introduction to Return Oriented Programming)
- Final challenge on a realistic case






Security Immersion




Security Immersion – Exclusive professional part-time program

 **Reference:** SI241

 **Duration:** 3 months to 6 months

 **Delivery:** On-site course / Virtual classroom course / Online course

 **Level:** Beginner / Intermediate

 **Audience:** All staff / Cybersecurity or IT staff

 **Language:** English

This track - exclusively proposed by Eviden - is a professional part-time apprenticeship in cybersecurity, delivered by our top subject-matter experts. It already has six training paths: SOC analyst, DFIR, Security Engineer, IAM, GRC, Cloud engineer. And we can craft new paths tailored to your organization's needs.

Practice being a top priority, thanks to this program the participants will get everyday hands-on exercises on the topics studied in the training sessions. This will allow them to put the learning into practice between the training sessions with our expert. In addition, they will have an easy and privileged access to world-class cybersecurity experts, and a close mentorship from them.

Finally, we can custom this program to the audience you want from junior to seniors, and both for upskill or reskill purposes.

Objectives:

- Learn, skills and enhanced the business continuity via a rotation on training and working in the company.
- Reinforce the security of the team.
- Upskill your team.

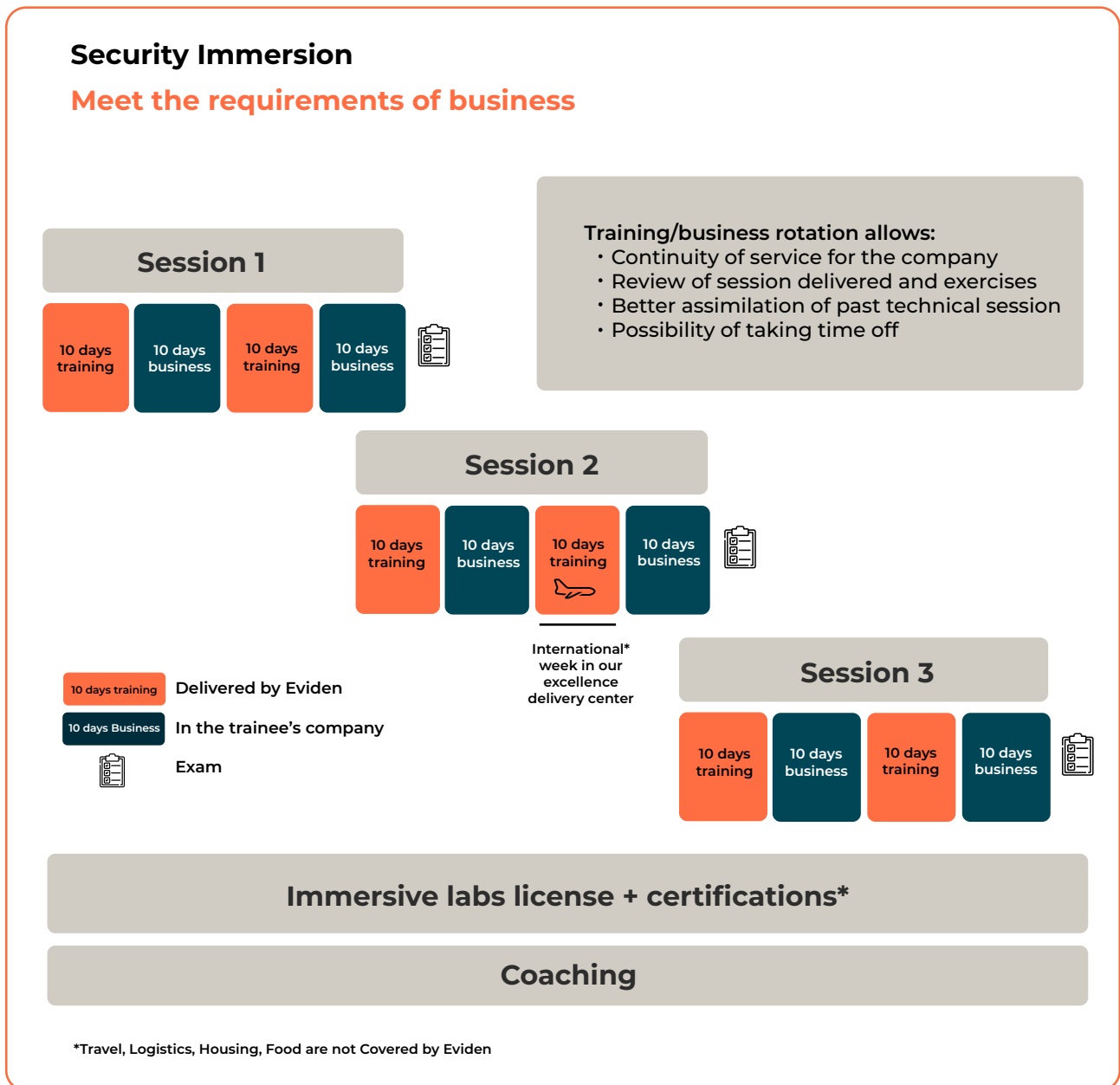
Program

The program will be designed according to the cyber companies needs and maturity.

We offer a wide range of technical session, mixing theory and practice, which can be adapted according to your training needs:

- GRC
- OT, IOT, IIOT
- IAM
- Cloud
- Network security
- System
- Sec Dev
- Offensive security
- And more

Example of timeline:







Cyber Crisis Exercise



Incident Response Tabletop Exercise

 **Reference:** CCE241

 **Duration:** 2 to 6 hours

 **Delivery:** On-site course / Virtual classroom course / Online course

 **Level:** Beginner / Intermediate / Advanced / Expert

 **Audience:** Cybersecurity or IT staff

 **Language:** English

The main purpose of Incident Response Tabletop Exercise (IR TTX) is to support companies' readiness for cybersecurity incidents. Training is flexible and is adapted to your requirements, experience and used technologies. It is done via simulation of security incidents via role play game based on realistic scenario via:

- Operational Tabletop Exercise (without mockup malware)
- Operational Tabletop Exercise (with mockup malware)

Prior to running of Tabletop Exercise scenario, Facilitator is collecting data and preparing plan. This is needed to ensure that scenario is customized and reflects structure of involved organization. After conducting of exercise, easy-to-understand evaluation report is prepared where we are capturing strong and weak points. It is done together with rating and recommendation in term of different dimensions: people, process, or technology.

Example scenarios:


- Organization is attacked via a 0-day vulnerability.
- Threat actor is starting to take control of your IT environment compromising high privileged account.


Objectives:

- Raise cybersecurity awareness and skills.
- Verify process for Incident Response.
- Determine how stakeholders involved in cybersecurity incident interact and respond.
- Assess the organization's capability to determine operational impacts of cyber-attacks and implement proper recovery procedures.
- Validate procedures.
- Expose and correct weaknesses in cybersecurity systems.
- Observe and describe the processes used to detect and mitigate cybersecurity threat.
- Capture findings as a trigger for continues improvement actions.

Crisis Simulation

 **Reference:** CCE242

 **Duration:** 3 to 6 hours

 **Delivery:** On-site course / Virtual classroom course / Online course

 **Level:** Beginner / Intermediate / Advanced / Expert

 **Audience:** All staff / Cybersecurity or IT staff / C-suite / VP / Directors

 **Language:** English

The main purpose of Crisis Simulation is to support companies' readiness for cyber crisis. Like Incident Response Operational Tabletop Exercise, the Crisis Simulation is flexible and is adapted to your requirements, experience. Training is also conducted via role play game based on realistic scenario. However, the focus here is put on managerial roles and responsibilities with typical dilemmas associated with among other C-Level Management.

Prior to running of Crisis Simulation scenario, Facilitator is collecting data and preparing plan. This is needed to ensure that scenario is customized and reflects structure of involved organization. After conducting of exercise, easy-to-understand evaluation report is prepared where we are capturing strong and weak points. It is done together with rating and recommendation in term of different dimensions: people, process, or technology.

Example scenario:

- Attacker encrypted application servers and left ransom note.

Objectives:

- Deliver the experience of cybersecurity crisis including sensitive data exposure.
- Awareness on how impact of targeted phishing and ransomware looks like.
- Identify key trigger points for decision making during crisis.
- Assess the organization's capability to determine operational impacts of cybersecurity.
- Understanding implications of sensitive data being compromised by threat actor.
- Understanding roles and cooperation between all stakeholders during crisis.
- Validate crisis management procedures.
- Capture findings as a trigger for continues improvement actions.






Cyber for executives




Cybersecurity Awareness for Executives

 **Reference:** CE241

 **Duration:** 2 hours

 **Delivery:** On-site course

 **Level:** Beginner / Intermediate / Advanced / Expert

 **Audience:** Management Boards, C-suite / VP / Directors Executive Teams

 **Language:** English

Cybersecurity is a Board level issue. Give your C-level and Executive teams the knowledge to lead the fight against cyber threats with this training session.

Objectives:


- Understand why cybersecurity is a board-level issue.
- Identify key responsibilities for cybersecurity.
- Know which critical questions to ask during a cyber-attack or data breach.


Program

- How has Cybersecurity evolved in recent years?
- What are the key Threats, Vulnerabilities and Risks (provided with industry context)
- Why has Cybersecurity become a board level priority in recent years?
- Board responsibilities for Cybersecurity
- The impact of recent cyber-attacks
- Strategy, Leadership and Governance responsibilities and liabilities
- Consequences of non-compliance, breaches, and relevant legislation
- Key question the board need to ask about their cybersecurity program
- Using Cyber Insurance
- Social Engineering Cybersecurity awareness


EU Regulatory Compliance: NIS-2/CER Directive and DORA Regulation | For executives

 **Reference:** CE242

 **Duration:** 1-2 hours up to 4 hours if attack simulations are to be included

 **Delivery:** On-site course

 **Level:** Beginner / Intermediate

 **Audience:** C-suite / VP / Director

 **Language:** English

According to EU Institutions impact Assessment study there will be approximately 160,000 for NIS-2 and 22,000 organizations under DORA scope, respectively starting early 2025. Despite that fact, still many companies and their top management is not aware about individual accountability for non-compliance with NIS2 (Network and Information Systems Directive 2), DORA (Digital Operational Resilience Act) or CER/RCE Directive (Resilience of Critical Entities Directive). One may think that under above EU Regulations specific role will be responsible, but it is not applicable and valid anymore. CISO (Chief Information Security Officer) or other Security Director or Officer are not mentioned in above regulations at all but can be considered under the terminology “management bodies.” The program of the training can be adjusted to your specific needs of addressing other regulations, like European Cybersecurity Act, Cyber Resilience Act, AI Act, etc.

Objectives:


- Understand what the scope of NIS-2 is, DORA, CER Regulations.
- What are the sanctions and accountability.
- What are ways of evidence collection to demonstrate effective supervision of management.

Program

- High level introduction to NIS-2, CER Directive and DORA Regulation.
 - Objective
 - Scope or exclusions: Industry, Sectors, Subsectors.
 - Dependencies between NIS-2, CER, and DORA.
 - Deadline for Implementation of requirements.
 - Penalties
 - Local Competent Authorities.
 - European level Competent Authorities.
- Management responsibilities
- Regular Management risk awareness and training
- Individual sanctions.
- Oversight approach and Regulator will audit compliance.
- What are the means of influence on non-compliant organization.
- Exemplary ways of evidence collection on management supervision of compliance activities, to demonstrate effectiveness of oversight over compliance with NIS-2, DORA, CER.
- Summary, Q & A.

EU Regulatory Compliance: NIS-2/CER Directive and DORA Regulation | For Cybersecurity, procurement, and sales teams

Reference: CE243

 **Duration:** 3-6 hours (half or whole 1 day) /days/weeks

 **Delivery:** On-site course / Virtual classroom course / Online course – all possible.

 **Level:** Beginner / Intermediate

 **Audience:** Sales Teams, Procurement Teams, or Other Employees groups, like Cybersecurity / Information Security Specialists

 **Language:** English

According to EU Institutions impact Assessment study there will be approximately 160,000 for NIS-2 and 22,000 organizations under DORA scope, respectively starting early 2025. The focus on NIS-2 Directive is further harmonization of requirements between financial and non-financial sector across 27 member states and its suppliers (ICT Third Party Service Providers in case of DORA) and supply chain in case of NIS-2 and CER Directive. That means that especially companies under DORA will expect from its ICT Third Party Service Providers specific requirements and regularly updated information on their cyber resilience posture. Despite that fact, still many companies and their sales teams, procurement will be surprised that such requirements including contract renegotiations will appear soon, if not appeared on the agenda of their supply-customer relations. Still a lot of organizations in scope is not able to speak and understand what is really required or is not about potential losing or reduction of business with Financial Entities as they would need to report ICT Concentration risk under DORA.

Program of the training can be adjusted to your specific needs of addressing other regulations, like European Cybersecurity Act, Cyber Resilience Act, AI Act, or specific employee target groups, etc.

Objectives:

- Understand what the scope of NIS-2 is, DORA, CER Regulations.
- How those regulations are impacting collection of evidence of compliance from supplier point of view, what to provide to customers, how current contractual arrangements will have to be updated.
- What are ways of evidence collection to demonstrate effective compliance.
- What sales or procurement teams might expect or must adjust in their communication with customers, processes.

Prerequisites

- Little or no knowledge of European Regulations

Program


- Introduction to current EU Regulatory Landscape (ECA, NIS2, DORA, CER)
- Regulatory requirements for DORA (FSI Industry) in cybersecurity and operational Resilience:
- Regulatory requirements for NIS 2 (Non-Financial Industry) in cybersecurity:
- Regulatory requirements for CER/RCE Directive in cybersecurity
- Relations of NIS 2 to DORA Regulation and CER/RCE Directive – how to put it all together
- Case study: decomposing NIS 2 Directive articles into use cases and risks risk-based compliance exercise

Holistic approach to ISO standards family

Reference: CE244

 **Duration:** 1-3 days

 **Delivery:** On-site course / Virtual classroom course / Online course

 **Level:** Beginner / Intermediate / Advanced / Expert / Masterclass on risk or how to combine ISO 27001 with industry ISMS, Privacy ISMS or other ISO family standard.

 **Audience:** All staff / Cybersecurity or IT staff / C-suite / VP / Directors

 **Language:** English

In today's complex regulatory and best practices environment it happens even cybersecurity, information security teams to be challenged on what best practices to follow which of it is the best fit for organization or how to map current documentation related to IT/Cyber BCM/ Resilience domain into various ISO best practices or non-ISO standards. With profound experience on how to integrate or map various standards, in particular ISO family standards, we can assist through the technical training how to select one and what to choose from. It is not classical ISO 27001 or other training – we share and learn on practical aspect of design, planning of controls objectives, implementation, auditing, what works and what does not.

This training module can be delivered for various levels: introduction, advanced training, or specific masterclass.

Objectives:

- To understand practical aspects of above ISO standards requirements,
- Experience how to officially implement and how to measure effectiveness of controls,

Prerequisites

- General orientation in cybersecurity Frameworks or Risk Assessment Frameworks


Program


- Introduction to PDCA Cycle, OODA loop, ISMS concepts.
- Integration of various standards, mapping challenges (Annex SL).
- Scope of Standard (Clause 1) – in case any standard is used which is not covered by Annex SL High Level Structure, the scope will be adjusted accordingly after clarification the scope of ISO standards to be in scope (it applies to the points 4-11 below).
- Normative references (Clause 2)
- Terminology (Clause 3)
- Scope of applicability in the given standards.
- Presentation of requirements, case studies related, exemplary documentation related to body of the standard (Clauses 4-7) Context, Leadership, Planning, Support of ISMS, BCMS, etc. In Case of ISO 31000 presentation of Principles and Risk Management Framework (Clauses 4 and 5)
 - » Presentation of Clause 8 Operation, i.e., execution phase and in case of ISO 31000 process (Clause 6).
 - » Presentation of ISMS, BCMS Performance Evaluation (Clause 9)
 - » Presentation of Improvement part (Clause 10)
 - » Annex part of Standards.
 - » Note: It must be agreed in advance upon the purchase of standards or on how standards will be used during the training. By default, this offer excludes buying standards for the participants.

Selected techniques of qualitative and quantitative risk analysis

 **Reference:** CE245

 **Duration:** 1-3 days

 **Delivery:** On-site course / Virtual classroom course / Online course (however preferred on-site for maximum efficiency and effectiveness of learning (proven many times).

 **Level:** Beginner / Intermediate / Advanced / Expert / Masterclass on risk or how to combine ISO 27001 with industry ISMS, BCMS or other ISO family standard.

 **Audience:** All staff / Cybersecurity or IT staff / Operational Risk Staff / Legal Staff, Managers – overview course

 **Language:** English

In today's complex regulatory and best practices environment it happens even cybersecurity, information security teams to be challenged on what risk analysis and risk assessment results show indicate to executives to support respective decision-making process. In the training there are presented one of the best practices to follow which of it is the best fit for organization or how to improve current risk analysis documentation related to IT/Cyber BCM/ Resilience risk assessment domain. We concentrate on proper understanding the terminology, cognitive challenges, silent assumptions, cognitive bias's role in risk analysis, etc. We share and learn practical aspects of design, planning of risk analysis methodologies with their objectives, implementation, auditing or proving that they are effective.

Objectives:

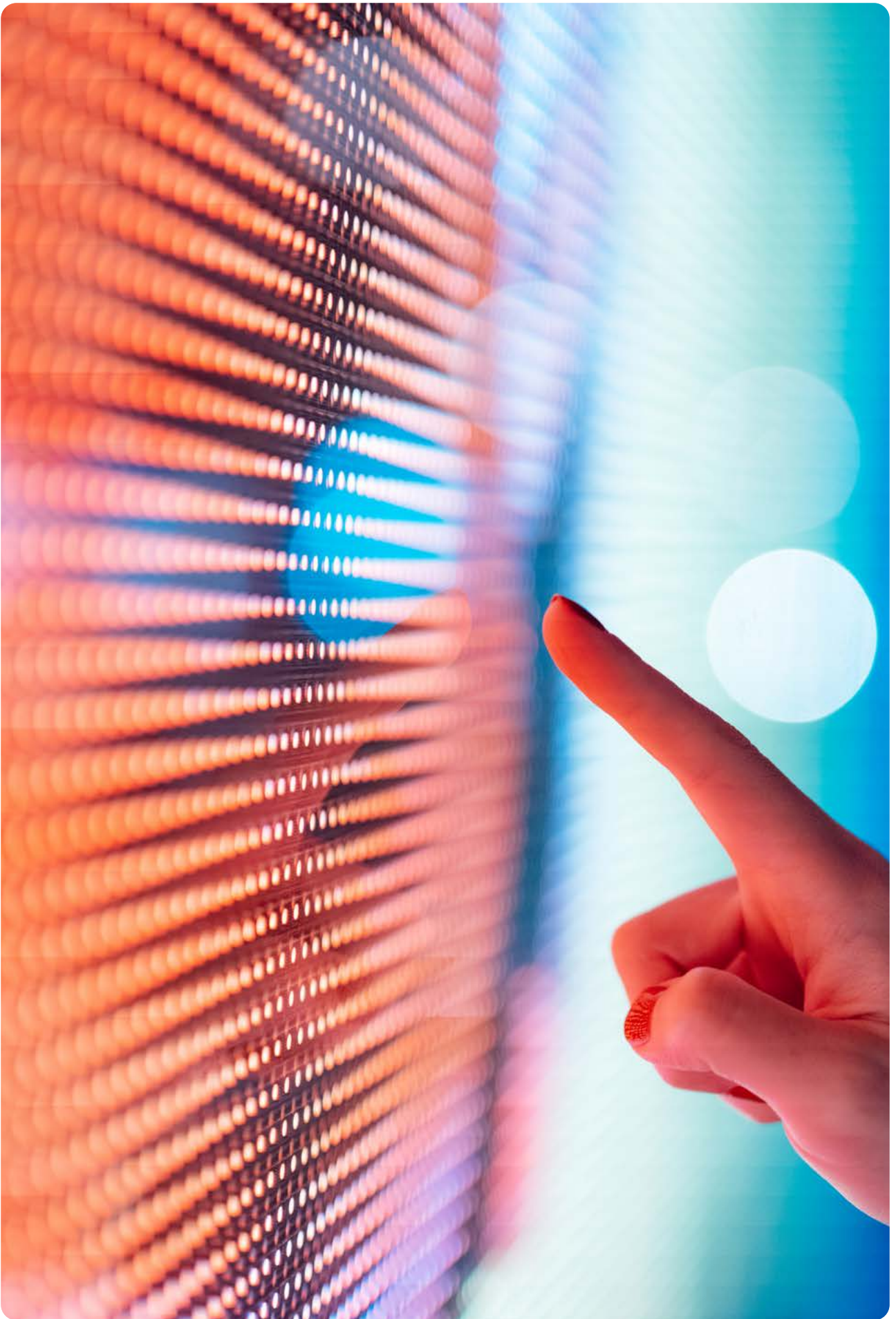
- Understand practical aspects risk analysis and using proper terminology of risk influences proper analytical thinking of risk analysis.
- Experience and strengthening understanding by practicing case studies to be done during training.

Prerequisites

- Little or General orientation in cybersecurity
- Frameworks or Risk Assessment Frameworks

Program

- Introduction – Risk analysis best practices
- Risk terminology & concepts – best practices
 - » ISO 31073:2022 – Risk Management Vocabulary (former ISO Guide 73:2009)
 - » ISO 31000:2018 - Risk management — Guidelines
 - » IEC 31010:2019 - Risk management — Risk assessment techniques
 - » ISO 27001:2022 - Information security, cybersecurity, and privacy protection — Information security management systems — Requirements
 - » ISO 27005:2022 - Information security, cybersecurity, and privacy protection — Guidance on managing information security risks.
- Risk management process for cybersecurity
 - » ISO 31000 vs ISO 27005 vs FAIR
- Case Study – Exercise
 - » Qualitative Risk Assessment
 - » Quantitative Risk Assessment



Connect with us

For more information or to request a quote, please contact us at cybersecurity-training@eviden.com

Connect with us



eviden.com

Eviden is a registered trademark © Copyright 2024, Eviden SAS – All rights reserved.