

Your path to better cybersecurity

Catalogue of pilot trainings



CYRUS
enhanced cybersecurity skills

This project has received funding from the European Union's Digital Europe Programme under grant agreement No 101100733.



Co-funded by the
European Union

About CYRUS

CYRUS is an initiative with the vision to **enhance cybersecurity skills** in the **transport and manufacturing** industries to effectively combat cybersecurity challenges.

Our project team consists of eleven partners from nine EU countries, working together for three years to raise awareness for cybersecurity and boost cybersecurity skills.

We develop **personalised, customised, work-based cybersecurity training** tailored to the specific needs of the workforce.

To develop the training courses, we **analysed cybersecurity skills, competencies, training needs and skill gaps**. Based on this analysis we **designed and developed training courses**, all tailored to fit into convenient **1 - 4 hour slots**.

We understand every organisation has different needs and we are eager to cater to the specifics of your team's interests and areas of potential growth!

About the training courses

In this catalogue you will find our pilot trainings, that are running from **July to October 2024**. At this stage of the project, you have the opportunity to **sample a selected range of our courses for free** in return for sharing your valuable feedback. The insights garnered will help us refine and customise these offerings to better suit your team's unique needs in the final round of training sessions scheduled for 2025.

The courses are for different **target groups**: engineers, administrative staff and operators, and are assigned to specific tracks.

- **The basic track** provides basic information to align attendants for the specialised tracks.
- **Track 1** focuses on **human-related security** with the goal to provide a clear understanding of human-centred security problems and solutions.
- **Track 2** delves into **cyber risk**. It has two specialisation tracks: 2.1 is for DevSecOps and security testers. 2.2 is for network specialists and incident responders.

You can find the tracks and the respective trainings on the next page of this catalogue.

Target groups

Engineers (ENG)

- Technical roles who have direct access, possibly not mediated by constrained HMI (human machine interface), can change the technical infrastructure
- Examples: Software developer, manufacturing / maintenance technician, welding inspector

Administrative staff (ADM)

- Non-technical roles with no direct access (maybe through several levels of mediation of IT) to the technical infrastructure or the operation of the system
- Examples: Human resource officer, team leader of the shopfloor team, supply chain manager

Operators (OPS)

- Non-technical roles with access to the technical infrastructure through severely constrained HMI (human machine interface). Operates the systems but typically cannot change it
- Examples: Rail maintainer, train driver, employee working on the shopfloor, machine operator

Proficiency levels

Beginner

- Has some awareness and understanding of basic techniques and concepts
- Learners develop basic awareness and understanding to follow and apply basic techniques and concepts under supervision after completing this level

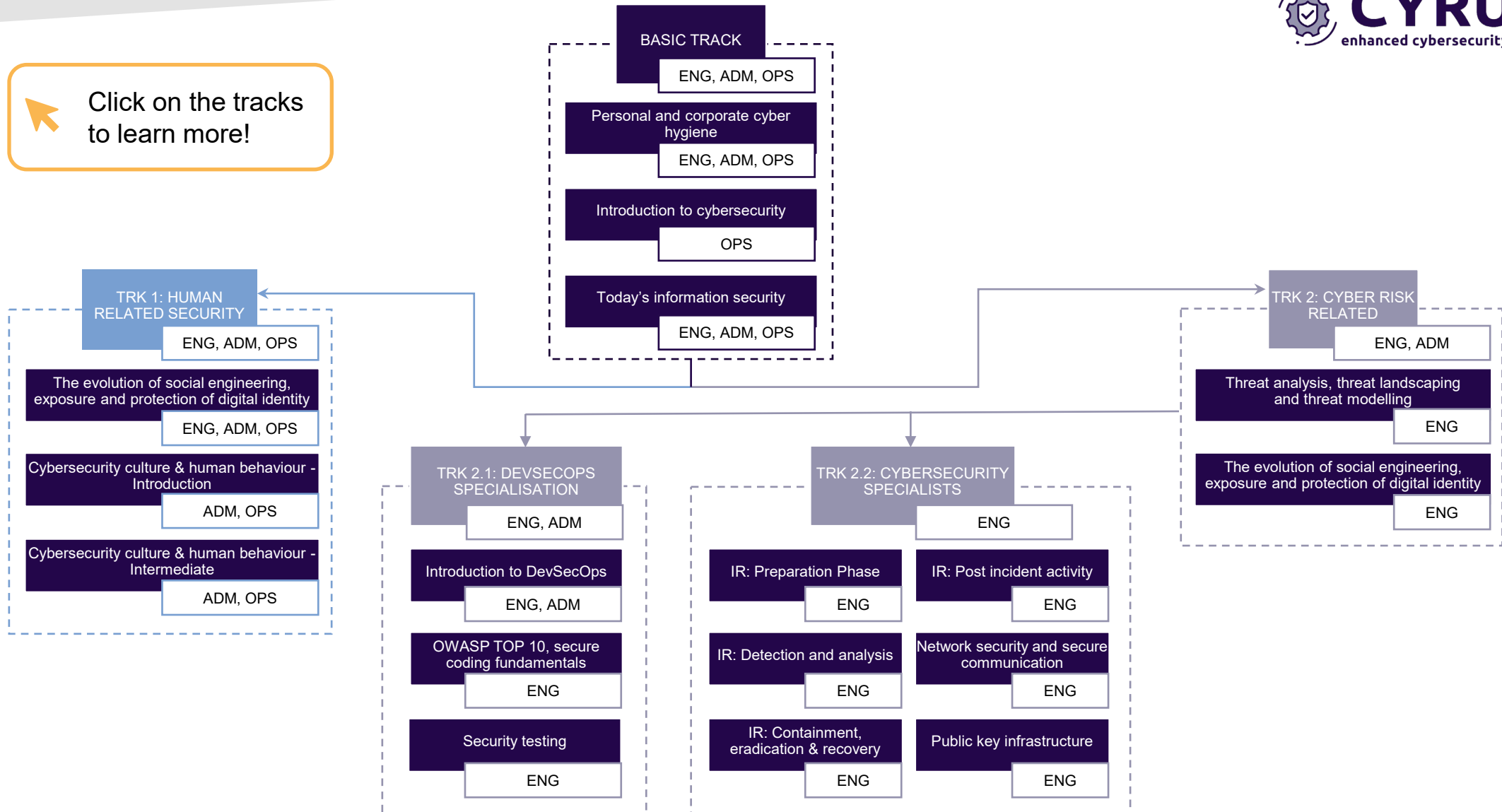
Skilled

- Can effectively perform and execute the tasks as requested
- Learners acquire the competences allowing them to effectively perform and execute the tasks as requested with limited level of autonomy after completing this level

Expert

- Provides guidance and troubleshoot related to this area of expertise
- Learners acquire the competences allowing them to provide guidance and troubleshoot related to this area of expertise with autonomy after completing this level

Click on the tracks to learn more!




Basic track

The trainings assigned to this track provide basic information to align attendants for the specialised tracks

[Back to overview](#)

Personal and corporate cyber hygiene

Best practices to identify main cyber threats and reduce cyber risk


- Proficiency level: beginner
- Target group: administrative staff
- Domain: transport and manufacturing
- Language: English
- Duration: 6 hours (2 sessions, 3 hours each)
- After this course you will be able to comprehend potential impacts of cyber threats and identify secure practices for cybersecurity in professional and private life
- To attend this course, it is recommended to have a basic understanding of cyber attacks and consequences
- This training is available online
- Dates: 9 September 2024, 14:00 - 17:00 CEST and 11 September 2024, 14:00 - 17:00 CEST
- Basic track
- Competence unit 3.1: cybersecure behaviour
- Provided by 

Save your seat!

[Back to overview](#)

Personal and corporate cyber hygiene

Best practices to identify main cyber threats and reduce cyber risk


- Proficiency level: beginner
- Target group: operators
- Domain: transport and manufacturing
- Language: English
- Duration: 6 hours (2 sessions, 3 hours each)
- After this course you will be able to comprehend potential impacts of cyber threats and identify secure practices for cybersecurity in professional and private life
- To attend this course, it is recommended to have a basic understanding of cyber attacks and consequences
- This training is available online
- Dates: 12 September 2024, 14:00 - 17:00 CEST and 13 September 2024, 14:00 - 17:00 CEST
- Basic track
- Competence unit 3.1: cybersecure behaviour
- Provided by 

Save your seat!

[Back to overview](#)

Personal and corporate cyber hygiene

Best practices to identify main cyber threats and reduce cyber risk


- Proficiency level: beginner
- Target group: engineers
- Domain: transport and manufacturing
- Language: English
- Duration: 6 hours (2 sessions, 3 hours each)
- After this course you will be able to comprehend potential impacts of cyber threats and identify secure practices for cybersecurity in professional and private life
- To attend this course, it is recommended to have a basic understanding of cyber attacks and consequences
- This training is available online
- Dates: 25 September 2024, 14:00 - 17:00 CEST and 26 September 2024, 14:00 - 17:00 CEST
- Basic track
- Competence unit 3.1: cybersecure behaviour
- Provided by 

Save your seat!

[Back to overview](#)

Introduction to cybersecurity

Understanding the basic concepts of cybersecurity, password hygiene, explanation of ransomware and phishing attacks, exploiting social engineering and recognition and response in case of their detection, as well as identification of attacks through email

- Proficiency level: beginner
- Target group: operators
- Domain: transport (railway sector)
- Language: Polish
- Duration: 3 hours
- After this course you will be able to recognise cyber threats, pay attention when performing routinary checks to avoid suspicious hardware, apply safe browsing and password hygiene practices and much more
- This is an in-person training in [Hotel Altus Poznań Old Town](#) (PL)*
- Date: 2 September 2024, 9:00 - 13:00 CEST
- Basic track
- Competence unit 1.1: cybersecurity fundamentals
- Provided by  **Polish Platform**
For Homeland Security


Save your seat!

*Please note: the training is free of charge. However, the project does not cover travel, accommodation or any additional costs.

[Back to overview](#)

Introduction to cybersecurity

Understanding the basic concepts of cybersecurity, password hygiene, explanation of ransomware and phishing attacks, exploiting social engineering and recognition and response in case of their detection, as well as identification of attacks through email


- Proficiency level: beginner
- Target group: operators
- Domain: transport (railway sector)
- Language: Polish
- Duration: 3 hours
- After this course you will be able to recognise cyber threats, pay attention when performing routinary checks to avoid suspicious hardware, apply safe browsing and password hygiene practices and much more
- This training is available online
- Date: 3 September 2024, 9:00 - 13:00 CEST
- Basic track
- Competence unit 1.1: cybersecurity fundamentals
- Provided by  **Polish Platform**
For Homeland Security

Save your seat!

[Back to overview](#)

Introduction to cybersecurity

Understanding the basic concepts of cybersecurity, password hygiene, explanation of ransomware and phishing attacks, exploiting social engineering and recognition and response in case of their detection, as well as identification of attacks through email


- Proficiency level: beginner
- Target group: operators
- Domain: available for SMEs & transport (railway sector)
- Language: English & Polish
- Duration: 3 hours
- After this course you will be able to recognise cyber threats, pay attention when performing routinary checks to avoid suspicious hardware, apply safe browsing and password hygiene practices and much more
- This training is available online, on demand
- Date: starting on 2 September 2024
- Basic track
- Competence unit 1.1: cybersecurity fundamentals
- Provided by  **Polish Platform**
For Homeland Security

Save your seat!

[Back to overview](#)

Today's information security

Introduction to the current cybercrime and cybersecurity scenarios


- Proficiency level: beginner
- Target group: administrative staff
- Domain: transport and manufacturing
- Language: English
- Duration: 3 hours
- After this course you will be able to identify and analyse trends and developments in cyber crime and cybersecurity, recognise the main threat categories and interpret security guidelines and procedures
- This training is available online
- Date: 2 September 2024, 14:00 - 17:00 CEST
- Basic track
- Competence unit 1.1: cybersecurity fundamentals
- Provided by 

Save your seat!

[Back to overview](#)

Today's information security

Introduction to the current cybercrime and cybersecurity scenarios


- Proficiency level: beginner
- Target group: operators
- Domain: transport and manufacturing
- Language: English
- Duration: 3 hours
- After this course you will be able to identify and analyse trends and developments in cyber crime and cybersecurity, recognise the main threat categories and interpret security guidelines and procedures
- This training is available online
- Date: 5 September 2024, 10:00 - 13:00 CEST
- Basic track
- Competence unit 1.1: cybersecurity fundamentals
- Provided by 

Save your seat!

[Back to overview](#)

Today's information security

Introduction to the current cybercrime and cybersecurity scenarios

- Proficiency level: beginner
- Target group: engineers
- Domain: transport and manufacturing
- Language: English
- Duration: 3 hours
- After this course you will be able to identify and analyse trends and developments in cyber crime and cybersecurity, recognise the main threat categories and interpret security guidelines and procedures
- This training is available online
- Date: 19 September 2024, 14:00 - 17:00 CEST
- Basic track
- Competence unit 1.1: cybersecurity fundamentals
- Provided by 

Save your seat!

[Back to overview](#)

Track 1: human related security


The trainings assigned to this track provide a clear understanding of human-centred security problems and solutions

[Back to overview](#)



The evolution of social engineering, exposure and protection of digital identity

Attacks on the human factor and related risks


- Proficiency level: beginner
- Target group: administrative staff
- Domain: transport and manufacturing
- Language: English
- Duration: 3 hours
- After this course you will be able to analyse the evolution of social engineering attacks and strategies for protecting digital identities, recognise human factors in cybersecurity and apply best practices for human resilience
- This training is available online
- Date: 3 October 2024, 10:00 - 13:00 CEST
- Tracks 1 & 2
- Competence unit 3.1: cybersecure behaviour
- Provided by 

Save your seat!

[Back to overview](#)

The evolution of social engineering, exposure and protection of digital identity

Attacks on the human factor and related risks


- Proficiency level: beginner
- Target group: operators
- Domain: transport and manufacturing
- Language: English
- Duration: 3 hours
- After this course you will be able to analyse the evolution of social engineering attacks and strategies for protecting digital identities, recognise human factors in cybersecurity and apply best practices for human resilience
- This training is available online
- Date: 7 October 2024, 10:30 - 13:30 CEST
- Tracks 1 & 2
- Competence unit 3.1: cybersecure behaviour
- Provided by 

Save your seat!

[Back to overview](#)

The evolution of social engineering, exposure and protection of digital identity

Attacks on the human factor and related risks


- Proficiency level: beginner
- Target group: engineers
- Domain: transport and manufacturing
- Language: English
- Duration: 3 hours
- After this course you will be able to analyse the evolution of social engineering attacks and strategies for protecting digital identities, recognise human factors in cybersecurity and apply best practices for human resilience
- This training is available online
- Date: 8 October 2024, 10:00 - 13:00 CEST
- Tracks 1 & 2
- Competence unit 3.1: cybersecure behaviour
- Provided by 

Save your seat!

[Back to overview](#)

Cybersecurity culture & human behaviour – introduction

Understanding human failures, following procedures, effective communication, understanding security culture and organisational factors with additional focus on achieving basic GDPR awareness


- Proficiency level: beginner
- Target group: administrative staff
- Domain: transport and manufacturing
- Language: English
- Duration: 4 hours
- After this course you will be able to foster a secure culture, analyse human factors in cybersecurity and enhance security posture through effective communication, while achieving basic GDPR awareness
- This training can be attended in-person & online
- Date: 9 September, 9:00 – 13:00 CEST
- Track 1: human related security
- Competence unit 3.1: cybersecure behaviour
- Provided by  **deepblue**
consulting & research

Save your seat!

[Back to overview](#)

Cybersecurity culture & human behaviour – introduction

Understanding human failures, following procedures, effective communication, understanding security culture and organisational factors with additional focus on achieving basic GDPR awareness

- Proficiency level: beginner
- Target group: operators
- Domain: transport and manufacturing
- Language: English
- Duration: 4 hours
- After this course you will be able to foster a secure culture, analyse human factors in cybersecurity and enhance security posture through effective communication, while achieving basic GDPR awareness
- This training can be attended in-person & online
- Date: 16 September, 9:00 – 13:00 CEST
- Track 1: human related security
- Competence unit 3.1: cybersecure behaviour
- Provided by  **deepblue**
consulting & research

Save your seat!

[Back to overview](#)

Cybersecurity culture & human behaviour – intermediate

Understanding human behaviour in cybersecurity, analysing past incidents, using tools to mitigate errors, understanding the importance of a just culture, understanding GDPR's implications and developing effective communication strategies

- Proficiency level: skilled
- Target group: administrative staff
- Domain: transport and manufacturing
- Language: English
- Duration: 4 hours
- After this course you will be able to build resilient cybersecurity cultures, distinguish the human role in cyber risks, navigate GDPR complexities and manage crisis communication effectively
- This training can be attended in-person & online
- Date: 13 September, 9:00 – 13:00 CEST
- Track 1: human related security
- Competence unit 3.2: cybersecurity commitment and secure behaviours
- Provided by  **deepblue**
consulting & research

Save your seat!

[Back to overview](#)

Cybersecurity culture & human behaviour – intermediate

Understanding human behaviour in cybersecurity, analysing past incidents, using tools to mitigate errors, understanding the importance of a just culture, understanding GDPR's implications and developing effective communication strategies

- Proficiency level: skilled
- Target group: operators
- Domain: transport and manufacturing
- Language: English
- Duration: 4 hours
- After this course you will be able to build resilient cybersecurity cultures, distinguish the human role in cyber risks, navigate GDPR complexities and manage crisis communication effectively
- This training can be attended in-person & online
- Date: 23 September, 9:00 – 13:00 CEST
- Track 1: human related security
- Competence unit 3.2: cybersecurity commitment and secure behaviours
- Provided by  **deepblue**
consulting & research

Save your seat!

[Back to overview](#)


Track 2: cyber risk related

The trainings assigned to this track delve into cyber risks. The track has two specialisation tracks for DevSecOps and security testers as well as for network specialists and incident responders

[Back to overview](#)

Threat analysis, threat landscaping & threat modelling

How to execute the whole process of threat analysis


- Proficiency level: skilled
- Target group: engineers
- Domain: transport and manufacturing
- Language: English
- Duration: 3 hours
- After this course you will be able to model threats and apply advanced cyber risk assessment frameworks to analyse threats and estimated risks
- Attendants of this course should have a basic understanding of the development process. Basic experience in development in any language is recommended.
- This training is available online
- Date: 14 October 2024, 14:00 - 17:00 CEST
- Track 2: cyber risk related
- Competence unit 2.1: internal policies and procedures
- Provided by 

Save your seat!

[Back to overview](#)

The evolution of social engineering, exposure and protection of digital identity

Attacks on the human factor and related risks


- Proficiency level: beginner
- Target group: administrative staff
- Domain: transport and manufacturing
- Language: English
- Duration: 3 hours
- After this course you will be able to analyse the evolution of social engineering attacks and strategies for protecting digital identities, recognise human factors in cybersecurity and apply best practices for human resilience
- This training is available online
- Date: 3 October 2024, 10:00 - 13:00 CEST
- Tracks 1 & 2
- Competence unit 3.1: cybersecure behaviour
- Provided by 

Save your seat!

[Back to overview](#)

The evolution of social engineering, exposure and protection of digital identity

Attacks on the human factor and related risks


- Proficiency level: beginner
- Target group: operators
- Domain: transport and manufacturing
- Language: English
- Duration: 3 hours
- After this course you will be able to analyse the evolution of social engineering attacks and strategies for protecting digital identities, recognise human factors in cybersecurity and apply best practices for human resilience
- This training is available online
- Date: 7 October 2024, 10:30 - 13:30 CEST
- Tracks 1 & 2
- Competence unit 3.1: cybersecure behaviour
- Provided by 

Save your seat!

[Back to overview](#)

The evolution of social engineering, exposure and protection of digital identity

Attacks on the human factor and related risks

- Proficiency level: beginner
- Target group: engineers
- Domain: transport and manufacturing
- Language: English
- Duration: 3 hours
- After this course you will be able to analyse the evolution of social engineering attacks and strategies for protecting digital identities, recognise human factors in cybersecurity and apply best practices for human resilience
- This training is available online
- Date: 8 October 2024, 10:00 - 13:00 CEST
- Tracks 1 & 2
- Competence unit 3.1: cybersecure behaviour
- Provided by 

Save your seat!

[Back to overview](#)


Track 2.1: DevSecOps specialisation

The trainings assigned to this track are specialised for DevSecOps or developers and security testers

[Back to overview](#)

Introduction to DevSecOps

This scenario is a guide on the basics of DevSecOps


- Proficiency level: expert
- Target group: administrative staff
- Domain: transport and manufacturing
- Language: English
- Duration: 1 hour
- After this course you will be able to understand what DevOps entails
- Attendees should have basic programming and scripting skills, basic DevOps and networking skills as well as knowledge of various operating systems
- This training is available online, on demand
- Date: starting on 1 July 2024
- Track 2.1: DevSecOps specialisation
- Competence unit 1.3: cybersecurity advanced procedures
- Provided by  **CYBER RANGES**
with Silensec

Save your seat!

[Back to overview](#)

Introduction to DevSecOps

This scenario is a guide on the basics of DevSecOps


- Proficiency level: expert
- Target group: engineers
- Domain: transport and manufacturing
- Language: English
- Duration: 1 hour
- After this course you will be able to understand what DevOps entails
- Attendees should have basic programming and scripting skills, basic DevOps and networking skills as well as knowledge of various operating systems
- This training is available online, on demand
- Date: starting on 1 July 2024
- Track 2.1: DevSecOps specialisation
- Competence unit 1.3: cybersecurity advanced procedures
- Provided by  **CYBER RANGES**
with Silensec

Save your seat!

[Back to overview](#)

OWASP TOP 10 part 1

Security introduction, broken access control, cryptographic failures


- Proficiency level: beginner
- Target group: engineers
- Domain: transport and manufacturing
- Language: English
- Duration: 4 hours
- After this course you will be able to navigate web vulnerabilities beyond OWASP TOP 10 and know how to avoid them (focusing on the topics mentioned above)
- This training is available online
- Date: 1 August 2024, 9:00 - 13:00 CEST
- Track 2.1: DevSecOps specialisation
- Competence unit 1.1: cybersecurity fundamentals
- Provided by  **SEARCH-LAB**
SECURITY EVALUATION ANALYSIS
AND RESEARCH LABORATORY

Save your seat!

[Back to overview](#)

OWASP TOP 10 part 2

Injection and insecure design


- Proficiency level: beginner
- Target group: engineers
- Domain: transport and manufacturing
- Language: English
- Duration: 4 hours
- After this course you will be able to navigate web vulnerabilities beyond OWASP TOP 10 and know how to avoid them (focusing on the topics mentioned above)
- This training is available online
- Date: 2 August 2024, 9:00 - 13:00 CEST
- Track 2.1: DevSecOps specialisation
- Competence unit 1.1: cybersecurity fundamentals
- Provided by  **SEARCH-LAB**
SECURITY EVALUATION ANALYSIS
AND RESEARCH LABORATORY

Save your seat!

[Back to overview](#)

OWASP TOP 10 part 3

Security misconfiguration, vulnerable & outdated components, identification & authentication failure


- Proficiency level: beginner
- Target group: engineers
- Domain: transport and manufacturing
- Language: English
- Duration: 4 hours
- After this course you will be able to navigate web vulnerabilities beyond OWASP TOP 10 and know how to avoid them (focusing on the topics mentioned above)
- This training is available online
- Date: 7 August 2024, 9:00 - 13:00 CEST
- Track 2.1: DevSecOps specialisation
- Competence unit 1.1: cybersecurity fundamentals
- Provided by  **SEARCH-LAB**
SECURITY EVALUATION ANALYSIS
AND RESEARCH LABORATORY

Save your seat!

[Back to overview](#)

OWASP TOP 10 part 4

Software & data integrity failures, security logging & monitoring failures, server-side request forgery


- Proficiency level: beginner
- Target group: engineers
- Domain: transport and manufacturing
- Language: English
- Duration: 4 hours
- After this course you will be able to navigate web vulnerabilities beyond OWASP TOP 10 and know how to avoid them (focusing on the topics mentioned above)
- This training is available online
- Date: 9 August 2024, 9:00 - 13:00 CEST
- Track 2.1: DevSecOps specialisation
- Competence unit 1.1: cybersecurity fundamentals
- Provided by  **SEARCH-LAB**
SECURITY EVALUATION ANALYSIS
AND RESEARCH LABORATORY

Save your seat!

[Back to overview](#)

Security testing part 1

Security testing methodology, techniques and tools


- Proficiency level: skilled
- Target group: engineers
- Domain: transport and manufacturing
- Language: English
- Duration: 4 hours
- After this course you will be able to understand security testing approaches and methodologies, get practical knowledge in using security testing techniques and tools
- Attendees should have basic skills of general quality assurance and testing
- This training is available online
- Date: 22 August 2024, 9:00 - 13:00 CEST
- Track 2.1: DevSecOps specialisation
- Competence unit 1.3: cybersecurity advanced procedures
- Provided by  **SEARCH-LAB**
SECURITY EVALUATION ANALYSIS
AND RESEARCH LABORATORY

Save your seat!

[Back to overview](#)

Security testing part 2

Testing the implementation, deployment environment

- Proficiency level: skilled
- Target group: engineers
- Domain: transport and manufacturing
- Language: English
- Duration: 4 hours
- After this course you will get practical knowledge in using security testing techniques and tools and know how to set up and operate the deployment environment securely
- Attendees should have basic skills of general quality assurance and testing
- This training is available online
- Date: 9 September 2024, 9:00 - 13:00 CEST
- Track 2.1: DevSecOps specialisation
- Competence unit 1.3: cybersecurity advanced procedures
- Provided by  **SEARCH-LAB**
SECURITY EVALUATION ANALYSIS
AND RESEARCH LABORATORY

Save your seat!

[Back to overview](#)


Track 2.2: Cybersecurity specialists

The trainings assigned to this track are specialised for network specialists and incident responders

[Back to overview](#)

Incident response – preparation phase

This scenario will walk you through the preparation phase of incident response


- Proficiency level: beginner
- Target group: engineers
- Domain: transport and manufacturing
- Language: English
- Duration: 1 hour
- After this course you will be able to prepare an incident response
- This training is available online, on demand
- Date: starting on 1 July 2024
- Track 2.2: cybersecurity specialists
- Competence unit 1.1: cybersecurity fundamentals
- Provided by  **CYBER RANGES**
with Silensec

Save your seat!

[Back to overview](#)

Incident response – detection and analysis

This scenario will walk you through the detection and analysis phase of incident response as defined by NIST


- Proficiency level: beginner
- Target group: engineers
- Domain: transport and manufacturing
- Language: English
- Duration: 1 hour
- After this course you will be able to detect and analyse an incident during an incident response
- This training is available online, on demand
- Date: starting on 1 July 2024
- Track 2.2: cybersecurity specialists
- Competence unit 1.1: cybersecurity fundamentals
- Provided by  **CYBER RANGES**
with Silensec

Save your seat!

[Back to overview](#)

Incident response – containment, eradication & recovery

This scenario will walk you through the containment eradication and recover phase of incident response


- Proficiency level: beginner
- Target group: engineers
- Domain: transport and manufacturing
- Language: English
- Duration: 1 hour
- After this course you will be able to contain and eradicate an incident and recover from it
- This training is available online, on demand
- Date: starting on 1 July 2024
- Track 2.2: cybersecurity specialists
- Competence unit 1.1: cybersecurity fundamentals
- Provided by  **CYBER RANGES**
with Silensec

Save your seat!

[Back to overview](#)

Incident response – post incident activity

This scenario will walk you through the post incident phase of incident response


- Proficiency level: beginner
- Target group: engineers
- Domain: transport and manufacturing
- Language: English
- Duration: 1 hour
- After this course you will be able to carry out post-incident activities during an incident response
- This training is available online, on demand
- Date: starting on 1 July 2024
- Track 2.2: cybersecurity specialists
- Competence unit 1.1: cybersecurity fundamentals
- Provided by  **CYBER RANGES**
with Silensec

Save your seat!

[Back to overview](#)

Network security and secure communication

Network security from data link to application layer showing common attacks against the used protocols


- Proficiency level: skilled
- Target group: engineers
- Domain: transport and manufacturing
- Language: English
- Duration: 4 hours
- After this course you will be able to understand the basic concepts of security, IT security and secure coding, the requirements of secure communication and much more
- Attendees should have basic skills of network engineering and general software development
- This training is available online
- Date: 23 September 2024, 9:00 - 13:00 CEST
- Track 2.2: cybersecurity specialists
- Competence unit 1.3: cybersecurity advanced procedures
- Provided by  **SEARCH-LAB**
SECURITY EVALUATION ANALYSIS
AND RESEARCH LABORATORY

Save your seat!

[Back to overview](#)

Public key infrastructure

Basics of public key infrastructure and how to use it

- Proficiency level: skilled
- Target group: engineers
- Domain: transport and manufacturing
- Language: English
- Duration: 4 hours
- After this course you will understand the basics of public key infrastructure and how to use it
- Attendees should have basic skills of general C/C++ development
- This training is available online
- Date: 2 October 2024, 9:00 - 13:00 CEST
- Track 2.2: cybersecurity specialists
- Competence unit 1.1: cybersecurity fundamentals
- Provided by  **SEARCH-LAB**
SECURITY EVALUATION ANALYSIS
AND RESEARCH LABORATORY

Save your seat!

[Back to overview](#)

We are happy to support you!



Questions?



www.cyrus-project.eu



info@cyrus-project.eu



This project is co-funded by the European Union. Views and opinions expressed are however those of the author(s) only and do not necessarily reflect those of the European Union or European Health and Digital Executive Agency. Neither the European Union nor the granting authority can be held responsible for them.

