

Cybersecurity Fundamentals

Ontdek de geheimen van cybersecurity: een 2-daagse cursus



Duik in het hart van cyberbeveiliging met onze intensieve, interactieve cursus, speciaal ontworpen om theorie en praktijk om te zetten in concrete vaardigheden. Maak in slechts twee dagen een tocht door de fundamentele aspecten en huidige uitdagingen van IT-beveiliging, dankzij een programma dat kennis en praktijk combineert.

- **Ontdek** de pijlers van cyberbeveiliging, van informatiebescherming tot risicobeheer, en begrijp waarom dit het fundament is waarop de beveiliging van elke organisatie rust.
- **Reis** naar het hart van de meest voorkomende en geavanceerde aanvallen. Leer hoe u kwetsbaarheden kunt identificeren en kunt anticiperen op de bewegingen van tegenstanders om ze beter te kunnen bestrijden.
- **Verdiep u** in geavanceerde technieken voor het beveiligen van uw digitale middelen.
- **Bereid u voor** om effectief te reageren op beveiligingsincidenten. Ontdek hoe responsteams crises beheren om schade te minimaliseren en de normale gang van zaken te herstellen.



Deze cursus, in het Engels, wordt geleid door Georges Ataya, professor en academisch directeur aan de Solvay Brussels School, vicevoorzitter van de Cybersecurity Coalition en consultant bij Ataya Partners. Een sessie in het Nederlands is mogelijk op aanvraag.

Ontdek de geheimen van cyberbeveiliging: een 2-daagse onderdompelingscursus

Deelnemers aan ons trainingprogramma over cyberbeveiliging kunnen aantonen dat ze de basisprincipes van cybersecurity begrijpen, en dat ze inzicht hebben in de essentiële rol van de security expert bij het **beschermen van bedrijfsgegevens en -infrastructuur**.

Naast theoretische presentaties over het begrijpen van cyberbeveiliging, bieden we workshops waarin deelnemers moeten reageren op vooraf gedefinieerde incidentscenario's. **Deze interactieve leerervaring** zal hen beter in staat stellen om cyberincidenten effectief te beheren en als team samen te werken om de digitale veiligheid van het bedrijf te garanderen.

TRAINING OBJECTIVES

- Understand the fundamentals of cyber security
- Raising awareness of threats and risks
- Presentation of security technologies and controls
- Ability to respond to basic security incidents
- Awareness of risk management
- Compliance and governance skills
- Improved business resilience
- Privacy awareness
- Use of best practice and security frameworks

COURSE CONTENT

During this course, you will discover the fundamental principles of cybersecurity and **develop the essential skills** to protect your organisation's data and systems.

The first part of the course is divided into four chapters.

Fundamentals of security

- 1.1 What is security?
- 1.2 Types of security
- 1.3 Specialised systems
- 1.4 Roles and responsibilities
- 1.5 Governance, risk management and compliance
- 1.6 Cyber security governance
- 1.7 Resilience
- 1.8 Business continuity and disaster recovery
- 1.9 Business impact analysis
- 1.10 Recovery concepts
- 1.11 Information security objectives

- 1.12 Privacy
- 1.13 Privacy versus security

Threat landscape

- 2.1 Cyber risk
- 2.2 Threats
- 2.3 Vulnerabilities
- 2.4 Cyber attacks
- 2.5 Attack attributes
- 2.6 Attack process
- 2.7 Malware and attacks
- 2.8 Risk assessment
- 2.9 Supply chain considerations
- 2.10 Risk management cycle
- 2.11 Risk management
- 2.12 Use of risk assessment results

Securing assets

- 3.1 Identification of industry risks, standards, frameworks and guidance
- 3.2 Architecture, models and frameworks
- 3.3 Security controls

Security operations and response

- 4.1 Security operations
- 4.2 Tools and technologies
- 4.3 Incident management
- 4.4 Forensics

The second part of the course will test participants with predefined scenarios. Based on different incidents, participants will have to formulate an appropriate response to preserve the organisation's systems.

Finally, participants will take a quiz at the end of the day to ensure that all the concepts have been correctly assimilated.

WHO SHOULD ATTEND?

- Co-workers who are not familiar with cyber security
- Students and recent graduates
- Organisational teams
- IT professionals

PREREQUISITES

There are no prerequisites for this course.

COURSE MATERIAL

The course presentation will be distributed to all course participants in paper and digital format. During the course, participants will receive a series of readings to help them understand the concepts presented during the course.

We will also be sharing with you the most important European guides and regulations in electronic format.

TEST AT THE END OF THE COURSE

A quiz in MCQ format will be distributed at the end of the course. Participants will have 60 minutes to answer the quiz, and will be given the notes and training materials that have been distributed.

If your business has several employees requiring cyber security training, [our on-demand training solutions](#) can be tailored to meet the specific needs and objectives of your team. Our instructors are practitioners with extensive industry experience, bringing their proven cyber security expertise to you and your colleagues.