cyVETsecurity

Co-funded by the Erasmus+ Programme of the European Union

O2. Cybersecurity challenges

A map of cybersecurity challenges for different VET profiles

This project has been funded with support from the European Commission. This publication [communication] reflects the views only of the author, and the Commission cannot be held responsible for any use which may be made of the information contained therein.

Table of contents

v. Challenge 11. DevSecOp: integrating security since the development phase (doc for students)
w. Challenge 12. Digital forensics in an unsafe digital world (doc for teachers)
x. Challenge 12. Digital forensics in an unsafe digital world (doc for students)
y. Challenge 13. Perimetral security (doc for teachers)
z. Challenge 13. Perimetral security (doc for students)

1. How to use this document

In this document you will find all the challenges developed by the project partners to acquire the learning outcomes described in "O1. Joint curriculum in cybersecurity in VET". The challenges have been developed according to 4 different profiles, described in O1. This does not mean, in all cases, that the challenges can only be used with those profiles they were created for. Depending on the complexity of the challenge, the target group, the skills (and confidence) of the teacher or the particular needs of companies in each case, a challenge in principle created for profile 1 (someone with a non-technical profile and with low requirements on information security) can be adequate for someone with a profile 3 (technical profile without an specialization in cybersecurity). Indeed, profile 3 includes a variety of professions (mechatronics, CNC operator, automation, and robotics…), very heterogenous, where IT knowledge differs widely. Thus, challenge one could be too simple from someone enrolled or graduate on automation but could be welcome by someone with a CNC operator profile. Moreover, in particular for the challenges exclusively addressed to profile 3 (challenges 5, 6 and 7), we advise that they will be provided by 2 teachers, one with an IT background and another one with an OT background. It could also be possible to use these challenges with mixed groups of students, some with an IT background and some with the OT profile in question (mechatronics, automation, electricity…).

In the map of challenges included in section 2, we have specified which challenges are adequate for each profile, but please take these recommendations in a flexible way and feel free to choose whichever suits your needs and your students´ better. O1 can be of help on this regard, as you will find there all learning outcomes addressed in each profile and then, using the map of challenges, select the one/s more suitable.

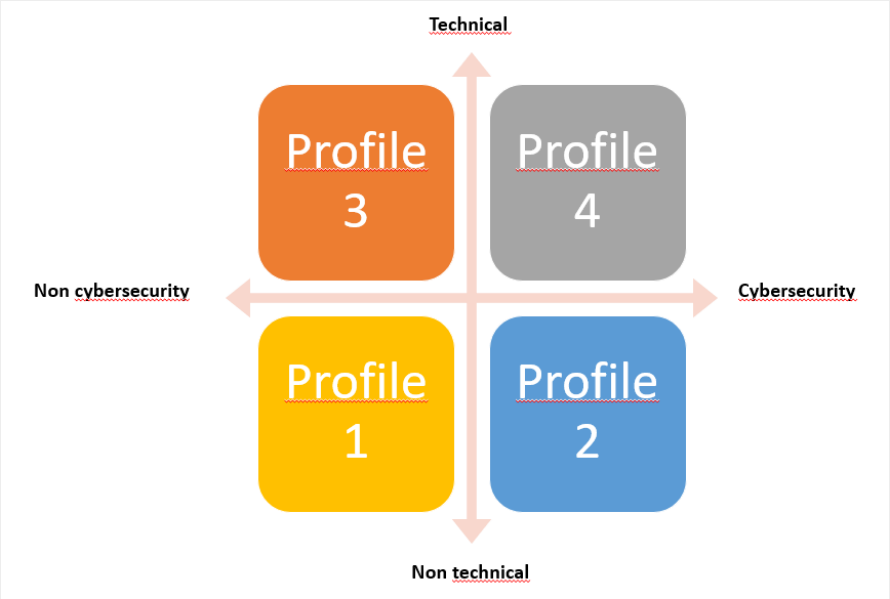
Regarding the way to deliver the challenges, during the project we saw 2 possible options that can suit different learning styles or VET systems. The first one is to present the challenge by the teacher, providing previously some theoretical background on the topics included in the challenge. The second option is to present the challenge to the students without a previous theoretical background, being the students the ones who need to research and figure out which knowledge they will need to solve the challenge. We have used both ways (for example, the first one in Scotland

and the second in the Basque Country) and both ways provide good results in terms of learning so choose the one which suits better your needs or the learning style used with your students.

All the challenges are divided in 2 documents, one for the students and one for the teachers. Both documents are very similar, including the description of the situation, the challenge the students will need to solve, the learning outcomes to be acquired, possible resources to use, the advised steps (and allocation of time to each) to solve the challenge and the assessment criteria. The document for the teachers includes also the previous requirements to carry out each the challenge (previous knowledge, software or equipment) and possible answers/results to be provided by the students for each evaluation criteria, in order to make assessment easier, especially in those cases where teachers are not IT specialists in information security themselves.

2. Map of challenges

The CyVETsecurity challenges were developed according to the different profiles defined in O1. As a reminder:



- **Profile 1** gathers professionals who lie within not technical profiles and who don´t need much cybersecurity knowledge and skills due to their profession, only those necessary for any person (for example, a cook, a car mechanic, a plumber, a nurse…). Modules/units of competence are focused on awareness (cybersecurity hygiene) and will deal with threats types, good practices in social media, threats mitigation and basic cybersecurity awareness.

- **Profile 2** gathers professionals who lie within not technical profiles but who need a higher level of expertise on cybersecurity due to the nature of their work, mainly because they manage sensitive information (for instance, a person working in a bank, an accountant, a person working in an insurance company, the administration of a hospital…). Modules/units of competence will focus mainly on data protection (regulations…) and secure data exchange and storage.

- **Profile 3** gathers professionals who lie within technical profiles but who need only limited knowledge and skills related to cybersecurity, mainly related to their job tasks (a person who works in a CNC machine, in robotics… within the context of an interconnected industry, digital industry, IoT). The units of competence in this profile will focus on cybersecurity related to the connection between OT and IT. As

- **Profile 4** gathers professionals with a technical profile (background in IT) and with specialised knowledge and skills on cybersecurity related to protection/prevention, monitoring and forensics. The units of competence will deal with analysis of vulnerabilities, security management, perimetral security and forensic analysis.

The challenges developed follow the description of these 4 profiles and cover the units of learning outcomes defined as necessary sets of knowledge and skills in cybersecurity for each of them. In the following map of challenges, we match each of them with the different profiles, making some distinctions in profile 3 (as it gathers a set of professions with very different levels of IT skills) and profile 4, as it gathers very different profiles inside the IT world.

	Profile 1	Profile 2	Profile 3		Profile 4				
			Mechatronics, CNC, engineering, electricity…	Automation, electronics, robotics…	Security auditor, network security consultant. VET programmes related: IT/IS audits, IT/IS network management	Security manager VET programmes related: IT/IS audits, IT/IS network management. Administration and IT.	Security software developer VET programmes related: App development, Web development, Multiplatform apps development	Forensic analyst VET programmes related: IT/IS audits, IT/IS network management	Security architect. VET programmes related: IT/IS audits, IT/IS network management, computing science
Challenge 1	X	X	X						
Challenge 2	X	X	X						
Challenge 3		X							
Challenge 4		X							
Challenge 5				X	X	X			
Challenge 6			X	X	X	X			
Challenge 7			X	X	X	X			
Challenge 8			X	X	X				
Challenge 9					X				
Challenge 10						X			
Challenge 11							X		
Challenge 12								X	
Challenge 13									X

cyVETsecurity

Co-funded by the Erasmus+ Programme of the European Union

SAFE DEVICE USE IN AN UNSAFE DIGITAL WORLD

Document for teachers

This project has been funded with support from the European Commission.
This publication [communication] reflects the views only of the author, and the Commission cannot be held responsible for any use which may be made of the information contained therein.

cyVETsecurity

Co-funded by the Erasmus+ Programme of the European Union

Duration of the challenge

3-6 hours

Description of the situation

You have received a new digital device as a gift (the teacher will specify which device you will use). As a responsible digital user, you want to try to ensure that the device and any information are protected where possible.

You plan to use the device for general use, such as email, browsing the web, social networking and online banking.

Your challenge is to demonstrate your understanding and awareness of the cyber security issues that are inherent with new digital devices.

Learning objectives

U1LO1. The learner is able to identify physical and virtual risks associated with technology

U1LO2. The learner is able to implement the strategies to prevent risks and updates themselves in this matter

U1LO3. The learner is able to install / update anti malware software

U1LO4. The learner is able to protect themselves from fraud by using secure passwords.

U1LO5. The learner is able to protect different vulnerable devices from digital threats (malware, phishing etc …)

U1LO6. The learner is able to identify sensitive/valuable information and attacks on different types of data

This project has been funded with support from the European Commission.
This publication [communication] reflects the views only of the author, and the Commission cannot be held responsible for any use which may be made of the information contained therein.

Minimum requirements to carry out the challenge

Previous knowledge	Equipment/software	Training resources
Having had exposure to or use of an internet enabled device such as a PC / Laptop/ Tablet or smartphone	An internet connected device, such as: PC Laptop Smartphone Tablet	• https://en.wikipedia.org/wiki/Computer_security • https://en.wikipedia.org/wiki/Digital_security • https://digitalguardian.com/blog/what-cyber-hygiene-definition-cyber-hygiene-benefits-best-practices-and-more • https://passwordsgenerator.net • https://howsecureismypassword.net/ • https://www.roboform.com/how-secure-is-my-password • https://lastpass.com/howsecure.php *There are a very large body of resources available for this curriculum. Teachers should use all resources available to them. These are the resources that have been issued to the students in the challenge.*

This project has been funded with support from the European Commission.
This publication [communication] reflects the views only of the author, and the Commission cannot be held responsible for any use which may be made of the information contained therein.

cyVETsecurity

Co-funded by the Erasmus+ Programme of the European Union

Schedule of the challenge

Suggested below are notional time allocations for the challenge:

- 0,5 hours to identify the parameters of the challenge (possibly including identifying who will carry out which task (s))
- 1 hour to look for information
- 0,2 hours to select information
- 0,2 hours to generate alternatives
- 0,3 hours to present proposals / collate findings and discuss them (within the student´s group)
- 0,2 hour to identify how findings will be presented (if not stipulated by teacher)
- 0,2 hours to prepare findings into appropriate format i.e. PowerPoint for presentation
- 0,15 hours to present / discuss findings
- 0,15 hours to evaluate / assess how you carried out the challenge and how you might make improvements for any future activities

This project has been funded with support from the European Commission.
This publication [communication] reflects the views only of the author, and the Commission cannot be held responsible for any use which may be made of the information contained therein.

Presentation of the results

The findings can be presented in whatever media the group decide upon. The findings must be in a form that can be retained following the challenge.

This could be a presentation of the findings, which may include but is not restricted to the following formats:

- Video
- Presentation using Software
- Oral \ verbal (This would need to be recorded)
- Written report
- Blog / vlog /wiki
- Any other suitable medium

Note: Teachers should decide the appropriate format for the students to present their results.

This project has been funded with support from the European Commission.
This publication [communication] reflects the views only of the author, and the Commission cannot be held responsible for any use which may be made of the information contained therein.

Evaluation criteria

The following *guidelines* are **suggestive** only and are provided as guidance to support the teacher.

Public presentation (20%)

A ***suggested*** evaluation table in ***Appendix A*** at the back of this document which contains criteria can be used to help the teacher assess public presentation skills

Teamwork performance (20%)

A **suggested** evaluation table in ***Appendix B*** at the back of this document contains criteria that can be used to help the teacher assess team working skills.

Findings from the challenge (60%). Possibly 10% per item.

1. The team groups multiple risks into 3 physical and 3 virtual.

Possible student responses:

Physical risks	Virtual / Software risks
Leaving device unattended/ device being stolen	Not have any anti-virus on device
Water damage to the device	Not updating to most recent software on device (patching)

This project has been funded with support from the European Commission.
This publication [communication] reflects the views only of the author, and the Commission cannot be held responsible for any use which may be made of the information contained therein.

Giving your password to someone	Weak security credentials on device (password / pin etc)

2. The team describes a strategy to prevent being compromised.

Items that ***should*** be included in the strategy (for the user of the device):

- Restricting access to the device by requiring user authentication (this should include an emphasis on pin / biometric (i.e. fingerprint) / strong passwords. 2 factor authentication (2FA) should also be **mentioned** as at the time of writing this is the 'direction of travel' for user authentication.)
- Update your device Operating System with latest security patches
- Regularly back up your data
- Use encryption / secure websites where possible
- Disable any unused services, such as wi-fi and Bluetooth
- Be educated (where possible), don't fall for Phishing etc
- Have up-to-date anti-malware software installed

3. The team installs / updates an anti-malware on a given device

This can be installing of new anti-malware (AM) software or ensuring that the current AM software is the most recent version. NIST.org have a list of guidance on available AM:- https://www.nist.org/news.php?extend.45.11

It also includes a free service where the user can upload any given file to be scanned remotely. https://www.virustotal.com/gui/home/upload. This may be of use if users cannot run scans locally on their device.

This project has been funded with support from the European Commission.
This publication [communication] reflects the views only of the author, and the Commission cannot be held responsible for any use which may be made of the information contained therein.

4. The team generates and tests a secure password

The student ***could*** use the links that are included in the resources section to:

- Generate a password –
- https://passwordsgenerator.net
- Test the generated Password –
- https://howsecureismypassword.net/
- https://www.roboform.com/how-secure-is-my-password
  https://lastpass.com/howsecure.php

5. The team identifies potential vulnerabilities of your new device and possible mechanisms for their protection.

This should be a minimum of 3 potential vulnerabilities and possible protection mechanisms, such as:

Potential vulnerabilities	**Mitigation**
The new device arrives with no authentication	Enable authentication on the device
Services such as wi-fi and Bluetooth are automatically enabled and can be compromised.	Turn off any unused or unnecessary services.
Downloading malware that might be embedded with new apps.	Download only from recommended sites / locations. Ensure anti malware software is installed and up to date.

This project has been funded with support from the European Commission.
This publication [communication] reflects the views only of the author, and the Commission cannot be held responsible for any use which may be made of the information contained therein.

6. The team identifies sensitive data and possible attacks depending on the nature of the data.

Below are some ***examples***:

Platform / Area of concern	**Type of data**	**Attack vector**
Social networks	Personally Identifiable Information (PII)	Social engineering, Phishing etc
Online Banking	Financial, PII	Social engineering, Phishing etc
Discarding old mail into the bin	Financial, PII	Dumpster diving
Email	Images / pictures	Steganography (concealing information inside images)

This project has been funded with support from the European Commission.
This publication [communication] reflects the views only of the author, and the Commission cannot be held responsible for any use which may be made of the information contained therein.

cyVETsecurity

Co-funded by the Erasmus+ Programme of the European Union

Appendix A

Presentation evaluation (Team or Individual)

Criteria	Excellent	Very good	Good	Fair	Not Done	Comments/Suggestions:
Oral Introduction: Introduced speaker, captured audience attention	4	3	2	1	0	
Body of Speech: Easy to follow and understand, information seemed accurate and complete	4	3	2	1	0	
Summary: Brief, clear, and provided a wrap-up of the topic	4	3	2	1	0	
Performance: Speaker showed good inflection, proper pronunciation, used expression to demonstrate points, appeared conversational and natural, made eye contact with audience, and voice was loud and clear enough to hear; reliance on notecards was limited	4	3	2	1	0	
Participant's Knowledge: Participant was able to answer questions from the audience after repeating the question	4	3	2	1	0	
Audience Attention: Held audience's attention for the duration	4	3	2	1	0	
Sources: Sources were listed at the end of the speech	1	0	0	0	0	

This project has been funded with support from the European Commission.
This publication [communication] reflects the views only of the author, and the Commission cannot be held responsible for any use which may be made of the information contained therein.

Appendix B

Goals						
Goals are unclear or poorly understood, resulting in little commitment to them.	1	2	3	4	5	Goals are clear, understood, and have the full commitment of team members.
Openness						
Members are guarded or cautious in discussions.	1	2	3	4	5	Members express thoughts, feelings, and ideas freely.
Mutual Trust						
Members are suspicious of one another's motives.	1	2	3	4	5	Members trust one another and do not fear ridicule or reprisal.
Attitudes Toward Difference						

This project has been funded with support from the European Commission.
This publication [communication] reflects the views only of the author, and the Commission cannot be held responsible for any use which may be made of the information contained therein.

Members smooth over differences and suppress or avoid conflict.	1	2	3	4	5	Members feel free to voice differences and work through them.
Support						
Members are reluctant to ask for or give help.	1	2	3	4	5	Members are comfortable giving and receiving help.
Participation						
Discussion is generally dominated by a few members.	1	2	3	4	5	All members are involved in discussion.
Decision-making						
Decisions are made by only a few members.	1	2	3	4	5	All members are involved in decision-making.
Flexibility						

This project has been funded with support from the European Commission.
This publication [communication] reflects the views only of the author, and the Commission cannot be held responsible for any use which may be made of the information contained therein.

The group is locked into established rules and procedures that members find difficult to change.	1	2	3	4	5	Members readily change procedures in response to new situations.
Use of Member Resources						
Individuals' abilities, knowledge and experience is not well utilized.	1	2	3	4	5	Each member's abilities, knowledge, and experience are fully utilized.

This project has been funded with support from the European Commission.
This publication [communication] reflects the views only of the author, and the Commission cannot be held responsible for any use which may be made of the information contained therein.

cyVETsecurity

Co-funded by the Erasmus+ Programme of the European Union

SAFE DEVICE USE IN AN UNSAFE DIGITAL WORLD

Document for students

This project has been funded with support from the European Commission.
This publication [communication] reflects the views only of the author, and the Commission cannot be held responsible for any use which may be made of the information contained therein.

Duration of the challenge

3-6 hours

Your team

Student / teacher should allocate the following:

Team name:

Team member names:

Description of the situation

You have received a new digital device as a gift (the teacher should specify which device / devices you will use). As a responsible digital user, you want to try to ensure that the device and any information are protected where possible.

You plan to use the device for general use, such as email, browsing the web, social networking and online banking.

Your challenge is to demonstrate your understanding and awareness of the cyber security issues that are inherent with new digital devices.

Learning objectives

U1LO1. The learner is able to identify physical and virtual risks associated with technology

This project has been funded with support from the European Commission.
This publication [communication] reflects the views only of the author, and the Commission cannot be held responsible for any use which may be made of the information contained therein.

U1LO2. The learner is able to implement the strategies to prevent risks and updates themselves in this matter

U1LO3. The learner is able to install / update anti malware software

U1LO4. The learner is able to protect themselves from fraud by using secure passwords.

U1LO5. The learner is able to protect different vulnerable devices from digital threats (malware, phishing etc…)

U1LO6. The learner is able to identify sensitive/valuable information and attacks on different types of data

Resources you can use

Some general resources to help you get started:

- https://en.wikipedia.org/wiki/Computer_security
- https://en.wikipedia.org/wiki/Digital_security
- https://digitalguardian.com/blog/what-cyber-hygiene-definition-cyber-hygiene-benefits-best-practices-and-more
- https://passwordsgenerator.net
- https://howsecureismypassword.net/
- https://www.roboform.com/how-secure-is-my-password
- https://lastpass.com/howsecure.php

Recommended process

In order to solve your challenge, you need to work in an organised way. We suggest you follow these steps:

1. Establish the parameters you need to solve the challenge. For example, in this case these could be: risks associated to technology, protective measures, vulnerable information (prone to be attacked).

This project has been funded with support from the European Commission.
This publication [communication] reflects the views only of the author, and the Commission cannot be held responsible for any use which may be made of the information contained therein.

2. Look for information related to those parameters (see resources proposed, but it is suggested you use others)
3. Select which information is important to solve the challenge.
4. Come up with different proposals to solve the challenge.
5. Select the proposal/proposals which are more effective from your group´s point of view.
6. Plan which actions you need to solve the challenge (once you know what you need to do, describe how you will do it).
7. Implement the actions.
8. Present the results (following teacher´s instructions).
9. Evaluate how you carried out the challenge

Evaluation criteria

- Your team groups multiple risks into 3 physical and 3 virtual.
- Your team describes a strategy to prevent being compromised.
- Your team installs / updates an anti-malware software on a given device.
- Your team generates and tests a secure password
- Your team identifies potential vulnerabilities of your new device and possible mechanisms for their protection.
- Your team identifies sensitive data and possible attacks depending on the nature of the data

This project has been funded with support from the European Commission.
This publication [communication] reflects the views only of the author, and the Commission cannot be held responsible for any use which may be made of the information contained therein.

cyVETsecurity

Co-funded by the Erasmus+ Programme of the European Union

PROTECTION OF PERSONAL DATA AND DIGITAL IDENTITY

Document for teachers

This project has been funded with support from the European Commission.
This publication [communication] reflects the views only of the author, and the Commission cannot be held responsible for any use which may be made of the information contained therein.

cyVETsecurity

Co-funded by the Erasmus+ Programme of the European Union

Duration of the challenge

24 hours / 3 days

Description of the situation

You have received a new digital device as a gift (the teacher will specify which device you will use). As a responsible digital user, you want to try to ensure that the device and any information are protected where possible.

You plan to use the device for general use, such as email, browsing the web, social networking and online banking.

Your challenge is to demonstrate your understanding and awareness of the cyber security issues that are inherent with new digital devices.

In particular you are required to focus on how your personal data and digital identify can be protected from possible security breaches, this will focus also on your online presence.

Learning objectives

U2LO1. The learner is able to adequate behaviour in the digital world and manage his/her digital trace properly

U2LO2. The learner is able to identify the perils of getting stolen or misused his/her digital identify by others

U2LO3. The learner is able to protect information relative to other people from his/her environment (as a worker/as a friend)

U2LO4. The learner is able to find, erase and/or modify information online about him/herself

U2LO5. The learner is able to manage his/her own digital trace

U2LO6. The learner is able to act in a critical way when sharing information online about him/herself

This project has been funded with support from the European Commission.
This publication [communication] reflects the views only of the author, and the Commission cannot be held responsible for any use which may be made of the information contained therein.

U2LO7. The learner is able to make use of multiple digital identities, addressed to different objectives

Minimum requirements to carry out the challenge

Previous knowledge	Equipment/ software	Training resources
Having had exposure to or use of an internet enabled device such as a PC / Laptop/ Tablet or smartphone	An internet connected device, such as: PC Laptop Smartphone Tablet	• http://www.identitytheft.org.uk/ • http://digitalfootprintimu.weebly.com/measure-your-footprint.html • https://www.tomsguide.com/us/personally-identifiable-information-definition,news-18036.html • https://www.bing.com/videos/search?q=How+to+Be+Safe+Online&&view=detail&mid=D895C76F4EB8001A78B0D895C76F4EB8001A78B0&&FORM=VRDGAR • https://www.bing.com/videos/search?q=How+to+Be+Safe+Online&&view=detail&mid=5824FB060F03A2765DDD5824FB060F03A2765DDD&&FORM=VDRVRV • https://staysafeonline.org/stay-safe-online/securing-key-accounts-devices/social-media/ • https://www.bing.com/videos/search?q=how+to+keep+information+secure+on+a+computer&&view=detail&mid=62715D037BCDF795775C62715D037BCDF795775C&&FORM=VRDGAR • https://www.bing.com/videos/search?q=how+to+protect+your+passwords+logins&&view=detail&mid=3

This project has been funded with support from the European Commission.
This publication [communication] reflects the views only of the author, and the Commission cannot be held responsible for any use which may be made of the information contained therein.

		FEF7F7615BF3B1226653FEF7F7615BF3B122665&&FORM=VDRVRV *There are a very large body of resources available for this curriculum. Teachers should use all resources available to them.* *These are the resources that have been issued to the students in the challenge.*

This project has been funded with support from the European Commission.
This publication [communication] reflects the views only of the author, and the Commission cannot be held responsible for any use which may be made of the information contained therein.

cyVETsecurity

Co-funded by the Erasmus+ Programme of the European Union

Schedule of the challenge

Suggested below are notional time allocations for the challenge:

- 2 hours to identify the parameters of the challenge (possibly including identifying who will carry out which task (s))
- 10 hours to look for information
- 2 hours to select information
- 2 hours to generate alternatives
- 2 hours to present proposals / collate findings and discuss them (within the student´s group)
- 1 hour to identify how findings will be presented (if not stipulated by teacher)
- 2 hours to prepare findings into appropriate format i.e. PowerPoint for presentation
- 2 hours to present / discuss findings
- 1 hour to evaluate / assess how you carried out the challenge and how you might make improvements for any future activities

This project has been funded with support from the European Commission.
This publication [communication] reflects the views only of the author, and the Commission cannot be held responsible for any use which may be made of the information contained therein.

Presentation of the results

The findings can be presented in whatever media the group decide upon. The findings must be in a form that can be retained following the challenge.

This could be a presentation of the findings, which may include but is not restricted to the following formats:

- Video
- Presentation using Software
- Oral \ verbal (This would need to be recorded)
- Written report
- Blog / vlog /wiki
- Any other suitable medium

Note: Teachers should decide the appropriate format for the students to present their results.

This project has been funded with support from the European Commission.
This publication [communication] reflects the views only of the author, and the Commission cannot be held responsible for any use which may be made of the information contained therein.

Evaluation criteria

The following *guidelines* are **suggestive** only and are provided as guidance to support the teacher.

Public presentation (20%)

A ***suggested*** evaluation table in ***Appendix A*** at the back of this document which contains criteria can be used to help the teacher assess public presentation skills

Teamwork performance (10%)

A **suggested** evaluation table in ***Appendix B*** at the back of this document contains criteria that can be used to help the teacher assess team working skills.

Findings from the challenge (70%). Possibly 10% per item.

1. The team is able to describe and understand the concept of their digital footprint and digital trace and regulation requirement.

Possible student responses:
Able to have an awareness of GDPR and its implications
When conducting web searching will have an awareness of how analytics works in the background of this process.

This project has been funded with support from the European Commission.
This publication [communication] reflects the views only of the author, and the Commission cannot be held responsible for any use which may be made of the information contained therein.

Digital footprint – student is aware of the 'mark' they leave online for content that they access – eg job applications and online profile being considered as part of this process.

2. The team describes the disadvantages of their PII (personal identifiable information) being used by others.

Items that should be included:

- Student is able to identify and explain what is meant by identify theft
- Student is able to identify and explain 3 scenarios in which their PII can be stolen
- Student is able to explain the disadvantages/risks to individuals/businesses of their PII being accessed

3. The team is able to identify and explain techniques which can be used to protect PII for both individuals and businesses

The following items should be included:

- Student is able to consider Password complexity
- Student is able to recommend password security storage methods
- Student is able to identify and explain how often and why password should be changed
- In a business environment students should be able to identify and explain ways in which PII can be protected on computer eg physical security and locking computer or logging off when moving away from it eg on breaks etc

This project has been funded with support from the European Commission.
This publication [communication] reflects the views only of the author, and the Commission cannot be held responsible for any use which may be made of the information contained therein.

4. The team and individually are able to find and edit information on their online profiles both personally and from an organisation perspective for information held on individuals

The following items should be included:

- The students collectively are able to edit and modify at least 3 different online profiles
- The students are able to identify and explain how they can get access to modifying their details held by at least 2 organisations
- The students are able to measure their digital footprint using online calculation website

5. The team are able to manage their digital trace/footprint

- The students are able to use online resources to manage their digital footprint and how they can make changes to it

6. The team are able to identify methods to use to ensure their PII is being shared safely and securely

- The students are able to identify at least 3 methods for sharing PII safely and securely
- The students are able to identify at least 3 methods which could be used to unlawfully extract PII from them

7. The team are able to use the most suitable digital identify for specific purposes for both individuals and businesses

This project has been funded with support from the European Commission.
This publication [communication] reflects the views only of the author, and the Commission cannot be held responsible for any use which may be made of the information contained therein.

• The students are able to setup and use a suitable online profiles for businesses, giving reasons for the options they select • The students are able to setup and use a suitable online profiles for individuals, giving reasons for the options they select on the social media profiles

This project has been funded with support from the European Commission.
This publication [communication] reflects the views only of the author, and the Commission cannot be held responsible for any use which may be made of the information contained therein.

cyVETsecurity

Co-funded by the Erasmus+ Programme of the European Union

Appendix A

Presentation evaluation (Team or Individual)

Criteria	Excellent	Very good	Good	Fair	Not Done	Comments/Suggestions:
Oral Introduction: Introduced speaker, captured audience attention	4	3	2	1	0	
Body of Speech: Easy to follow and understand, information seemed accurate and complete	4	3	2	1	0	
Summary: Brief, clear, and provided a wrap-up of the topic	4	3	2	1	0	
Performance: Speaker showed good inflection, proper pronunciation, used expression to demonstrate points, appeared conversational and natural, made eye contact with audience, and voice was loud and clear enough to hear; reliance on notecards was limited	4	3	2	1	0	
Participant's Knowledge: Participant was able to answer questions from the audience after repeating the question	4	3	2	1	0	
Audience Attention: Held audience's attention for the duration	4	3	2	1	0	
Sources: Sources were listed at the end of the speech	1	0	0	0	0	

This project has been funded with support from the European Commission.
This publication [communication] reflects the views only of the author, and the Commission cannot be held responsible for any use which may be made of the information contained therein.

cyVETsecurity

Co-funded by the Erasmus+ Programme of the European Union

Appendix B

Goals						
Goals are unclear or poorly understood, resulting in little commitment to them.	1	2	3	4	5	Goals are clear, understood, and have the full commitment of team members.
Openness						
Members are guarded or cautious in discussions.	1	2	3	4	5	Members express thoughts, feelings, and ideas freely.
Mutual Trust						
Members are suspicious of one another's motives.	1	2	3	4	5	Members trust one another and do not fear ridicule or reprisal.
Attitudes Toward Difference						

This project has been funded with support from the European Commission.
This publication [communication] reflects the views only of the author, and the Commission cannot be held responsible for any use which may be made of the information contained therein.

Members smooth over differences and suppress or avoid conflict.	1	2	3	4	5	Members feel free to voice differences and work through them.
Support						
Members are reluctant to ask for or give help.	1	2	3	4	5	Members are comfortable giving and receiving help.
Participation						
Discussion is generally dominated by a few members.	1	2	3	4	5	All members are involved in discussion.
Decision-making						
Decisions are made by only a few members.	1	2	3	4	5	All members are involved in decision-making.
Flexibility						

This project has been funded with support from the European Commission.
This publication [communication] reflects the views only of the author, and the Commission cannot be held responsible for any use which may be made of the information contained therein.

The group is locked into established rules and procedures that members find difficult to change.	1	2	3	4	5	Members readily change procedures in response to new situations.
Use of Member Resources						
Individuals' abilities, knowledge and experience is not well utilized.	1	2	3	4	5	Each member's abilities, knowledge, and experience are fully utilized.

This project has been funded with support from the European Commission.
This publication [communication] reflects the views only of the author, and the Commission cannot be held responsible for any use which may be made of the information contained therein.

cyVETsecurity

Co-funded by the Erasmus+ Programme of the European Union

PROTECTION OF PERSONAL DATA AND DIGITAL IDENTITY

Document for students

This project has been funded with support from the European Commission.
This publication [communication] reflects the views only of the author, and the Commission cannot be held responsible for any use which may be made of the information contained therein.

cyVETsecurity

Co-funded by the Erasmus+ Programme of the European Union

Duration of the challenge

24 hours / 3 days

Your team

Student / teacher should allocate the following:

Team name:

Team member names:

Description of the situation

You have received a new digital device as a gift (the teacher will specify which device you will use). As a responsible digital user, you want to try to ensure that the device and any information are protected where possible.

You plan to use the device for general use, such as email, browsing the web, social networking and online banking.

Your challenge is to demonstrate your understanding and awareness of the cyber security issues that are inherent with new digital devices.

In particular you are required to focus on how your personal data and digital identify can be protected from possible security breaches, this will focus also on your online presence.

Learning objectives

U2LO1. The learner is able to control behaviour in the digital world and manage his/her digital trace properly

U2LO2. The learner is able to identify the perils of getting stolen or misused his/her digital identify by others

U2LO3. The learner is able to protect information relative to other people from his/her environment (as a worker, as a friend.)

This project has been funded with support from the European Commission.
This publication [communication] reflects the views only of the author, and the Commission cannot be held responsible for any use which may be made of the information contained therein.

U2LO4. The learner is able to find, erase and/or modify information online about him/herself

U2LO5. The learner is able to manage his/her own digital trace

U2LO6. The learner is able to act in a critical way when sharing information online about him/herself

U2LO7. The learner is able to make use of multiple digital identities, addressed to different objectives

Resources you can use

Some general resources to help you get started:

- http://www.identitytheft.org.uk/
- https://www.tomsguide.com/us/personally-identifiable-information-definition,news-18036.html
- https://www.bing.com/videos/search?q=How+to+Be+Safe+Online&&view=detail&mid=D895C76F4EB8001A78B0D895C76F4EB8001A78B0&&FORM=VRDGAR
- https://www.bing.com/videos/search?q=How+to+Be+Safe+Online&&view=detail&mid=5824FB060F03A2765DDD5824FB060F03A2765DDD&&FORM=VDRVRV
- https://www.bing.com/videos/search?q=how+to+keep+information+secure+on+a+computer&&view=detail&mid=62715D037BCDF795775C62715D037BCDF795775C&&FORM=VRDGAR
- https://www.bing.com/videos/search?q=how+to+protect+your+passwords+logins&&view=detail&mid=3FEF7F7615BF3B1226653FEF7F7615BF3B122665&&FORM=VDRVRV

Recommended process

In order to solve your challenge, you need to work in an organised way. We suggest you follow these steps:

This project has been funded with support from the European Commission.
This publication [communication] reflects the views only of the author, and the Commission cannot be held responsible for any use which may be made of the information contained therein.

1. Establish the parameters you need to solve the challenge. For example, in this case these could be: risks associated to technology, protective measures, vulnerable information (prone to be attacked).
2. Look for information related to those parameters (see resources proposed, but it is suggested you use others)
3. Select which information is important to solve the challenge.
4. Come up with different proposals to solve the challenge.
5. Select the proposal/proposals which are more effective from your group´s point of view.
6. Plan which actions you need to solve the challenge (once you know what you need to do, describe how you will do it).
7. Implement the actions.
8. Present the results (following teacher´s instructions).
9. Evaluate how you carried out the challenge

Evaluation criteria

- Your team is able to describe and understand the concept of their digital footprint and digital trace and regulation requirement.
- Your team describes the disadvantages of their PII being used by others
- Your team is able to identify and explain techniques which can be used to protect PII for both individuals and businesses
- Your team and individually are able to find and edit information on their online profiles both personally and from an organisation perspective for information held on individuals
- Your team are able to manage their digital trace/footprint
- Your team are able to identify methods to use to ensure their PII is being shared safely and securely

This project has been funded with support from the European Commission.
This publication [communication] reflects the views only of the author, and the Commission cannot be held responsible for any use which may be made of the information contained therein.

- Your team are able to use the most suitable digital identify for specific purposes for both individuals and businesses

This project has been funded with support from the European Commission.
This publication [communication] reflects the views only of the author, and the Commission cannot be held responsible for any use which may be made of the information contained therein.

cyVETsecurity

Co-funded by the Erasmus+ Programme of the European Union

Information Security as Part of Organisation's Security Practices

&

Introduction to Cyber Security Defence

Document for teachers

This project has been funded with support from the European Commission.
This publication [communication] reflects the views only of the author, and the Commission cannot be held responsible for any use which may be made of the information contained therein.

cyVETsecurity

Co-funded by the Erasmus+ Programme of the European Union

Duration of the challenge

12 hours / 2 days

Description of the situation

You participate in an information security exercise at your company. You will find three different real-life examples that you need to look at from the perspective of your organization or example company. Company can be real or fictional.

The challenge contains three real examples that utilize typical features of real-life security incidents, misconduct, and crime. In each case, the risks associated with the event are analysed and current security issues are highlighted. Read each scenario and discuss with your colleague / group. Pick up useful tips and advice. Put events in the context of your own business and ask the questions: Could this happen in our company? How should we prepare for such a situation? Start the necessary actions to business data security risks can be better management.

Your challenge is to find the right solutions (prevent those things to happen again in future) all of three scenarios for your business by discuss to your group/colleagues and presenting the solutions you find in your business.

Scenario 1 CEO scam: The last office minutes of Friday afternoon are on the way. This will cause the email to drop, which should be dealt with urgently. From Sally Spectra, CFO of the company. All right - drop off for a quick checkout and then spend the weekend.

For example, this is how the CEO fraud can go. The offender will contact the financial management of the company or the person authorized to handle payment transactions and

This project has been funded with support from the European Commission.
This publication [communication] reflects the views only of the author, and the Commission cannot be held responsible for any use which may be made of the information contained therein.

apply pressure through an urgent credit transfer. He may represent the company's CFO or CEO and possibly also a representative of the partner firm, such as a lawyer. Contacts are made by email or phone around the end of the workday, typically on a Friday, with the recipient having the least time and concentration to start figuring out what it really is. A cheater who does his background work can increase his credibility by mentioning the names of familiar colleagues.

A request for payment via email may have an email address that is almost identical to the real business, such as sally.spectra@company.com instead of sally.spectra@conpany.com. The message can also come from just the right person, but it is also used by a hacker who has broken into an email. (Säästöpankki Finnish bank https://www.saastopankki.fi/fi-fi/asiakaspalvelu/vinkit/yrittajyys/yrittaja-ala-lankea-laskuhuijauksiin. Referred to 15.10.2019)

Scenario 2 Microsoft Office 365 account under attack: The wave of attacks on Office 365 badges is not going away. Attacks have evolved over the past year to make it more difficult to identify. Tivi (Finnish IT-newspaper) was contacted by a reader who was a victim of phishing this week. He had received a link to a Dropbox from someone he knew, with the title: "Proposal 2019.pdf". The file came from no-reply@dropbox.com and was sent by the person with whom he had been discussing a specific agreement. He expected the shared file to be related to this issue. "There was nothing to suggest that this was a scam," the person tells Tivi. After opening a PDF file shared with Dropbox, he ended up with a link to a page prompting him to sign in to Office 365. The recipient of the message entered his Office 365 login on the site. He realized his e-mail had been hijacked after he began receiving surprising contacts from his contacts.

Some of his English-speaking acquaintances had tried to inquire by replying to an e-mail whether it was a virus.

"Strangely enough, they had received an English response that denied it was a virus and called for the file to be opened and returned," wonders to Tivi.

This project has been funded with support from the European Commission.
This publication [communication] reflects the views only of the author, and the Commission cannot be held responsible for any use which may be made of the information contained therein.

The phenomenon is familiar to the Finnish Transport and Communications Agency's Traficom Cyber Security Center. According to security expert Ville Kontinen, similar scams are being carried out by constantly exploiting not only Dropbox but also files shared through Google Drive and SharePoint services, for example.

“The way it works is that once one victim has been taken over, he or she will be able to distribute files extensively to the victim through unknown services. The pdf is open to everyone with a direct link,” says Kontinen.

Files are shared on behalf of the victim through a file sharing service. Some of the sharing accounts may have been previously hijacked and the victims' accounts will be left with files for later use.

The PDF file that opens from the file service includes, for example, a genuine SharePoint logo and a button that you are advised to press. It is possible to include hypertext links in a pdf file in the same way as in Word files, for example. (Finnish IT-newspaper https://www.tivi.fi/uutiset/varo-aitoa-dropbox-viestia-ovela-huijaus-kaappaa-office-tunnukset/a2c0295f-aece-4696-ab51-edb19ff52448. Referred to 15.10.2019)

Scenario 3 Stolen laptop: WASHINGTON (Reuters) - The U.S. Secret Service said on Friday a laptop was stolen from an agent’s car in New York City but that such agency-issued computers contain multiple layers of security and are not permitted to contain classified information.

The agency said in a statement that it was withholding additional comment while an investigation continues.

ABC News, citing law enforcement sources, said the laptop contained floor plans for Trump Tower, details on the criminal investigation of Hillary Clinton’s use of a private email server

This project has been funded with support from the European Commission.
This publication [communication] reflects the views only of the author, and the Commission cannot be held responsible for any use which may be made of the information contained therein.

and other national security information.

The New York Daily News, citing police sources, said authorities had been searching for the laptop since it was stolen on Thursday morning from the agent's vehicle in the New York City borough of Brooklyn.

Some items stolen with the laptop, including coins and a black bag with the Secret Service insignia on it, were later recovered, the newspaper reported.

CBS News, also citing law enforcement sources, said that some of the documents on the computer included important files on Pope Francis.
The agent also told investigators that while nothing about the White House or foreign leaders is stored on the laptop, the information there could compromise national security, the Daily News reported.

"There's data on there that's highly sensitive," a police source told the newspaper, adding: "They're scrambling like mad."

Separately CNN, citing an unnamed U.S. Secret Service source, reported on Friday that a California man who scaled the White House fence last week was on the property's south grounds for at least 15 minutes before he was captured. (Reuters https://www.reuters.com/article/us-usa-trump-laptop/secret-service-says-laptop-stolen-from-agents-car-in-new-york-idUSKBN16O2EH Referred to 15.10.2019)

This project has been funded with support from the European Commission.
This publication [communication] reflects the views only of the author, and the Commission cannot be held responsible for any use which may be made of the information contained therein.

Learning objectives

U4L01: The learner is able to observe, assess, prevent and report information risks in work place

U4L02: The learner is able to utilise organisation's security systems in relation with information security

U4L03: The learner is able to manage physical security in the premises

U4L04: The learner is able to work safely in mobile and cloud services

U4L05: The learner is able to ensure material and data storage and protection

U4L06: The learner is able to apply basics of software safety: operating systems, applications

U5L01: The learner is able to identify critical information from different media

U5L02: The learner is able to assess the vulnerability of critical infrastructure for society

U5L03: The learner is able to identify cyber-attacks and threats

Minimum requirements to carry out the challenge

Previous knowledge	Equipment/software	Training resources
Basic knowledge about email software's.	Electronic device with Internet connection for information search.	• National Cyber Security Centre Finland. Online publication (ISSN 1799-0157) Protection against Microsoft Office 365 credential phishing and data breaches • Police university college. Cybercrime, Law and Technology in Finland and Beyond • General Data Protection Regulation GPDR • Each group should find at least two national resources

This project has been funded with support from the European Commission.
This publication [communication] reflects the views only of the author, and the Commission cannot be held responsible for any use which may be made of the information contained therein.

cyVETsecurity

Co-funded by the Erasmus+ Programme of the European Union

Schedule of the challenge

Suggested below are notional time allocations for the challenge:

- 2 hours to identify the parameters of the challenge (possibly including identifying who will carry out which task (s))
- 4 hours to look for information
- 2 hours to present proposals / collate findings and discuss them (within the student´s group)
- 2 hours to prepare findings into appropriate format i.e. PowerPoint for presentation
- 1 hours to present / discuss findings
- 1 hour to evaluate / assess how you carried out the challenge and how you might make improvements for any future activities

This project has been funded with support from the European Commission.
This publication [communication] reflects the views only of the author, and the Commission cannot be held responsible for any use which may be made of the information contained therein.

cyVETsecurity

Co-funded by the Erasmus+ Programme of the European Union

Presentation of the results

The findings can be presented in whatever media the group decide upon. The findings must be in a form that can be retained following the challenge.

This could be a presentation of the findings, which may include but is not restricted to the following formats:

- Video
- Presentation
- Verbal
- Written report
- Blog, vlog, wiki, podcast
- Any other suitable media

This project has been funded with support from the European Commission.
This publication [communication] reflects the views only of the author, and the Commission cannot be held responsible for any use which may be made of the information contained therein.

Evaluation criteria

The following *guidelines* are **suggestive** only and are provided as guidance to support the teacher.

Public presentation (15%)

A ***suggested*** evaluation table in ***Appendix A*** at the back of this document which contains criteria can be used to help the teacher assess public presentation skills

Teamwork performance (30%)

A **suggested** evaluation table in ***Appendix B*** at the back of this document contains criteria that can be used to help the teacher assess team working skills.

Findings from the challenge (55%). Possibly 10% per item.

- **Scenario 1**
  - **Human factor effects?**
  - **Exploitation of trust**
- **Scenario 2: keywords**
  - **Phishing**
  - **hacking, identity theft and fraud.**
  - **Fake sites**
  - **Two-step authentication**
  - **Multifactor (2FA, MFA)**
  - **Financial benefits**
  - **Sensitive data**

This project has been funded with support from the European Commission.
This publication [communication] reflects the views only of the author, and the Commission cannot be held responsible for any use which may be made of the information contained therein.

- **Scenario 3: key words**
  - **National security**
  - **Information security practices & policies**
  - **Physical security**
  - **Remote control**

This project has been funded with support from the European Commission.
This publication [communication] reflects the views only of the author, and the Commission cannot be held responsible for any use which may be made of the information contained therein.

Appendix A

Presentation evaluation (Team or Individual)

Criteria	Excellent	Very good	Good	Fair	Not Done	Comments/Suggestions:
Oral Introduction: Introduced speaker, captured audience attention	4	3	2	1	0	
Body of Speech: Easy to follow and understand, information seemed accurate and complete	4	3	2	1	0	
Summary: Brief, clear, and provided a wrap-up of the topic	4	3	2	1	0	
Performance: Speaker showed good inflection, proper pronunciation, used expression to demonstrate points, appeared conversational and natural, made eye contact with audience, and voice was loud and clear enough to hear; reliance on notecards was limited	4	3	2	1	0	
Participant's Knowledge: Participant was able to answer questions from the audience after repeating the question	4	3	2	1	0	
Audience Attention: Held audience's attention for the duration	4	3	2	1	0	
Sources: Sources were listed at the end of the speech	1	0	0	0	0	

This project has been funded with support from the European Commission.
This publication [communication] reflects the views only of the author, and the Commission cannot be held responsible for any use which may be made of the information contained therein.

cyVETsecurity

Co-funded by the Erasmus+ Programme of the European Union

Appendix B

Goals						
Goals are unclear or poorly understood, resulting in little commitment to them.	1	2	3	4	5	Goals are clear, understood, and have the full commitment of team members.
Openness						
Members are guarded or cautious in discussions.	1	2	3	4	5	Members express thoughts, feelings, and ideas freely.
Mutual Trust						
Members are suspicious of one another's motives.	1	2	3	4	5	Members trust one another and do not fear ridicule or reprisal.
Attitudes Toward Difference						

This project has been funded with support from the European Commission.
This publication [communication] reflects the views only of the author, and the Commission cannot be held responsible for any use which may be made of the information contained therein.

Members smooth over differences and suppress or avoid conflict.	1	2	3	4	5	Members feel free to voice differences and work through them.
Support						
Members are reluctant to ask for or give help.	1	2	3	4	5	Members are comfortable giving and receiving help.
Participation						
Discussion is generally dominated by a few members.	1	2	3	4	5	All members are involved in discussion.
Decision-making						
Decisions are made by only a few members.	1	2	3	4	5	All members are involved in decision-making.
Flexibility						

This project has been funded with support from the European Commission.
This publication [communication] reflects the views only of the author, and the Commission cannot be held responsible for any use which may be made of the information contained therein.

The group is locked into established rules and procedures that members find difficult to change.	1	2	3	4	5	Members readily change procedures in response to new situations.
Use of Member Resources						
Individuals' abilities, knowledge and experience is not well utilized.	1	2	3	4	5	Each member's abilities, knowledge, and experience are fully utilized.

This project has been funded with support from the European Commission.
This publication [communication] reflects the views only of the author, and the Commission cannot be held responsible for any use which may be made of the information contained therein.

cyVETsecurity

Co-funded by the Erasmus+ Programme of the European Union

Information security as part of organisation´s security practices and Introduction to cybersecurity defence (doc for students)

Document for students

This project has been funded with support from the European Commission.
This publication [communication] reflects the views only of the author, and the Commission cannot be held responsible for any use which may be made of the information contained therein.

cyVETsecurity

Co-funded by the Erasmus+ Programme of the European Union

Duration of the challenge

8 hours

Your team

Student / teacher should allocate the following:

Team name:

Team member names:

Description of the situation

You participate in an information security exercise at your company. You will find three different real-life examples that you need to look at from the perspective of your organization or example company. Company can be real or fictional.

The challenge contains three real examples that utilize typical features of real-life security incidents, misconduct, and crime. In each case, the risks associated with the event are analysed and current security issues are highlighted. Read each scenario and discuss with your colleague / group. Pick up useful tips and advice. Put events in the context of your own business and ask the questions: Could this happen in our company? How should we prepare for such a situation? Start the necessary actions to business data security risks can be better management.

Your challenge is to find the right solutions (prevent those things to happen again in future) all of three scenarios for your business by discuss to your group/colleagues and presenting the solutions you find in your business.

This project has been funded with support from the European Commission.
This publication [communication] reflects the views only of the author, and the Commission cannot be held responsible for any use which may be made of the information contained therein.

Scenario 1 CEO scam: The last office minutes of Friday afternoon are on the way. This will cause the email to drop, which should be dealt with urgently. From Sally Spectra, CFO of the company. All right - drop off for a quick checkout and then spend the weekend.

For example, this is how the CEO fraud can go. The offender will contact the financial management of the company or the person authorized to handle payment transactions and apply pressure through an urgent credit transfer. He may represent the company's CFO or CEO and possibly also a representative of the partner firm, such as a lawyer. Contacts are made by email or phone around the end of the workday, typically on a Friday, with the recipient having the least time and concentration to start figuring out what it really is. A cheater who does his background work can increase his credibility by mentioning the names of familiar colleagues.

A request for payment via email may have an email address that is almost identical to the real business, such as sally.spectra@company.com instead of sally.spectra@conpany.com. The message can also come from just the right person, but it is also used by a hacker who has broken into an email. (Säästöpankki Finnish bank https://www.saastopankki.fi/fi-fi/asiakaspalvelu/vinkit/yrittajyys/yrittaja-ala-lankea-laskuhuijauksiin. Referred to 15.10.2019)

Scenario 2 Microsoft Office 365 account under attack: The wave of attacks on Office 365 badges is not going away. Attacks have evolved over the past year to make it more difficult to identify. Tivi (Finnish IT-newspaper) was contacted by a reader who was a victim of phishing this week. He had received a link to a Dropbox from someone he knew, with the title: "Proposal 2019.pdf". The file came from no-reply@dropbox.com and was sent by the

This project has been funded with support from the European Commission.
This publication [communication] reflects the views only of the author, and the Commission cannot be held responsible for any use which may be made of the information contained therein.

person with whom he had been discussing a specific agreement. He expected the shared file to be related to this issue. "There was nothing to suggest that this was a scam," the person tells Tivi. After opening a PDF file shared with Dropbox, he ended up with a link to a page prompting him to sign in to Office 365. The recipient of the message entered his Office 365 login on the site. He realized his e-mail had been hijacked after he began receiving surprising contacts from his contacts.

Some of his English-speaking acquaintances had tried to inquire by replying to an e-mail whether it was a virus.

"Strangely enough, they had received an English response that denied it was a virus and called for the file to be opened and returned," wonders to Tivi.

The phenomenon is familiar to the Finnish Transport and Communications Agency's Traficom Cyber Security Center. According to security expert Ville Kontinen, similar scams are being carried out by constantly exploiting not only Dropbox but also files shared through Google Drive and SharePoint services, for example.

“The way it works is that once one victim has been taken over, he or she will be able to distribute files extensively to the victim through unknown services. The pdf is open to everyone with a direct link,” says Kontinen.

Files are shared on behalf of the victim through a file sharing service. Some of the sharing accounts may have been previously hijacked and the victims' accounts will be left with files for later use.

The PDF file that opens from the file service includes, for example, a genuine SharePoint logo and a button that you are advised to press. It is possible to

This project has been funded with support from the European Commission.
This publication [communication] reflects the views only of the author, and the Commission cannot be held responsible for any use which may be made of the information contained therein.

include hypertext links in a pdf file in the same way as in Word files, for example. (Finnish IT-newspaper https://www.tivi.fi/uutiset/varo-aitoa-dropbox-viestia-ovela-huijaus-kaappaa-office-tunnukset/a2c0295f-aece-4696-ab51-edb19ff52448. Referred to 15.10.2019)

Scenario 3 Stolen laptop: WASHINGTON (Reuters) - The U.S. Secret Service said on Friday a laptop was stolen from an agent's car in New York City but that such agency-issued computers contain multiple layers of security and are not permitted to contain classified information.

The agency said in a statement that it was withholding additional comment while an investigation continues.

ABC News, citing law enforcement sources, said the laptop contained floor plans for Trump Tower, details on the criminal investigation of Hillary Clinton's use of a private email server and other national security information.

The New York Daily News, citing police sources, said authorities had been searching for the laptop since it was stolen on Thursday morning from the agent's vehicle in the New York City borough of Brooklyn.

Some items stolen with the laptop, including coins and a black bag with the Secret Service insignia on it, were later recovered, the newspaper reported.

CBS News, also citing law enforcement sources, said that some of the documents on the computer included important files on Pope Francis.
The agent also told investigators that while nothing about the White House or foreign leaders is stored on the laptop, the information there could compromise national security, the Daily News reported.

This project has been funded with support from the European Commission.
This publication [communication] reflects the views only of the author, and the Commission cannot be held responsible for any use which may be made of the information contained therein.

"There's data on there that's highly sensitive," a police source told the newspaper, adding: "They're scrambling like mad."

Separately CNN, citing an unnamed U.S. Secret Service source, reported on Friday that a California man who scaled the White House fence last week was on the property's south grounds for at least 15 minutes before he was captured. (Reuters https://www.reuters.com/article/us-usa-trump-laptop/secret-service-says-laptop-stolen-from-agents-car-in-new-york-idUSKBN16O2EH Referred to 15.10.2019)

Learning objectives

U4LO1: The learner is able to observe, assess, prevent and report information risks in work place

U4LO2: The learner is able to utilise organisation's security systems in relation with information security

U4LO3: The learner is able to manage physical security in the premises

U4LO4: The learner is able to work safely in mobile and cloud services

U4LO5: The learner is able to ensure material and data storage and protection

U4LO6: The learner is able to apply basics of software safety: operating systems, applications

U5LO1: The learner is able to identify critical information from different media

U5LO2: The learner is able to assess the vulnerability of critical infrastructure for society

U5LO3: The learner is able to identify cyber-attacks and threats

Resources you can use

Some publications to help you get detailed information:

- National Cyber Security Centre Finland. Online publication (ISSN 1799-0157)
  Protection against Microsoft Office 365 credential phishing and data breaches

- Police university college.
  Cybercrime, Law and Technology in Finland and Beyond

This project has been funded with support from the European Commission.
This publication [communication] reflects the views only of the author, and the Commission cannot be held responsible for any use which may be made of the information contained therein.

- General Data Protection Regulation
  GPDR

Recommended process

In order to solve your challenge, you can work in a group of 2-4 persons. You can use following steps for your working:

1. Get familiar three given scenarios
2. Discuss with your group about the all three scenarios
3. Use provided publications for specific information. With other sources, remember source criticising.
4. Use your fictional or real company as a context in the scenarios
5. Estimate possibilities of the scenarios to be true at your fictional or real company
6. Make the necessary changes to prevent this from happening
7. Once you know what you need to do, describe how you will do it
8. Present the results (following teacher´s instructions).
9. Evaluate how you carried out the challenge

Evaluation criteria

- Shows an understanding of the CIA triad
- Clearly shows the impact of not meeting confidentiality agreements
- Provide example process/procedure, based upon best practice examples for managing important business data.
- Provide evidence, either real or simulated, that the designed process/procedure meets requirements of organisation.
- Suitable reflection/evaluation and improvement suggestions should be evident.

This project has been funded with support from the European Commission.
This publication [communication] reflects the views only of the author, and the Commission cannot be held responsible for any use which may be made of the information contained therein.

cyVETsecurity

Co-funded by the Erasmus+ Programme of the European Union

INFORMATION SECURITY MANAGEMENT AND REGULATIONS IN AN UNSAFE DIGITAL WORLD

Document for teachers

This project has been funded with support from the European Commission.
This publication [communication] reflects the views only of the author, and the Commission cannot be held responsible for any use which may be made of the information contained therein.

Duration of the challenge

48 hours / 6 days

Description of the situation

You have been promoted into a new role (DPO – Data Protection Officer), within your organisation. You will be responsible for overseeing the company's data protection strategy and its implementation to ensure compliance with appropriate data security requirements.

As part of this challenge, you will create or be issued with a suitable scenario to allow you to meet the learning objectives and evaluation criteria below.

Your challenge is to demonstrate your understanding and awareness of the cyber security regulations, common terminology, and the need for adequate procedures and processes.

As part of your preparation, consultation with your teacher is highly advised to ensure you have understood all the elements of this task.

Learning objectives

- **U3LO1**. The learner is able to understand the importance of information security and its significance for the organization
- **U3LO2**. The learner is able to identify basic laws, regulations and ethical principles of cybersecurity and information security instructions (for example GDPR and ISO 27 000 series)
- **U3LO3**. The learner is able to plan his / her own work based on work place information security instructions

This project has been funded with support from the European Commission.
This publication [communication] reflects the views only of the author, and the Commission cannot be held responsible for any use which may be made of the information contained therein.

- **U3LO4**. The learner is able to work applying tele / data communication security: confidentiality, integrity, availability
- **U3LO5**. The learner is able to implement staff safety training: security guidelines, control and monitoring

Minimum requirements to carry out the challenge		
Previous knowledge	**Equipment / software**	**Training resources**
IT Literate Basic awareness of GDPR. Basic understanding of the importance of business data. Awareness of contemporary laws and regulations regarding data security.	A suitable internet enabled device that will allow research and generation of evidence.	https://ec.europa.eu/digital-single-market/en/news/cybersecurity-act-strengthens-europes-cybersecurity https://docs.microsoft.com/en-us/previous-versions/windows/it-pro/windows-server-2012-r2-and-2012/hh831364(v%3Dws.11) https://www.certificationeurope.com/certification/cyber-essentials/ ISO27000 Series Links https://www.itgovernance.co.uk/iso27000-family https://www.iso.org/obp/ui/#iso:std:iso-iec:27000:ed-5:v1:en https://www.iso27001security.com/html/27000.html GDPR Links https://gdpr-info.eu/ https://en.wikipedia.org/wiki/General_Data_Protection_Regulation

This project has been funded with support from the European Commission.
This publication [communication] reflects the views only of the author, and the Commission cannot be held responsible for any use which may be made of the information contained therein.

		There are a very large body of resources available for this curriculum. Teachers should use all resources available to them. *These are the resources that have been issued to the students in the challenge.*

This project has been funded with support from the European Commission.
This publication [communication] reflects the views only of the author, and the Commission cannot be held responsible for any use which may be made of the information contained therein.

Schedule of the challenge

Suggested below are **notional** time allocations for the challenge:

- 4 hours to identify the parameters of the challenge (possibly including identifying who will carry out which task (s))
- 20 hours to look for information
- 12 hours to present proposals / collate findings and discuss them (within the student´s group)
- 3 hour to identify how findings will be presented (if not stipulated by teacher)
- 3 hours to prepare findings into appropriate format i.e. PowerPoint for presentation
- 2 hours to present / discuss findings
- 3 hour to evaluate / assess how you carried out the challenge and how you might make improvements for any future activities

This project has been funded with support from the European Commission.
This publication [communication] reflects the views only of the author, and the Commission cannot be held responsible for any use which may be made of the information contained therein.

Presentation of the results

The findings can be presented in whatever media the group decide upon. The findings must be in a form that can be retained following the challenge.

This could be a presentation of the findings, which may include but is not restricted to the following formats:

- Video
- Presentation using Software
- Oral \ verbal (This would need to be recorded)
- Written report
- Blog / vlog /wiki
- Any other suitable medium

Note: Teachers should decide the appropriate format for the students to present their results.

This project has been funded with support from the European Commission.
This publication [communication] reflects the views only of the author, and the Commission cannot be held responsible for any use which may be made of the information contained therein.

Evaluation criteria

The following *guidelines* are **suggestive** only and are provided as guidance to support the teacher.

Public presentation (10%)

A ***suggested*** evaluation table in ***Appendix A*** at the back of this document which contains criteria can be used to help the teacher assess public presentation skills

Teamwork performance (10%)

A **suggested** evaluation table in ***Appendix B*** at the back of this document contains criteria that can be used to help the teacher assess team working skills.

Findings from the challenge (80%). Possibly 10% per item (U3LO1 to U3LO5).

Marking Rubric

Area / Learning objectives	Evaluation Criteria	Expected
U3LO1 The learner is able to understand the importance of information security and its significance for the organization **Item 1**	The Learner clearly explains the organisations current security guidelines	This should be related to a fictional or real organisation. It should include the reference to salient data that requires to be protected/handled correctly The report/presentation or demonstration should emphasise the need to keep data secure, these

This project has been funded with support from the European Commission.
This publication [communication] reflects the views only of the author, and the Commission cannot be held responsible for any use which may be made of the information contained therein.

		should be supported with examples.
U3LO1 The learner is able to understand the importance of information security and its significance for the organization **Item 2**	The learner suggests improvements or identifies best practices to organisations guidelines	The submission should include the specifics relating to the data being processed, what the data is, as well as how important that data is
U3LO2 The learner is able to identify basic laws, regulations and ethical principles of cybersecurity and information security instructions (for example GDPR and ISO 27 000 series) **Item 3**	The Learner identifies the Core concepts, regulations and procedures of information security and cybersecurity	The report/presentation should include reference to salient laws/regulations/standards that relate/apply to the scenario presented. It may be tempting to simply state ISO 27000, however this is a range of standards, and it should be emphasised that they should provide reference to specific standards within this range.
U3LO2 The learner is able to identify basic laws, regulations and ethical	The Learner is able to apply regulations related to information security	The submission should include the submitters' thoughts on the ethical

This project has been funded with support from the European Commission.
This publication [communication] reflects the views only of the author, and the Commission cannot be held responsible for any use which may be made of the information contained therein.

principles of cybersecurity and information security instructions (for example GDPR and ISO 27 000) **Item 4**		implications when processing the data.
U3LO3 The learner is able to plan his / her own work based on work place information security instructions **Item 5**	The Learner applies information security instructions	When data is involved there will normally be a flow of the data (data journey), and this flow needs to provide guidance to the user of how the data integrity/protection should be carried out at each stage of the process. This area of the submission could utilise a flowchart to show this process. The flowchart could also show example timings, which would allow suitable planning to be done.
U3LO4. The learner is able to work applying tele / data communication security: confidentiality, integrity, availability	The Learner explains the meaning of confidentiality, integrity, and availability	The submission should identify and explain the CIA (Confidentiality, Integrity, Availability) triad, and how it relates to the scenario

This project has been funded with support from the European Commission.
This publication [communication] reflects the views only of the author, and the Commission cannot be held responsible for any use which may be made of the information contained therein.

Item 6		
U3LO4 The learner is able to work applying tele / data communication security: confidentiality, integrity, availability **Item 7**	The Learner explains the possible consequences of breaching confidentiality	The submission should extend their explanation of the CIA triad to include their understanding of the consequences if data confidentiality is breached. For example organisations would typically have SLA (Service Level Agreements) that can relate to the CIA
U3LO5 The learner is able to implement staff safety training: security guidelines, control and monitoring **Item 8**	The Learner prepares a short set of instructions on information security for an organization or a group of organisation's personnel	The submission should include suggestions on how the process/scenario chosen could be disseminated to employees, highlighting the importance of proper training to ensure consistency of use and their understanding of the impact if the data isn't processed properly and according to the guidelines being presented in this submission.

This project has been funded with support from the European Commission.
This publication [communication] reflects the views only of the author, and the Commission cannot be held responsible for any use which may be made of the information contained therein.

Co-funded by the Erasmus+ Programme of the European Union

Possible Student responses

NOTE: This suggested solution identifies generic examples for the evaluation criteria identified in the challenge. It has been drawn from many different sources, and is not intended to be a single cohesive piece of work. The bulleted points are intended to help the teacher identify areas that may be covered. The example provided is not exhaustive.

Fictional Scenario

You have been employed as a Data Protection Officer for a local business. Your prime role is to ensure the secure recording and storage of customer data that is being collected by your team.

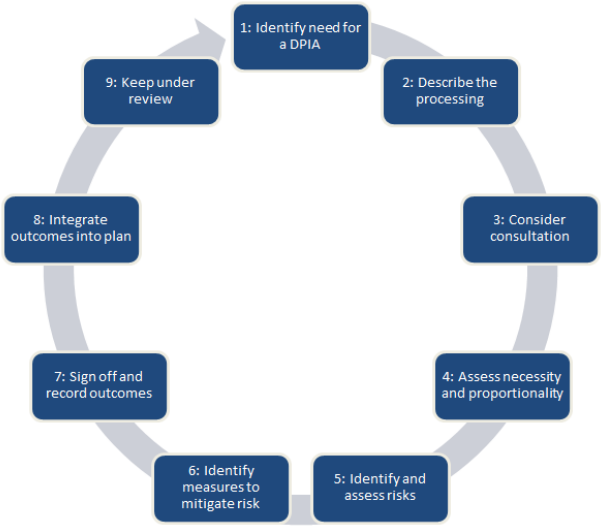
Item 1:

- Reference to the checking of the organisations' Privacy Policy, e.g. ensure stakeholders (anyone involved in the processing of data) are fully aware of how data is being processed, used and stored.

Item 2:

- Evaluate if the policies/procedures ensure confidentiality of user data, both stored, in process, and in transit (Encryption)
- Evaluate if the policies/procedures ensure integrity of data.
- Impact Assessment for example:-

This project has been funded with support from the European Commission.
This publication [communication] reflects the views only of the author, and the Commission cannot be held responsible for any use which may be made of the information contained therein.



https://ico.org.uk/for-organisations/guide-to-data-protection/guide-to-the-general-data-protection-regulation-gdpr/accountability-and-governance/data-protection-impact-assessments/

Item 3:

- Identify the relevant standards and guidelines that would be required when considering their scenario. E.g GDPR (Article 6: If the data subject has given consent to the processing of his or her personal data;), and ISO 27001 Information security management systems – requirements, ISO 27003 Information security management systems – Implementation guidance, ISO 27014 Information technology – security techniques – governance of information security
- If the data is stored in the cloud, ISO 27018 code of practice for protection of personally identifiable information (PII) in public clouds acting as PII processors.
- If data is to be stored, the ISO 27040 should apply
- Reference to cyber essentials scheme could also be used.

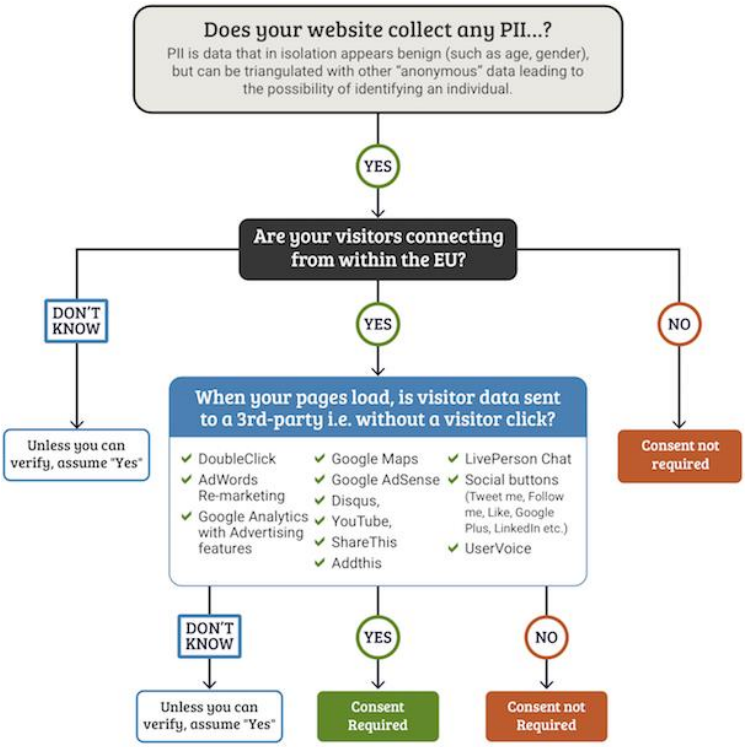
This project has been funded with support from the European Commission.
This publication [communication] reflects the views only of the author, and the Commission cannot be held responsible for any use which may be made of the information contained therein.

Item 4:

- As the scenario could relate to collecting, processing, and storing customer PII data, then the collection of the data should comply with GDPR (Article 6: If the data subject has given consent to the processing of his or her personal data;) and ISO 27001, while cloud based processing would be ISO 27018

Item 5:

- As DPO I/we are required to deploy customer data collection policy, based upon the previously identified guidelines. This will involve the creation of process documentation/flowchart information that will aid the training and understanding of multiple data stakeholders within the organization, an example process flow is shown below:-



Courtesy of: https://brianclifton.com/blog/2018/05/21/gdpr-request-consent-before-tracking/

This project has been funded with support from the European Commission.
This publication [communication] reflects the views only of the author, and the Commission cannot be held responsible for any use which may be made of the information contained therein.

Item 6:

- **Confidentiality**, **Integrity** and **Availability**, also known as the CIA triad, is a model designed to guide policies for information security within an organization. The elements of the triad are considered the three most crucial components of security.
- **Confidentiality** is roughly equivalent to privacy. Measures undertaken to ensure confidentiality are designed to prevent sensitive information from reaching the wrong people, while making sure that the right people can, in fact, get it:
- A good example of methods used to ensure confidentiality is an account number or routing number when banking online. Data encryption is a common method of ensuring confidentiality. User IDs and passwords constitute a standard procedure; two-factor authentication is becoming the norm.
- **Integrity** involves maintaining the consistency, accuracy, and trustworthiness of data over its entire life cycle. Data must not be changed in transit, and steps must be taken to ensure that data cannot be altered by unauthorized people (for example, in a breach of confidentiality)
- **Availability** is best ensured by rigorously maintaining all hardware, performing hardware repairs immediately when needed and maintaining a correctly functioning operating system environment that is free of software conflicts. Submissions could also explore the impact of SLAs.

Item 7:

Potential Impact of Data Breach

- Financial Costs (GDPR Fines)
- Reputational Damage
- Potential Litigation
- Civil or criminal convictions

This project has been funded with support from the European Commission.
This publication [communication] reflects the views only of the author, and the Commission cannot be held responsible for any use which may be made of the information contained therein.

- CEO/CIO/CSO Dismissal

Item 8:

The training guides, provided, could cover multiple aspects including GDPR, for example:-

- Introduction to GDPR
- Scope of GDPR
- What is personal data (PII) and special category data
- The six principles for the collection and processing of personal information
- Amendments to GDPR
- How the GDPR has been implemented across the EU
- Data controller vs data processor
- Data subject rights
- Collecting, requesting and processing personal data
- Breaches and other offences under GDPR and subsequent penalties

They could show their deeper understanding by providing a suitable flowchart/process diagram relating to the scenario chosen.

This project has been funded with support from the European Commission.
This publication [communication] reflects the views only of the author, and the Commission cannot be held responsible for any use which may be made of the information contained therein.

Appendix A

Criteria	Excellent	Very good	Good	Fair	Not Done	Comments/Suggestions:
Oral Introduction: Introduced speaker, captured audience attention	4	3	2	1	0	
Body of Speech: Easy to follow and understand, information seemed accurate and complete	4	3	2	1	0	
Summary: Brief, clear, and provided a wrap-up of the topic	4	3	2	1	0	
Performance: Speaker showed good inflection, proper pronunciation, used expression to demonstrate points, appeared conversational and natural, made eye contact with	4	3	2	1	0	

This project has been funded with support from the European Commission.
This publication [communication] reflects the views only of the author, and the Commission cannot be held responsible for any use which may be made of the information contained therein.

audience, and voice was loud and clear enough to hear; reliance on notecards was limited					
Participant's Knowledge: Participant was able to answer questions from the audience after repeating the question	4	3	2	1	0
Audience Attention: Held audience's attention for the duration	4	3	2	1	0
Sources: Sources were listed at the end of the speech	1	0	0	0	0

This project has been funded with support from the European Commission.
This publication [communication] reflects the views only of the author, and the Commission cannot be held responsible for any use which may be made of the information contained therein.

cyVETsecurity

Co-funded by the Erasmus+ Programme of the European Union

Appendix B Team working evaluation

Goals						
Goals are unclear or poorly understood, resulting in little commitment to them.	1	2	3	4	5	Goals are clear, understood, and have the full commitment of team members.
Openness						
Members are guarded or cautious in discussions.	1	2	3	4	5	Members express thoughts, feelings, and ideas freely.
Mutual Trust						
Members are suspicious of one another's motives.	1	2	3	4	5	Members trust one another and do not fear ridicule or reprisal.
Attitudes Toward Difference						
Members smooth over differences and suppress or avoid conflict.	1	2	3	4	5	Members feel free to voice differences and work through them.

This project has been funded with support from the European Commission.
This publication [communication] reflects the views only of the author, and the Commission cannot be held responsible for any use which may be made of the information contained therein.

Support						
Members are reluctant to ask for or give help.	1	2	3	4	5	Members are comfortable giving and receiving help.
Participation						
Discussion is generally dominated by a few members.	1	2	3	4	5	All members are involved in discussion.
Decision-making						
Decisions are made by only a few members.	1	2	3	4	5	All members are involved in decision-making.
Flexibility						

This project has been funded with support from the European Commission.
This publication [communication] reflects the views only of the author, and the Commission cannot be held responsible for any use which may be made of the information contained therein.

The group is locked into established rules and procedures that members find difficult to change.	1	2	3	4	5	Members readily change procedures in response to new situations.
Use of Member Resources						
Individuals' abilities, knowledge and experience is not well utilized.	1	2	3	4	5	Each member's abilities, knowledge, and experience are fully utilized.

This project has been funded with support from the European Commission.
This publication [communication] reflects the views only of the author, and the Commission cannot be held responsible for any use which may be made of the information contained therein.

cyVETsecurity

Co-funded by the Erasmus+ Programme of the European Union

INFORMATION SECURITY MANAGEMENT AND REGULATIONS IN AN UNSAFE DIGITAL WORLD

Document for students

This project has been funded with support from the European Commission.
This publication [communication] reflects the views only of the author, and the Commission cannot be held responsible for any use which may be made of the information contained therein.

cyVETsecurity

Co-funded by the Erasmus+ Programme of the European Union

Duration of the challenge

Notionally 48 hours / 6 days

Your team

Student / teacher should allocate the following:

Team name:

Team member names:

Description of the situation

You have been promoted into a new role (DPO – Data Protection Officer), within your organisation. You will be responsible for overseeing the company's data protection strategy and its implementation to ensure compliance with appropriate data security requirements.

As part of this challenge, you will create or be issued with a suitable scenario to allow you to meet the learning objectives and evaluation criteria below.

Your challenge is to demonstrate your understanding and awareness of the cyber security regulations, common terminology, and the need for adequate procedures and processes.

As part of your preparation, consultation with your teacher is highly advised to ensure you have understood all the elements of this task.

This project has been funded with support from the European Commission.
This publication [communication] reflects the views only of the author, and the Commission cannot be held responsible for any use which may be made of the information contained therein.

Learning objectives

- **U3LO1**. The learner is able to understand the importance of information security and its significance for the organization
- **U3LO2**. The learner is able to identify basic laws, regulations and ethical principles of cybersecurity and information security instructions (for example GDPR and ISO 27 000 series)
- **U3LO3**. The learner is able to plan his / her own work based on work place information security instructions
- **U3LO4**. The learner is able to work applying tele / data communication security: confidentiality, integrity, availability
- **U3LO5**. The learner is able to implement staff safety training: security guidelines, control and monitoring

Resources you can use

Some general resources to help you get started:

https://ec.europa.eu/digital-single-market/en/news/cybersecurity-act-strengthens-europes-cybersecurity

https://docs.microsoft.com/en-us/previous-versions/windows/it-pro/windows-server-2012-r2-and-2012/hh831364(v%3Dws.11)

https://www.certificationeurope.com/certification/cyber-essentials/

ISO27000 Series Links

https://www.itgovernance.co.uk/iso27000-family

https://www.iso.org/obp/ui/#iso:std:iso-iec:27000:ed-5:v1:en

https://www.iso27001security.com/html/27000.html

GDPR Links

https://gdpr-info.eu/

https://en.wikipedia.org/wiki/General_Data_Protection_Regulation

Recommended process

This project has been funded with support from the European Commission.
This publication [communication] reflects the views only of the author, and the Commission cannot be held responsible for any use which may be made of the information contained therein.

In order to solve your challenge, you need to work in an organised way. We suggest you follow these steps:

1. Establish the parameters you need to solve the challenge. For example, in this case these could be: recognised industry regulations/laws/guidelines that impact your chosen organisation.
2. Look for information related to those parameters (see resources proposed, but it is suggested you use others)
3. Select which information is important to solve the challenge.
4. Come up with different proposals to solve the challenge.
5. Select the proposal/proposals which are more effective from your group´s point of view.
6. Plan which actions you need to solve the challenge (once you know what you need to do, describe how you will do it).
7. Implement the actions.
8. Present the results (following teacher´s instructions).
9. Evaluate how you carried out the challenge

Evaluation criteria

- Clearly explain the organisations current security guidelines
- Suggest improvements or identify best practices to organisations' guidelines
- Identify the Core concepts, regulations and procedures of information security and cybersecurity
- Apply regulations related to information security
- Apply information security instructions
- Explain the meaning of confidentiality, integrity, and availability
- Explain the possible consequences of breaching confidentiality
- Prepare a short set of instructions on information security for an organization or a group of organisation's personnel

This project has been funded with support from the European Commission.
This publication [communication] reflects the views only of the author, and the Commission cannot be held responsible for any use which may be made of the information contained therein.

cyVETsecurity

Co-funded by the Erasmus+ Programme of the European Union

Basic knowledge of the relation between IT & OT

Document for teachers

This project has been funded with support from the European Commission.
This publication [communication] reflects the views only of the author, and the Commission cannot be held responsible for any use which may be made of the information contained therein.

cyVETsecurity

Co-funded by the Erasmus+ Programme of the European Union

Duration of the challenge

24 hours / 3 days

Description of the situation

For the company where you work, a device is placed with control via a microcontroller. The company has various locations in the Netherlands and abroad.
The control must also be possible via a different location. To achieve this, a connection must be made over the internet. To understand how the device is connected, a virtual setup must be made via Packet Tracer.
If you have made the correct configuration, a secure connection must be made via a VPN.

To complete this assignment you will have to investigate:
- Functions of Packet Tracer
- the GUI settings of a wifi router (WRT300N),
- Port forwarding
- VPN

A document must be delivered with the details of Packet Tracer with the description of the settings. The document must also contain a description of at least 3 threats that you may encounter. In the research into security standards you answer the following questions:
Select 3 standards from the following list and give a short description in your own words:
- IEC 62443 / ISA99,
- NIST 800 82,
- NIST 800 53,
- NERC CIP,
- CyberEssentials,
- NISTIR7228

Select 3 protocols from the following list and give a short description in your own words:
- PLC,
- SCADA,
- HMI,
- MES,
- MODBUS,
- PROFINET

This project has been funded with support from the European Commission.
This publication [communication] reflects the views only of the author, and the Commission cannot be held responsible for any use which may be made of the information contained therein.

Give two examples of a Firewall that can be used for industrial use.

Learning objectives

U6LO1. The learner is able to differentiate IT versus OT

U6LO2. The learner is able to understand basic knowledge of networking (cisco,hp)

U6LO3. The learner is able to identify the main threats and effects of a cyber attack in an industrial environment.

U6LO4. The learner is able to describe the main Information Security Standards in IT

U6LO5. The learner identifies the main security standards related to OT

U6LO6. The learner is able to identify some security measures in industrial processes

U6LO7. The learner is able to identify which are the main components and common protocols in OT

Minimum requirements to carry out the challenge

Previous knowledge	Equipment/software	Training resources
Is able to work with laptop, PC and smartphone.	An internet connected device, such as: PC Laptop Smartphone	• https://www.youtube.com/channel/UCCMyf3_4h3zw7DSNW2d0SKg • https://en.wikipedia.org/wiki/Operational_Technology • https://en.wikipedia.org/wiki/Cyber_security_standards

This project has been funded with support from the European Commission.
This publication [communication] reflects the views only of the author, and the Commission cannot be held responsible for any use which may be made of the information contained therein.

Is familiar with network/internet. Has understanding of microcontroller.	Software: Packet Tracer Office	• https://automation.isa.org/industrial-firewall-cybersecurity-threats-vulnerabilities-risks-security/ • https://en.wikipedia.org/wiki/IP_address • https://www.youtube.com/watch?v=-K6jMYBfuIY • Explain the challenge and what is expected. • The teacher should build the network challenge together with te students so they can follow and get an understanding of the software. • Leave the port forwarding configuration open so the students can do this alone. • Guide the student though the VPN challenge in Paket tracer, explain what the steps are and how you set it up. *There are a very large body of resources available for this curriculum. Teachers should use all resources available to them.* *These are the resources that have been issued to the students in the challenge.*

This project has been funded with support from the European Commission.
This publication [communication] reflects the views only of the author, and the Commission cannot be held responsible for any use which may be made of the information contained therein.

cyVETsecurity

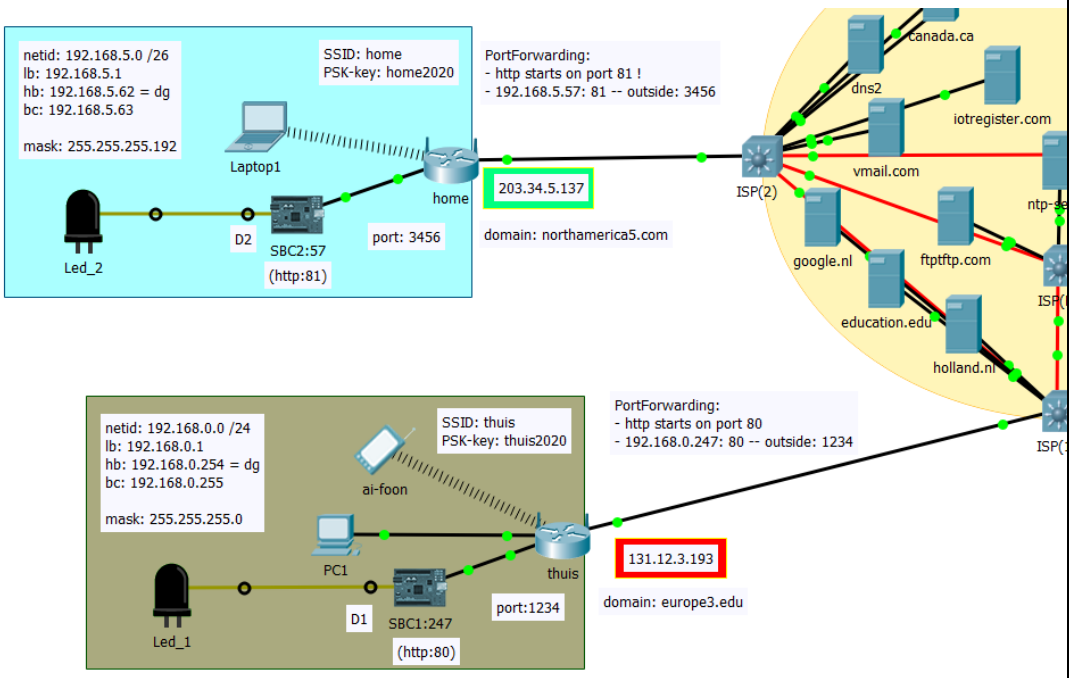
Co-funded by the Erasmus+ Programme of the European Union

Schedule of the challenge

Suggested below are notional time allocations for the challenge:

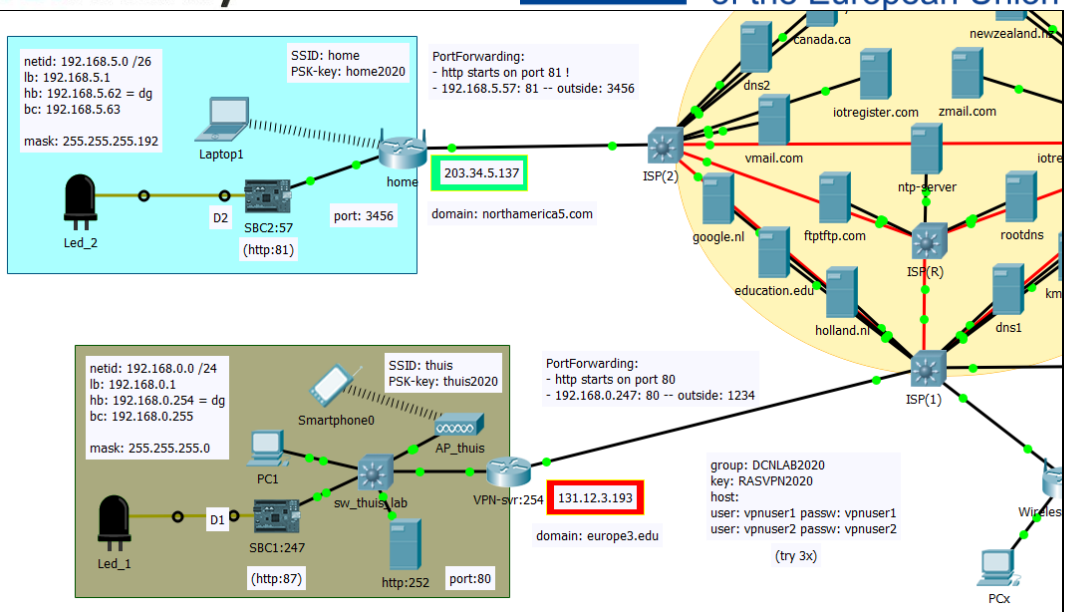
1 hour to explain the challenge

3 hours to teach Packet tracer part of portforwarding as the example:



3 hours teaching VPN in packet tracer :

This project has been funded with support from the European Commission.
This publication [communication] reflects the views only of the author, and the Commission cannot be held responsible for any use which may be made of the information contained therein.



3 hours tinkering and configuring for students with Packet tracer

10 hours writing the assignment with research

2 hours checking the outcome of the challenge

1 hour team discussion

1 hour to make final adjustments and to present to teacher

This project has been funded with support from the European Commission.
This publication [communication] reflects the views only of the author, and the Commission cannot be held responsible for any use which may be made of the information contained therein.

cyVETsecurity

Co-funded by the Erasmus+ Programme of the European Union

Presentation of the results

The students deliver their challenge to the teacher. Teacher will evaluate their product and can ask some questions to check what the student learned.

As the students work together, they must deliver their own product.

The products that must be delivered are:

- Packet tracer document
- Explanation of subject of the challenge in a written report
- verbal substantiation of the teachers questions

This project has been funded with support from the European Commission.
This publication [communication] reflects the views only of the author, and the Commission cannot be held responsible for any use which may be made of the information contained therein.

Evaluation criteria

The following *guidelines* are **suggestive** only and are provided as guidance to support the teacher.

Teamwork performance (10%)

A **suggested** evaluation table in ***Appendix A*** at the back of this document contains criteria that can be used to help the teacher assess team working skills

Challenges:

Network configuration (20%)

The document must also contain a description of at least 3 threats that you may encounter. (20%)

Three security standards. (20%)

Three protocols (20%)

Two examples of Firewall (10%)

Teachers are free to determine their own graduation.

This project has been funded with support from the European Commission.
This publication [communication] reflects the views only of the author, and the Commission cannot be held responsible for any use which may be made of the information contained therein.

cyVETsecurity

Co-funded by the Erasmus+ Programme of the European Union

Appendix A

Goals						
Goals are unclear or poorly understood, resulting in little commitment to them.	1	2	3	4	5	Goals are clear, understood, and have the full commitment of team members.
Openness						
Members are guarded or cautious in discussions.	1	2	3	4	5	Members express thoughts, feelings, and ideas freely.
Mutual Trust						
Members are suspicious of one another's motives.	1	2	3	4	5	Members trust one another and do not fear ridicule or reprisal.
Attitudes Toward Difference						

This project has been funded with support from the European Commission.
This publication [communication] reflects the views only of the author, and the Commission cannot be held responsible for any use which may be made of the information contained therein.

Members smooth over differences and suppress or avoid conflict.	1	2	3	4	5	Members feel free to voice differences and work through them.
Support						
Members are reluctant to ask for or give help.	1	2	3	4	5	Members are comfortable giving and receiving help.
Participation						
Discussion is generally dominated by a few members.	1	2	3	4	5	All members are involved in discussion.
Decision-making						
Decisions are made by only a few members.	1	2	3	4	5	All members are involved in decision-making.
Flexibility						

This project has been funded with support from the European Commission.
This publication [communication] reflects the views only of the author, and the Commission cannot be held responsible for any use which may be made of the information contained therein.

The group is locked into established rules and procedures that members find difficult to change.	1	2	3	4	5	Members readily change procedures in response to new situations.
Use of Member Resources						
Individuals' abilities, knowledge and experience is not well utilized.	1	2	3	4	5	Each member's abilities, knowledge, and experience are fully utilized.

This project has been funded with support from the European Commission.
This publication [communication] reflects the views only of the author, and the Commission cannot be held responsible for any use which may be made of the information contained therein.

cyVETsecurity

Co-funded by the Erasmus+ Programme of the European Union

Basic knowledge of the relation between IT & OT

Document for students

This project has been funded with support from the European Commission.
This publication [communication] reflects the views only of the author, and the Commission cannot be held responsible for any use which may be made of the information contained therein.

cyVETsecurity

Co-funded by the Erasmus+ Programme of the European Union

Duration of the challenge

24 hours / 3 days

Your team

Student / teacher should allocate the following:

Team name:

Team member names:

Description of the situation

For the company where you work, a device is placed with control via a microcontroller. The company has various locations in the Netherlands and abroad.
The control must also be possible via a different location. To achieve this, a connection must be made over the internet. To understand how the device is connected, a virtual setup must be made via Packet Tracer.
If you have made the correct configuration, a secure connection must be made via a VPN.

To complete this assignment you will have to investigate:
- Functions of Packet Tracer
- the GUI settings of a wifi router (WRT300N),
- Port forwarding
- VPN

A document must be delivered with the details of Packet Tracer with the description of the settings.

The document must also contain a description of at least 3 threats that you may encounter.

In the research into security standards you answer the following questions:
Select 3 standards from the following list and give a short description in your own words:
- IEC 62443 / ISA99,
- NIST 800 82,

This project has been funded with support from the European Commission.
This publication [communication] reflects the views only of the author, and the Commission cannot be held responsible for any use which may be made of the information contained therein.

- NIST 800 53,
- NERC CIP,
- CyberEssentials,
- NISTIR7228

Select 3 protocols from the following list and give a short description in your own words:

- PLC,
- SCADA,
- HMI,
- MES,
- MODBUS,
- PROFINET

Give two examples of a Firewall that can be used for industrial use.

Learning objectives

U6LO1. The learner is able to differentiate IT versus OT

U6LO2. The learner is able to understand basic knowledge of networking (cisco,hp)

U6LO3. The learner is able to identify the main threats and effects of a cyber attack in an industrial environment.

U6LO4. The learner is able to describe the main Information Security Standards in IT

U6LO5. The learner identifies the main security standards related to OT

U6LO6. The learner is able to identify some security measures in industrial processes

U6LO7. The learner is able to identify which are the main components and common protocols in OT

This project has been funded with support from the European Commission.
This publication [communication] reflects the views only of the author, and the Commission cannot be held responsible for any use which may be made of the information contained therein.

Resources you can use

Some general resources to help you get started:

- https://www.youtube.com/channel/UCCMyf3_4h3zw7DSNW2d0SKg
- https://en.wikipedia.org/wiki/Operational_Technology
- https://en.wikipedia.org/wiki/Cyber_security_standards
- https://automation.isa.org/industrial-firewall-cybersecurity-threats-vulnerabilities-risks-security/
- https://en.wikipedia.org/wiki/IP_address
- https://www.youtube.com/watch?v=-K6jMYBfuIY

Recommended process

In order to solve your challenge, you need to work in an organised way. We suggest you follow these steps:

1. Define the questions and activities from the challenge description
2. Look for information related to those parameters (see resources proposed, but it is suggested you use others)
3. Select which information is important to solve the challenge.
4. Write your answers and explanations in your own words.
5. You work in groups but write your own paper.
6. Share your research with each other
7. Implement the actions.
8. Present the results (following teacher´s instructions).
9. Evaluate how you carried out the challenge

This project has been funded with support from the European Commission.
This publication [communication] reflects the views only of the author, and the Commission cannot be held responsible for any use which may be made of the information contained therein.

Evaluation criteria

- Check if all Learning objectives are covered
- Check if you can explain what you did in the challenge
- The virtual network with Packet tracer works

This project has been funded with support from the European Commission.
This publication [communication] reflects the views only of the author, and the Commission cannot be held responsible for any use which may be made of the information contained therein.

cyVETsecurity

Co-funded by the Erasmus+ Programme of the European Union

Company procedures and machines

Document for teachers

This project has been funded with support from the European Commission.
This publication [communication] reflects the views only of the author, and the Commission cannot be held responsible for any use which may be made of the information contained therein.

cyVETsecurity

Co-funded by the Erasmus+ Programme of the European Union

Duration of the challenge

19 hours

Description of the situation

You work in a company or your profession. You can simulate this as your practical class as your work area.

There are a number of security levels within the company to chart the degree of security.
Study IEC 62443 and think of an example for each level for your company.

There are rules and regulations within the school / company if there should be a security breach. Read the procedures of the school / company and write down the procedure if there should be a virus in a machine software

Give three examples of a breach in the security of a machine. Make a description of this so that non-technical staff understands what it is about.

The teacher provides the student with a network monitoring tool and discusses this with the student. Explain about the program and what is visible.
The teacher shows abnormalities and the student gives an explanation about this and sets up an email to the IT specialist to indicate what he has seen.

The student makes a network drawing with router, switch pc and machine. He describes how the machine can be accessed and what the different devices do. The explanation must be written in simple language.

You must deliver a written document and a film of max. 10 minutes to explain the parts of the challenge.

Learning objectives

U7LO1. The learner is able to name and describe the levels in the industrial process.

This project has been funded with support from the European Commission.
This publication [communication] reflects the views only of the author, and the Commission cannot be held responsible for any use which may be made of the information contained therein.

U7LO2. The learner is able to apply company procedures, detecting possible problems and informing a specialist about any security issues.

U7LO3. The learner is able to detect malfunction in the machine or breaches in the machine security.

U7LO4. The learner is able to identify the risks of plugging in random USB in a company network/machines/computers

U7LO5. The learner is able to read out a network monitoring tool to detect unusual network traffic.

U7LO6. The learner is able to understand networking protocols routing/vpn/PF/etc..

Minimum requirements to carry out the challenge

Previous knowledge	Equipment/software	Training resources
Is able to work with laptop, PC and smartphone. Is familiar with network/internet. Has understanding and working of	An internet connected device, such as: PC Laptop Smartphone Software: Packet Tracer Office Network monitoring tool School IT security protocol	• https://en.wikipedia.org/wiki/Cyber_security_standards • https://en.wikipedia.org/wiki/Computer_network • https://www.cnczone.com/forums/uncategorised-cam-discussion/1448-cnc.html • Explain the challenge and what is expected. • The teacher makes a choise witch network monitoring tool the student need to use and provide the explanation of the tool.

This project has been funded with support from the European Commission.
This publication [communication] reflects the views only of the author, and the Commission cannot be held responsible for any use which may be made of the information contained therein.

machines (automated)		*There are a very large body of resources available for this curriculum. Teachers should use all resources available to them. These are the resources that have been issued to the students in the challenge.*

This project has been funded with support from the European Commission.
This publication [communication] reflects the views only of the author, and the Commission cannot be held responsible for any use which may be made of the information contained therein.

cyVETsecurity

Co-funded by the Erasmus+ Programme of the European Union

Schedule of the challenge

Suggested below are notional time allocations for the challenge:

1 hour to explain the challenge

4 hours to teach the network monitoring tool

10 hours for research and writing the document

1 hour team discussion

1 hour to make final adjustments

2 hours to make the film and present the film

This project has been funded with support from the European Commission.
This publication [communication] reflects the views only of the author, and the Commission cannot be held responsible for any use which may be made of the information contained therein.

cyVETsecurity

Co-funded by the Erasmus+ Programme of the European Union

Presentation of the results

The students deliver their challenge to the teacher. Teacher will evaluate their product.

The film that the student make is freely interpretable and students can choose any form. (Action, comedy etc.) The students can use their smartphone.

As the students work together, they must deliver their own product.

This project has been funded with support from the European Commission.
This publication [communication] reflects the views only of the author, and the Commission cannot be held responsible for any use which may be made of the information contained therein.

Evaluation criteria

The following *guidelines* are **suggestive** only and are provided as guidance to support the teacher.

Teamwork performance (10%)

A **suggested** evaluation table in ***Appendix A*** at the back of this document contains criteria that can be used to help the teacher assess team working skills

Challenges:

Security level (10%)

Rules and regulations (10%)

Three security breaches. (20%)

Network monitoring (20%)

Network explanation (10%)

Film (20%)

Teachers are free to determine their own graduation.

This project has been funded with support from the European Commission.
This publication [communication] reflects the views only of the author, and the Commission cannot be held responsible for any use which may be made of the information contained therein.

Appendix A

Goals						
Goals are unclear or poorly understood, resulting in little commitment to them.	1	2	3	4	5	Goals are clear, understood, and have the full commitment of team members.
Openness						
Members are guarded or cautious in discussions.	1	2	3	4	5	Members express thoughts, feelings, and ideas freely.
Mutual Trust						
Members are suspicious of one another's motives.	1	2	3	4	5	Members trust one another and do not fear ridicule or reprisal.
Attitudes Toward Difference						

This project has been funded with support from the European Commission.
This publication [communication] reflects the views only of the author, and the Commission cannot be held responsible for any use which may be made of the information contained therein.

Members smooth over differences and suppress or avoid conflict.	1	2	3	4	5	Members feel free to voice differences and work through them.
Support						
Members are reluctant to ask for or give help.	1	2	3	4	5	Members are comfortable giving and receiving help.
Participation						
Discussion is generally dominated by a few members.	1	2	3	4	5	All members are involved in discussion.
Decision-making						
Decisions are made by only a few members.	1	2	3	4	5	All members are involved in decision-making.
Flexibility						

This project has been funded with support from the European Commission.
This publication [communication] reflects the views only of the author, and the Commission cannot be held responsible for any use which may be made of the information contained therein.

The group is locked into established rules and procedures that members find difficult to change.	1	2	3	4	5	Members readily change procedures in response to new situations.
Use of Member Resources						
Individuals' abilities, knowledge and experience is not well utilized.	1	2	3	4	5	Each member's abilities, knowledge, and experience are fully utilized.

This project has been funded with support from the European Commission.
This publication [communication] reflects the views only of the author, and the Commission cannot be held responsible for any use which may be made of the information contained therein.

cyVETsecurity

Co-funded by the Erasmus+ Programme of the European Union

Company procedures and machines

Document for students

This project has been funded with support from the European Commission.
This publication [communication] reflects the views only of the author, and the Commission cannot be held responsible for any use which may be made of the information contained therein.

cyVETsecurity

Co-funded by the Erasmus+ Programme of the European Union

Duration of the challenge

19 hours

Your team

Student / teacher should allocate the following:

Team name:

Team member names:

Description of the situation

You work in a company or your profession. You can simulate this as your practical class as your work area.

There are a number of security levels within the company to chart the degree of security.
Study IEC 62443 and think of an example for each level for your company.

There are rules and regulations within the school / company if there should be a security breach. Read the procedures of the school / company and write down the procedure if there should be a virus in a machine software

Give three examples of a breach in the security of a machine. Make a description of this so that non-technical staff understands what it is about.

The teacher provides the student with a network monitoring tool and discusses this with the student. Explain about the program and what is visible.
The teacher shows abnormalities and the student gives an explanation about this and sets up an email to the IT specialist to indicate what he has seen.

The student makes a network drawing with router, switch pc and machine. He describes how the machine can be accessed and what the different devices do. The explanation must be written in simple language.

This project has been funded with support from the European Commission.
This publication [communication] reflects the views only of the author, and the Commission cannot be held responsible for any use which may be made of the information contained therein.

You must deliver a written document and a film of max. 10 minutes to explain the parts of the challenge.

Learning objectives

U7LO1. The learner is able to name and describe the levels in the industrial process.

U7LO2. The learner is able to apply company procedures, detecting possible problems and informing a specialist about any security issues.

U7LO3. The learner is able to detect malfunction in the machine or breaches in the machine security.

U7LO4. The learner is able to identify the risks of plugging in random USB in a company network/machines/computers

U7LO5. The learner is able to read out a network monitoring tool to detect unusual network traffic.

U7LO6. The learner is able to understand networking protocols routing/vpn/PF/etc..

Resources you can use

Some general resources to help you get started:

- https://en.wikipedia.org/wiki/Cyber_security_standards
- https://en.wikipedia.org/wiki/Computer_network
- https://www.cnczone.com/forums/uncategorised-cam-discussion/1448-cnc.html

Recommended process

In order to solve your challenge, you need to work in an organised way. We suggest you follow these steps:

1. Define the questions and activities from the challenge description

This project has been funded with support from the European Commission.
This publication [communication] reflects the views only of the author, and the Commission cannot be held responsible for any use which may be made of the information contained therein.

2. Look for information related to those parameters (see resources proposed, but it is suggested you use others)
3. Select which information is important to solve the challenge.
4. Write your answers and explanations in your own words.
5. You work in groups but write your own paper.
6. Share your research with each other
7. Implement the actions.
8. Present the results (following teacher´s instructions).
9. Evaluate how you carried out the challenge

Evaluation criteria

- Check if all Learning objectives are covered
- Check if you can explain what you did in the challenge
- Present the film
- The teacher will explain his/her graduation

This project has been funded with support from the European Commission.
This publication [communication] reflects the views only of the author, and the Commission cannot be held responsible for any use which may be made of the information contained therein.

cyVETsecurity

Co-funded by the Erasmus+ Programme of the European Union

GDPR and data protection

Document for teachers

This project has been funded with support from the European Commission.
This publication [communication] reflects the views only of the author, and the Commission cannot be held responsible for any use which may be made of the information contained therein.

cyVETsecurity

Co-funded by the Erasmus+ Programme of the European Union

Duration of the challenge

10 hours

Description of the situation

Investigate GDPR of your country and answer the following questions:

Where can you find the official GDPR guidelines?

What are the most relevant guidelines for OT cyber security? (name 3)

What is the difference between GDPR of your own country and two other European country's?

What does your school do with GDPR in your profession?

What is your own advise of protection of a computer guided machine?

Take a computer guided machine and investigate what information is sensitive?

What are the dangers of a computer guided machine?

Make a presentation of max 15 minutes to present the answers of these questions.

This project has been funded with support from the European Commission.
This publication [communication] reflects the views only of the author, and the Commission cannot be held responsible for any use which may be made of the information contained therein.

Learning objectives

U8LO1. The learner is able to identify which are the data protection regulations in his/her country and in Europe.

U8LO2. The learner is able to work in a secure way with data connected to the different kind of machines used at work.

Minimum requirements to carry out the challenge

Previous knowledge	Equipment/software	Training resources
Is able to work with laptop, PC and smartphone. Is familiar with network/internet. Has understanding and working of machines (automated)	An internet connected device, such as: PC Laptop Smartphone Software: Office	• https://gdpr-info.eu/ • https://companyweek.com/articles/cybersecurity-for-manufacturers-staying-in-control-of-cnc-machines • https://www.researchgate.net/publication/313915539_Detecting_cyber-physical_attacks_in_CyberManufacturing_systems_with_machine_learning_methods • https://ec.europa.eu/info/law/law-topic/data-protection/ *There are a very large body of resources available for this curriculum. Teachers should use all resources available to them.* *These are the resources that have been issued to the students in the challenge.*

This project has been funded with support from the European Commission.
This publication [communication] reflects the views only of the author, and the Commission cannot be held responsible for any use which may be made of the information contained therein.

cyVETsecurity

Co-funded by the Erasmus+ Programme of the European Union

Schedule of the challenge

Suggested below are notional time allocations for the challenge:

1 hour to explain the challenge

8 hours research an answering the questions

1 hours to make the presentation

Presentation of the results

The students deliver their presentation to the teacher and present to the class.

Teacher will evaluate their product.

Students work alone.

This project has been funded with support from the European Commission.
This publication [communication] reflects the views only of the author, and the Commission cannot be held responsible for any use which may be made of the information contained therein.

Evaluation criteria

The following *guidelines* are **suggestive** only and are provided as guidance to support the teacher.

Challenges:

Where can you find the official GDPR guidelines? (10%)

What are the most relevant guidelines for OT cyber security? (name 3) (15%)

What is the difference between GDPR of your own country and two other European country's? (10%)

What does your school do with GDPR in your profession? (10%)

What is your own advice of protection of a computer guided machine? (10%)

Take a computer guided machine and investigate what information is sensitive? (15%)

What are the dangers of a computer guided machine? (10%)

Presentation (20%)

In ***Appendix A*** an example of an assessment form for presentations.

Teachers are free to determine their own graduation.

This project has been funded with support from the European Commission.
This publication [communication] reflects the views only of the author, and the Commission cannot be held responsible for any use which may be made of the information contained therein.

cyVETsecurity

Co-funded by the Erasmus+ Programme of the European Union

Appendix A

Assessment form Oral Presentations

Student name:
Grade:

	O.	Comments
Content Clearly Consistent Coordination with target group Quality Main and side issues		
Form Introduction, center, lock Transitions Logical structure Balanced Timetable		
Verbal presentation Word choice and sentence structure Tempo Intelligibility Intonation Variety		
Non-verbal expression Attitude Facial expression Supporting gestures Contact with the public		

This project has been funded with support from the European Commission.
This publication [communication] reflects the views only of the author, and the Commission cannot be held responsible for any use which may be made of the information contained therein.

Tools Clear, well-arranged Supportive Integrated in argument Dosage, timing Service		

In the second column the judgment is summarized in ++, +, ± or -; in the third column explained this judgment.

This project has been funded with support from the European Commission.
This publication [communication] reflects the views only of the author, and the Commission cannot be held responsible for any use which may be made of the information contained therein.

cyVETsecurity

Co-funded by the Erasmus+ Programme of the European Union

GDPR and data protection

Document for students

This project has been funded with support from the European Commission.
This publication [communication] reflects the views only of the author, and the Commission cannot be held responsible for any use which may be made of the information contained therein.

cyVETsecurity

Co-funded by the Erasmus+ Programme of the European Union

Duration of the challenge

10 hours

Your team

Student / teacher should allocate the following:

Team name:

Description of the situation

Investigate GDPR of your country and answer the following questions:

Where can you find the official GDPR guidelines?

What are the most relevant guidelines for OT cyber security? (name 3)

What is the difference between GDPR of your own country and two other European country's?

What does your school do with GDPR in your profession?

What is your own advice of protection of a computer guided machine?

Take a computer guided machine and investigate what information is sensitive?

What are the dangers of a computer guided machine?

Make a presentation of max 15 minutes to present the answers of these questions.

This project has been funded with support from the European Commission.
This publication [communication] reflects the views only of the author, and the Commission cannot be held responsible for any use which may be made of the information contained therein.

Learning objectives

U8LO1. The learner is able to identify which are the data protection regulations in his/her country and in Europe.

U8LO2. The learner is able to work in a secure way with data connected to the different kind of machines used at work.

Resources you can use

Some general resources to help you get started:

- https://gdpr-info.eu/
- https://companyweek.com/articles/cybersecurity-for-manufacturers-staying-in-control-of-cnc-machines
- https://www.researchgate.net/publication/313915539_Detecting_cyber-physical_attacks_in_CyberManufacturing_systems_with_machine_learning_methods
- https://ec.europa.eu/info/law/law-topic/data-protection/

Recommended process

In order to solve your challenge, you need to work in an organised way. We suggest you follow these steps:

1. Define the questions and activities from the challenge description
2. Look for information related to those parameters (see resources proposed, but it is suggested you use others)
3. Select which information is important to solve the challenge.
4. Write your answers and explanations in your own words.
5. Present the results (following teacher´s instructions).
6. Evaluate how you carried out the challenge

This project has been funded with support from the European Commission.
This publication [communication] reflects the views only of the author, and the Commission cannot be held responsible for any use which may be made of the information contained therein.

Evaluation criteria

- Check if all Learning objectives are covered
- Check if you can explain what you did in the challenge
- Make a presentation.
- The teacher will explain his/her graduation

This project has been funded with support from the European Commission.
This publication [communication] reflects the views only of the author, and the Commission cannot be held responsible for any use which may be made of the information contained therein.

cyVETsecurity

Co-funded by the Erasmus+ Programme of the European Union

IT/OT environment

Document for teachers

This project has been funded with support from the European Commission.
This publication [communication] reflects the views only of the author, and the Commission cannot be held responsible for any use which may be made of the information contained therein.

Duration of the challenge

24 hours / 3 days

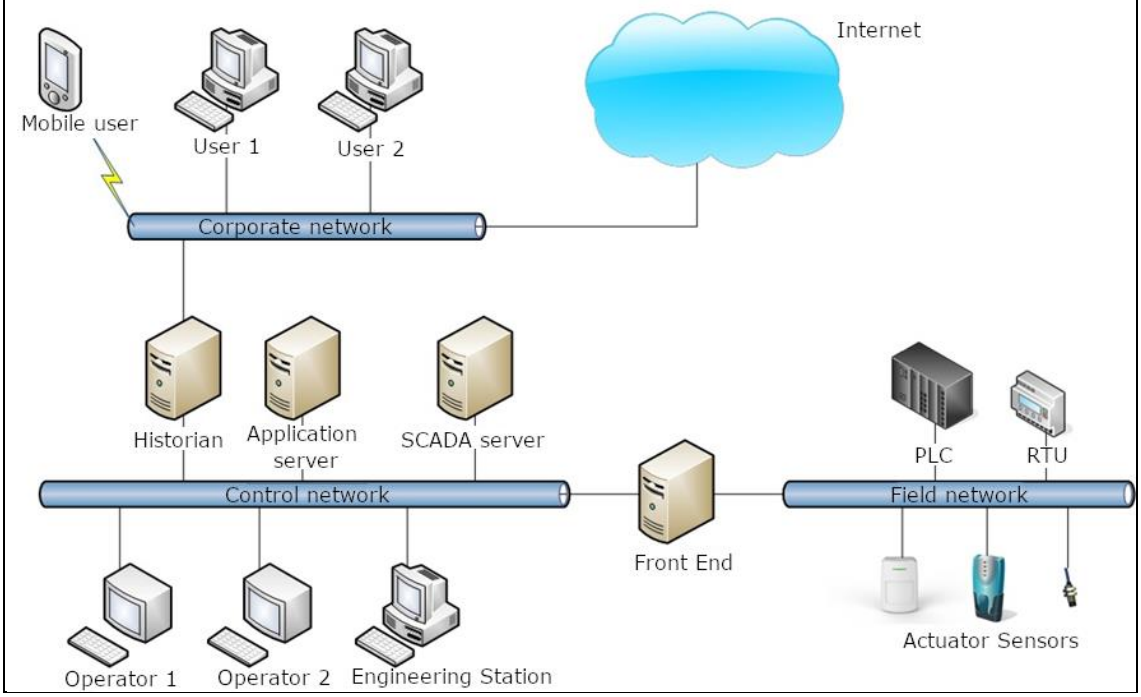
Description of the situation

A factory automation company asks for advice on the safety of its production plant.

The company has its IT and OT departments, but they don't know how to jointly manage the complete security of company information.

They have sent us the current design of their company's infrastructure and ask us to help their technicians to redesign a new optimal system model, which guarantees them to be safe from cyber-attacks. This model must have the necessary mechanisms to comply with current legislation corresponding to the sector.

The initial scheme is shown below (network without segmentation):



This project has been funded with support from the European Commission.
This publication [communication] reflects the views only of the author, and the Commission cannot be held responsible for any use which may be made of the information contained therein.

In this design it can be seen as what network infrastructure has traditionally been in industrial control systems, a flat network defined by functionality. As can be seen in the image, there are no security elements to carry out segmentation and bad practices are used such as using server computers with two network cards to join different networks.

You must propose different network segmentation solutions of an industrial control system, with different levels of security in each case.

Tasks to perform:

- Identify the system components, describing the functions of each component.
- Redesign the system with segmentation strategies.
- Identify the main regulations / standards to consider cybersecurity.

Learning objectives

U6LO1. The learner is able to differentiate IT versus OT

U6LO3. The learner is able to identify the main threats and effects of a cyber attack in an industrial environment.

U6LO4. The learner is able to describe the main Information Security Standards in IT

U6LO5. The learner identifies the main security standards related to OT

U6LO6. The learner is able to identify some security measures in industrial processes

U6LO7. The learner is able to identify which are the main components and common protocols in OT

U7LO1. The learner is able to name and describe the levels in the industrial process.

U7LO2. The learner is able to apply company procedures, detecting possible problems and informing a specialist about any security issues.

This project has been funded with support from the European Commission.
This publication [communication] reflects the views only of the author, and the Commission cannot be held responsible for any use which may be made of the information contained therein.

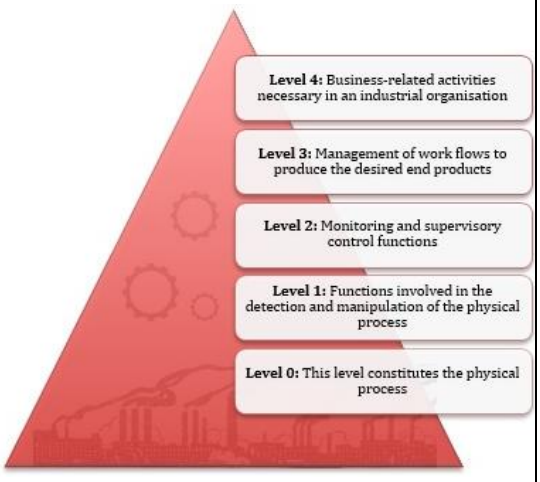
U7LO3. The learner is able to detect malfunction in the machine or breaches in the machine security.

U7LO6. The learner is able to understand networking protocols routing/vpn/PF/etc.

U8LO1. The learner is able to identify which are the data protection regulations in his/her country and in Europe.

U8LO2. The learner is able to work in a secure way with data connected to the different kind of machines used at work.

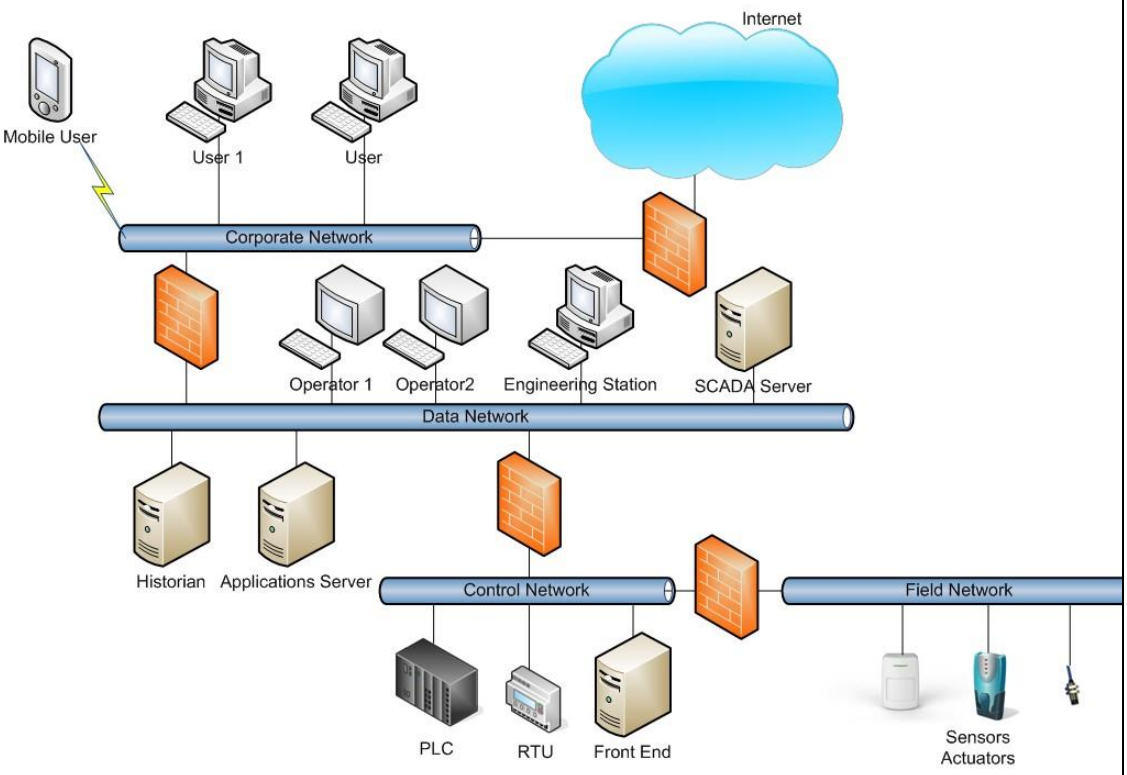
Minimum requirements to carry out the challenge

Previous knowledge	Equipment/software	Training resources
Is able to work with laptop, PC and smartphone. Is familiar with network/internet. Has understanding of microcontroller.	An internet connected device, such as: PC Laptop Smartphone Software: Office	ISA-95 divides control systems into five levels. These levels also allow a first separation of networks to be carried out and show how to perform segmentation.  In a correctly segmented industrial control system at least four types of different network must be defined: a process network, a control network, a data or

This project has been funded with support from the European Commission.
This publication [communication] reflects the views only of the author, and the Commission cannot be held responsible for any use which may be made of the information contained therein.

		control centre network, and a data exchange network. Added to these there are the corporate network and the external network to complete the network architecture. Depending on the level of criticality of the system or the level of security that one wishes to obtain, different strategies and/or tools will be employed to carry out a correct segmentation: Air Gap, IDS/IPS, Virtual networks, Firewall, Data diodes,

Basic segmentation of an industrial control system: This infrastructure is in charge of separating each network through a firewall. The elements have been placed in different networks and adequate rules must be defined for the communications necessary between the different devices to take place.



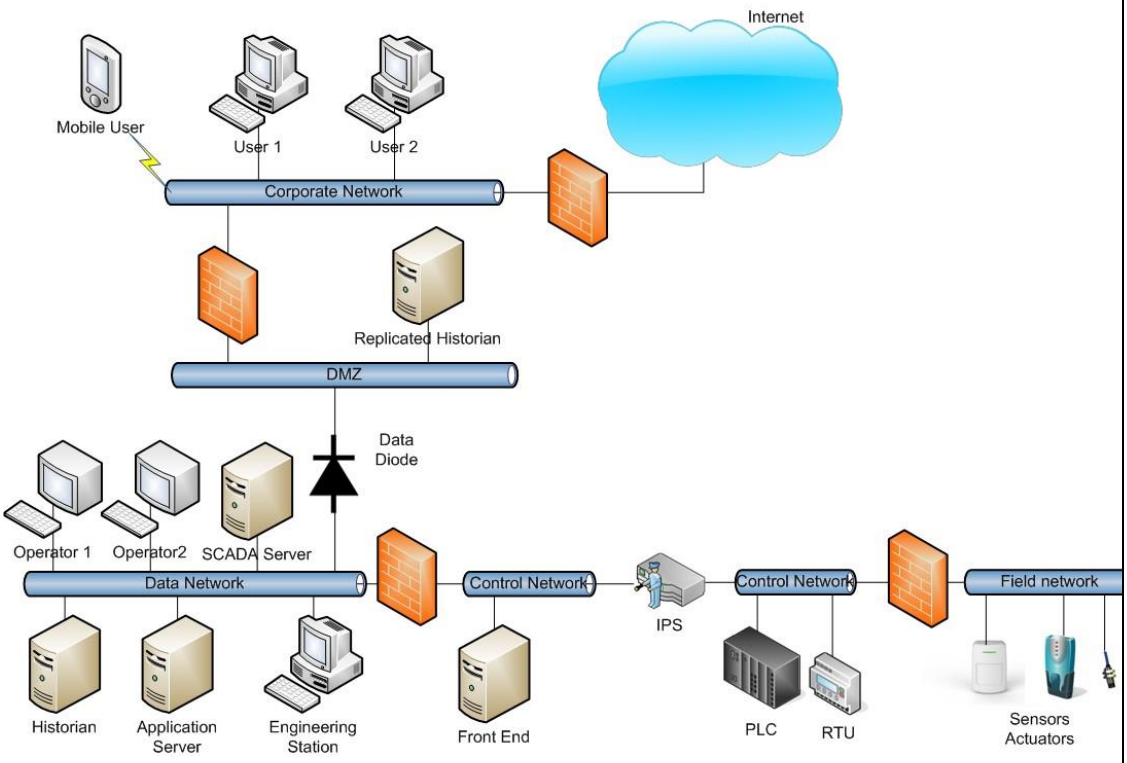
Advanced segmentation for an industrial control system: A further step in security comes through the incorporation of other network security elements, such as data diodes and IPS

This project has been funded with support from the European Commission.
This publication [communication] reflects the views only of the author, and the Commission cannot be held responsible for any use which may be made of the information contained therein.

devices. In this advanced infrastructure, the inclusion of a DMZ network has been opted for to separate the corporate network from the data network. As such, the exchange of historian data with the corporate network is carried out by a replicate historian through a data diode, thus preventing the original from being affected.

A traffic inspection has also been included amongst the elements of the control network, to ensure that the data that come to the Front-End and, subsequently, to the SCADA server, are correct.

Another possible segmentation could be carried out by using VLAN and PVLAN to group together different elements of the control network and the field network and provide an even greater level of security and segmentation.



In industrial control systems, as with any other type of network, the first obstacle to overcome when faced with a technical or security incident is to ensure that its scope is as restricted and as limited as possible. In this regard, network segmentation must be viewed as a cornerstone that must never be missing in secure design.

Main regulations / standards to consider in matter cybersecurity:

Europe:

This project has been funded with support from the European Commission.
This publication [communication] reflects the views only of the author, and the Commission cannot be held responsible for any use which may be made of the information contained therein.

- NIS Directive (Network and Information Security) and European Cybersecurity Strategy/Cybersecurity Act Certification Schema
- General Data Protection Regulation (GDPR).

State laws: cybersecurity, data protection, infrastructure protection…

Information Security/IT Standards: ISO 27001, COBIT, NIST, SANS

OT Security Standards: IEC 62443/ ISA 99, NIST 800 82, NIST 800 53, NERC CIP, CyberEssentials, NISTIR7228…

Schedule of the challenge

Suggested below are notional time allocations for the challenge:

1 hour to explain the challenge.

9 hours researching (search and organize information).

10 hours writing the assignment with research.

2 hours checking the outcome of the challenge.

1 hour team discussion.

1 hour to make final adjustments and to present to teacher.

This project has been funded with support from the European Commission.
This publication [communication] reflects the views only of the author, and the Commission cannot be held responsible for any use which may be made of the information contained therein.

Presentation of the results

The students deliver their challenge to the teacher. Teacher will evaluate their product and can ask some questions to check what the student learned.

As the students work together, they must deliver their own product.

The products that must be delivered are:

- Explanation of subject of the challenge in a written report
- verbal substantiation of the teacher's questions

Evaluation criteria

The following *guidelines* are **suggestive** only and are provided as guidance to support the teacher.

Teamwork performance (10%)

A **suggested** evaluation table in ***Appendix A at*** the back of this document contains criteria that can be used to help the teacher assess team working skills

Challenge (90%):

The document must contain:

- The description of all the components of the original system. (30%)
- A basic segmentation of the industrial control system (40%)
- 2 security standards and 2 regulations. (20%)

Teachers are free to determine their own graduation.

This project has been funded with support from the European Commission.
This publication [communication] reflects the views only of the author, and the Commission cannot be held responsible for any use which may be made of the information contained therein.

cyVETsecurity

Co-funded by the Erasmus+ Programme of the European Union

Appendix A

Goals						
Goals are unclear or poorly understood, resulting in little commitment to them.	1	2	3	4	5	Goals are clear, understood, and have the full commitment of team members.
Openness						
Members are guarded or cautious in discussions.	1	2	3	4	5	Members express thoughts, feelings, and ideas freely.
Mutual Trust						
Members are suspicious of one another's motives.	1	2	3	4	5	Members trust one another and do not fear ridicule or reprisal.
Attitudes Toward Difference						
Members smooth over differences and suppress or avoid conflict.	1	2	3	4	5	Members feel free to voice differences and work through them.

This project has been funded with support from the European Commission.
This publication [communication] reflects the views only of the author, and the Commission cannot be held responsible for any use which may be made of the information contained therein.

Support						
Members are reluctant to ask for or give help.	1	2	3	4	5	Members are comfortable giving and receiving help.
Participation						
Discussion is generally dominated by a few members.	1	2	3	4	5	All members are involved in discussion.
Decision-making						
Decisions are made by only a few members.	1	2	3	4	5	All members are involved in decision-making.
Flexibility						
The group is locked into established rules and procedures that members find difficult to change.	1	2	3	4	5	Members readily change procedures in response to new situations.

This project has been funded with support from the European Commission.
This publication [communication] reflects the views only of the author, and the Commission cannot be held responsible for any use which may be made of the information contained therein.

Use of Member Resources						
Individuals' abilities, knowledge and experience is not well utilized.	1	2	3	4	5	Each member's abilities, knowledge, and experience are fully utilized.

This project has been funded with support from the European Commission.
This publication [communication] reflects the views only of the author, and the Commission cannot be held responsible for any use which may be made of the information contained therein.

cyVETsecurity

Co-funded by the Erasmus+ Programme of the European Union

IT/OT environment

Document for students

This project has been funded with support from the European Commission.
This publication [communication] reflects the views only of the author, and the Commission cannot be held responsible for any use which may be made of the information contained therein.

cyVETsecurity

Co-funded by the Erasmus+ Programme of the European Union

Duration of the challenge

24 hours / 3 days

Your team

Student / teacher should allocate the following:

Team name:

Team member names:

Description of the situation

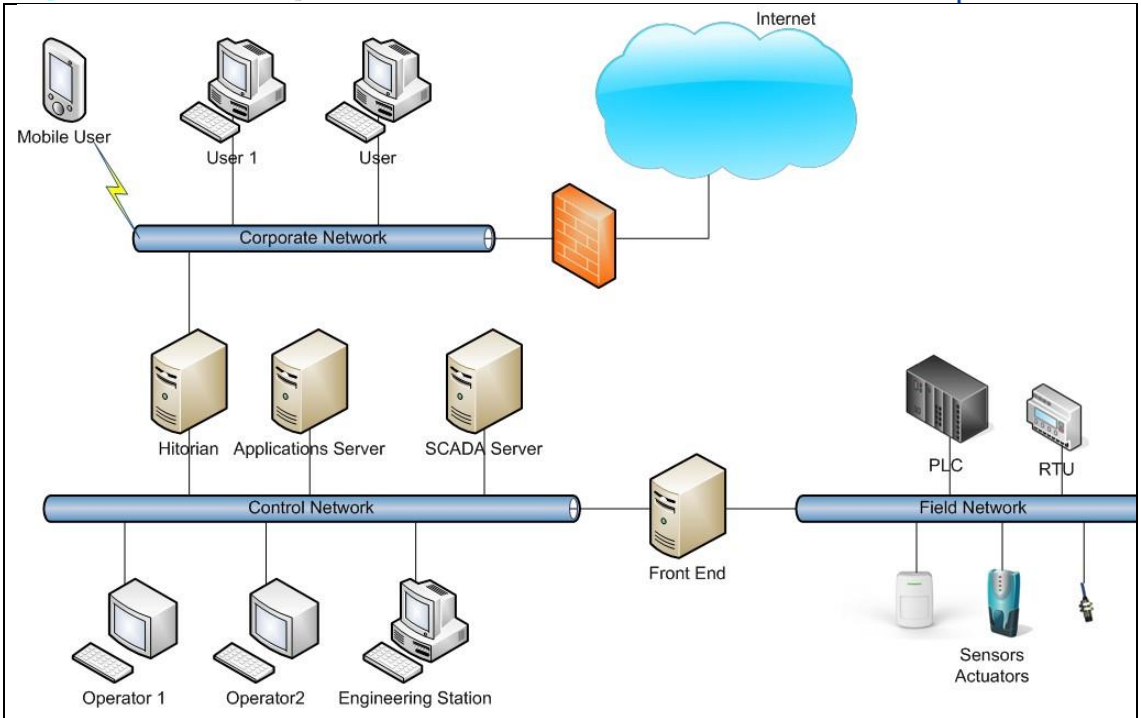
A factory automation company asks for advice on the safety of its production plant.

The company has its IT and OT departments, but they don't know how to jointly manage the complete security of company information.

They have sent us the current design of their company's infrastructure and ask us to help their technicians to redesign a new optimal system model, which guarantees them to be safe from cyber-attacks. This model must have the necessary mechanisms to comply with current legislation corresponding to the sector.

The initial scheme is shown below (network without correct segmentation):

This project has been funded with support from the European Commission.
This publication [communication] reflects the views only of the author, and the Commission cannot be held responsible for any use which may be made of the information contained therein.



In this design it can be seen as what network infrastructure has traditionally been in industrial control systems, a flat network defined by functionality. As can be seen in the image, there are no security elements to carry out segmentation and bad practices are used such as using server computers with two network cards to join different networks.

You must propose different network segmentation solutions of an industrial control system, with different levels of security in each case.

Tasks to perform:

- Identify the system components, describing the functions of each component.
- Redesign the system with segmentation strategies.
- Identify the main regulations / standards to consider cybersecurity.

Learning objectives

U6LO1. The learner is able to differentiate IT versus OT

U6LO3. The learner is able to identify the main threats and effects of a cyber attack in an industrial environment.

This project has been funded with support from the European Commission.
This publication [communication] reflects the views only of the author, and the Commission cannot be held responsible for any use which may be made of the information contained therein.

U6LO4. The learner is able to describe the main Information Security Standards in IT

U6LO5. The learner identifies the main security standards related to OT

U6LO6. The learner is able to identify some security measures in industrial processes

U6LO7. The learner is able to identify which are the main components and common protocols in OT

U7LO1. The learner is able to name and describe the levels in the industrial process.

U7LO2. The learner is able to apply company procedures, detecting possible problems and informing a specialist about any security issues.

U7LO3. The learner is able to detect malfunction in the machine or breaches in the machine security.

U7LO6. The learner is able to understand networking protocols routing/vpn/PF/etc.

U8LO1. The learner is able to identify which are the data protection regulations in his/her country and in Europe.

U8LO2. The learner is able to work in a secure way with data connected to the different kind of machines used at work.

Resources you can use

Some general resources to help you get started:

- ISA 95 levels and network differentiation: https://isaeurope.com/isa-95/ https://www.isa.org/isa95/
- Other segmentations: RG 5.71 levels: https://scp.nrc.gov/slo/regguide571.pdf
- Segmentation Strategies: ISA 99/ IEC 62443 https://www.isa.org/isa99/
- https://ec.europa.eu/digital-single-market/en/network-and-information-security-nis-directive
- https://gdpr.eu/
- https://www.iso.org/isoiec-27001-information-security.html

This project has been funded with support from the European Commission.
This publication [communication] reflects the views only of the author, and the Commission cannot be held responsible for any use which may be made of the information contained therein.

- https://www.isaca.org/resources/cobit
- https://www.nist.gov/

Recommended process

In order to solve your challenge, you need to work in an organised way. We suggest you follow these steps:

1. Define the questions and activities from the challenge description
2. Look for information related to those parameters (see resources proposed, but it is suggested you use others)
3. Select which information is important to solve the challenge.
4. Write your answers and explanations in your own words.
5. You work in groups but write your own paper.
6. Share your research with each other
7. Implement the actions.
8. Present the results (following teacher´s instructions).
9. Evaluate how you carried out the challenge

Evaluation criteria

- Check if all Learning objectives are covered
- Check if you can explain what you did in the challenge

This project has been funded with support from the European Commission.
This publication [communication] reflects the views only of the author, and the Commission cannot be held responsible for any use which may be made of the information contained therein.

cyVETsecurity

Co-funded by the Erasmus+ Programme of the European Union

Penetration test

Document for teachers

This project has been funded with support from the European Commission.
This publication [communication] reflects the views only of the author, and the Commission cannot be held responsible for any use which may be made of the information contained therein.

cyVETsecurity

Co-funded by the Erasmus+ Programme of the European Union

Duration of the challenge

24 hours / 3 days

Description of the situation

Using online scanners, the student must scan and do security search for 3-5 different webpages. Most of the tools can scan malware, blacklisting status, injected spam etc. Some of them could make even vulnerability report.

For different webpages students can use different scanners, but they can also scan one webpage with different scanners. Before scanning the student should set goals for scanning, what kind of vulnerabilities the scanner should help to find. After scanning and information (evidences) gathering the team should discuss about the findings and write vulnerability report:

- Vulnerability name and date of discovery
- Description of the vulnerability
- Possible impacts
- Guidance for fixing

Learning objectives

U1LO1. The learner is able to identify and apply the phases of the Audit Process

U1LO2. The learner is able to collect evidences

U1LO3. The learner is able to search and exploit vulnerability

U1LO4. The learner is able to do a vulnerability report

This project has been funded with support from the European Commission.
This publication [communication] reflects the views only of the author, and the Commission cannot be held responsible for any use which may be made of the information contained therein.

Minimum requirements to carry out the challenge

Previous knowledge	Equipment/software	Training resources
Is able to work with laptop, PC and smartphone. Is familiar with network/internet. Has understanding of common vulnerabilities of webpages.	An internet connected device, such as: PC Laptop Smartphone Software: Packet Tracer Office	Online scanners: • https://sitecheck.sucuri.net/ • https://www.ssllabs.com/ssltest/ • https://pentest-tools.com/ Free online scanners https://geekflare.com/online-scan-website-security-vulnerabilities/ Other resources and articles: • https://securitytrails.com/blog/online-vulnerability-scanning-tools • https://resources.infosecinstitute.com/14-popular-web-application-vulnerability-scanners/ • https://resources.whitesourcesoftware.com/blog-whitesource/web-vulnerability-scanners • Guide the students how to use scanners • How to gather information (evidences) and to analyse • How to write vulnerability report *There are a very large body of resources available for this curriculum. Teachers*

This project has been funded with support from the European Commission.
This publication [communication] reflects the views only of the author, and the Commission cannot be held responsible for any use which may be made of the information contained therein.

		should use all resources available to them. *These are the resources that have been issued to the students in the challenge.*

This project has been funded with support from the European Commission.
This publication [communication] reflects the views only of the author, and the Commission cannot be held responsible for any use which may be made of the information contained therein.

Schedule of the challenge

Suggested below are notional time allocations for the challenge:

1 hour to explain the challenge

6 hours to teach how to use scanners

4 hours to collect evidences

6 hours based on scanner output to search and exploit vulnerabilities

2 hours for team discussion

4 hours to write vulnerability report

1 hours to make final adjustments and to present to teacher

Presentation of the results

The students deliver their challenge to the teacher. Teacher will evaluate their report and can ask some questions to check what the student learned.

The result must be:

- Vulnerability report
- Verbal substantiation of the teacher's questions

This project has been funded with support from the European Commission.
This publication [communication] reflects the views only of the author, and the Commission cannot be held responsible for any use which may be made of the information contained therein.

Evaluation criteria

The following *guidelines* are **suggestive** only and are provided as guidance to support the teacher.

Teamwork performance (20%)

A **suggested** evaluation table in ***Appendix A*** at the back of this document contains criteria that can be used to help the teacher assess team working skills

Challenges:

Vulnerability report (60%)

Verbal substantiation of the teacher's questions (20%)

Teachers are free to determine their own graduation.

This project has been funded with support from the European Commission.
This publication [communication] reflects the views only of the author, and the Commission cannot be held responsible for any use which may be made of the information contained therein.

cyVETsecurity

Co-funded by the Erasmus+ Programme of the European Union

Appendix A

Goals						
Goals are unclear or poorly understood, resulting in little commitment to them.	1	2	3	4	5	Goals are clear, understood, and have the full commitment of team members.
Openness						
Members are guarded or cautious in discussions.	1	2	3	4	5	Members express thoughts, feelings, and ideas freely.
Mutual Trust						
Members are suspicious of one another's motives.	1	2	3	4	5	Members trust one another and do not fear ridicule or reprisal.
Attitudes Toward Difference						
Members smooth over differences and suppress or avoid conflict.	1	2	3	4	5	Members feel free to voice differences and work through them.

This project has been funded with support from the European Commission.
This publication [communication] reflects the views only of the author, and the Commission cannot be held responsible for any use which may be made of the information contained therein.

Support						
Members are reluctant to ask for or give help.	1	2	3	4	5	Members are comfortable giving and receiving help.
Participation						
Discussion is generally dominated by a few members.	1	2	3	4	5	All members are involved in discussion.
Decision-making						
Decisions are made by only a few members.	1	2	3	4	5	All members are involved in decision-making.
Flexibility						
The group is locked into established rules and procedures that members find difficult to change.	1	2	3	4	5	Members readily change procedures in response to new situations.

This project has been funded with support from the European Commission.
This publication [communication] reflects the views only of the author, and the Commission cannot be held responsible for any use which may be made of the information contained therein.

Use of Member Resources						
Individuals' abilities, knowledge and experience is not well utilized.	1	2	3	4	5	Each member's abilities, knowledge, and experience are fully utilized.

This project has been funded with support from the European Commission.
This publication [communication] reflects the views only of the author, and the Commission cannot be held responsible for any use which may be made of the information contained therein.

cyVETsecurity

Co-funded by the Erasmus+ Programme of the European Union

Appendix B

Guidance for teachers on implementing the challenge

This challenge can be delivered as a standalone challenge or aligned / embedded with other appropriate qualifications / learning. It may be prudent to ensure the evidence generated from the challenge is appropriate to map to the criteria for the aligned qualification.

The delivery method for this challenge is completely at the discretion of the teacher. This teacher document is presuming the students will be issued with the student challenge document and provide findings based on this. However, for example, the teacher could issue the challenge and proposed findings and instruct the students to establish how the teacher came to these findings.

I. The time stipulated for this challenge is notional only and the time allocated should be determined by the teacher according to the knowledge and skill level of the student(s) undertaking the challenge.

II. The percentage allocated for grading the findings are suggested only and should be adjusted to suit the context / learning environment in which the challenge is being delivered. For example, if the students are not expected to be graded for team working or presentation skills, then 100% of the grades could be assigned to their findings.

This project has been funded with support from the European Commission.
This publication [communication] reflects the views only of the author, and the Commission cannot be held responsible for any use which may be made of the information contained therein.

cyVETsecurity

Co-funded by the Erasmus+ Programme of the European Union

Penetration test

Document for students

This project has been funded with support from the European Commission.
This publication [communication] reflects the views only of the author, and the Commission cannot be held responsible for any use which may be made of the information contained therein.

cyVETsecurity

Co-funded by the Erasmus+ Programme of the European Union

Duration of the challenge

24 hours / 3 days

Your team

Student / teacher should allocate the following:

Team name:

Team member names:

Description of the situation

Using online scanners, you must scan and do security search for 5 different webpages (SME). You must use the scanners output to search and exploit vulnerabilities. After team discussion you must write vulnerability report:

- Vulnerability name and date of discovery
- Description of the vulnerability
- Possible impacts
- Guidance for fixing

Learning objectives

U1LO1. The learner is able to identify and apply the phases of the Audit Process

U1LO2. The learner is able to collect evidences

U1LO3. The learner is able to search and exploit vulnerability

U1LO4. The learner is able to do a vulnerability report

This project has been funded with support from the European Commission.
This publication [communication] reflects the views only of the author, and the Commission cannot be held responsible for any use which may be made of the information contained therein.

Resources you can use

Some general resources to help you get started:

Online scanners:

- https://sitecheck.sucuri.net/
- https://www.ssllabs.com/ssltest/
- https://pentest-tools.com/

- Learn how to use scanners
- How to use scanners output
- Write vulnerability report

Recommended process

In order to solve your challenge, you need to work in an organised way. We suggest you follow these steps:

1. Define the questions and activities from the challenge description
2. Learn to use online scanners, at least one of them
3. Collect evidences.
4. Search and exploit vulnerabilities.
5. Write vulnerability report.
    a. Vulnerability name and date of discovery
    b. Description of the vulnerability
    c. Possible impacts
    d. Guidance for fixing

This project has been funded with support from the European Commission.
This publication [communication] reflects the views only of the author, and the Commission cannot be held responsible for any use which may be made of the information contained therein.

6. Share report with your team
7. Present the results (following teacher´s instructions).
8. Evaluate how you carried out the challenge

Evaluation criteria

- Check if all learning objectives are covered
- Check if you can explain what you did in the challenge
- The vulnerability report is covered

This project has been funded with support from the European Commission.
This publication [communication] reflects the views only of the author, and the Commission cannot be held responsible for any use which may be made of the information contained therein.

cyVETsecurity

Co-funded by the Erasmus+ Programme of the European Union

Information Security Governance and Management

Document for teachers

This project has been funded with support from the European Commission.
This publication [communication] reflects the views only of the author, and the Commission cannot be held responsible for any use which may be made of the information contained therein.

cyVETsecurity

Co-funded by the Erasmus+ Programme of the European Union

Duration of the challenge

24 hours / 3 days

Description of the situation

The challenge objective will be to manage the security of a service company in the IT sector.

To implement an Information Security Management System (ISMS), you must follow the steps of the appropriate standard.

You must perform a risk assessment on the assets of the company and propose solutions to reduce the level of risk of the company.

1. Identify at least 10 assets to protect the company.
2. Identify at least 4 possible threats for each asset.
3. Risk assessment: choose the probability and impact of each threat on each asset (RISK = PROBABILITY x IMPACT).

PROBABILITY	
1-Low	The threat occurs at most once each year.
2-Medium	The threat occurs at most once a month.
3-High	The threat is given at most once a week.
IMPACT	
1-Low	The damage derived from the threat has no relevant consequences for the company.
2-Medium	The damage derived from the threat has significant consequences for the company.
3-High	The damage derived from the threat has serious consequences for the company.

4. Develop proposals to reduce the level of potential risk that is above the stipulated limit.

RISK ACCEPTANCE CRITERIA	
Risk <= 4	The company considers the risk of little noteworthy.
Risk > 4	The company considers the notable risk and must proceed with its treatment.

This project has been funded with support from the European Commission.
This publication [communication] reflects the views only of the author, and the Commission cannot be held responsible for any use which may be made of the information contained therein.

Example:

RISK ASSESSMENT				
ASSET	THREAT	PROBABILITY	IMPACT	RISK
Web Server	Denial of Service (DoS)	3	2	6
…	…	1	3	3
…	…	1	2	2

Learning objectives

U10LO1. The learner knows and understands standards and safety regulations (ISO, ISACA, NIST).

U10LO2. The learner is able to implement information security governance (ISMS).

U10LO3. The learner is able to carry out a risk analysis.

U10LO4. The learner is able to work applying the regulations about personal information (RGPD).

Minimum requirements to carry out the challenge

Previous knowledge	Equipment/software	Training resources
Is able to work with laptop, PC and smartphone. Is familiar with	An internet connected device, such as: PC Laptop Smartphone	ISO/IEC 27000: Information security management systems (ISMS): https://www.iso.org/standard/73906.html ISO/IEC 27001: requirements for an information security management system (ISMS): https://www.iso.org/standard/54534.html ISO/IEC 27002: Code of practice for information security controls: https://www.iso.org/standard/54533.html

This project has been funded with support from the European Commission.
This publication [communication] reflects the views only of the author, and the Commission cannot be held responsible for any use which may be made of the information contained therein.

network/internet. Has computer skills.	Software: Office	MAGERIT Methodology: https://administracionelectronica.gob.es/ctt/verPestanaDescargas.htm?idIniciativa=184&idioma=en#.X6hJTWhKjtQ RGPD: https://gdprinfo.eu/ ISACA: https://www.isaca.org/resources/it-risk NIST: https://csrc.nist.gov/Projects/risk-management

Schedule of the challenge

Suggested below are notional time allocations for the challenge:

- 2 hours to identify the parameters of the challenge.
- 10 hours to look for information.
- 2 hours to select information.
- 2 hours to generate alternatives.
- 2 hours to present proposals / collate findings and discuss them.
- 1 hour to identify how findings will be presented.
- 2 hours to prepare findings into appropriate format.
- 2 hours to present / discuss findings.
- 1 hour to evaluate / assess how you carried out the challenge and how you might make improvements for any future activities.

This project has been funded with support from the European Commission.
This publication [communication] reflects the views only of the author, and the Commission cannot be held responsible for any use which may be made of the information contained therein.

Presentation of the results

The findings can be presented in whatever media the group decide upon. The findings must be in a form that can be retained following the challenge.

This could be a presentation of the findings, which may include but is not restricted to the following formats:

- Presentation using Software.
- Video.
- Written report.
- Blog / vlog / website
- Any other suitable medium.

Note: Teachers should decide the appropriate format for the students to present their results.

Evaluation criteria

The following *guidelines* are **suggestive** only and are provided as guidance to support the teacher (Guidance in Appendix C section (iii))

Public presentation (20%)

A ***suggested*** evaluation table in ***Appendix A*** at the back of this document which contains criteria can be used to help the teacher assess public presentation skills.

Teamwork performance (20%)

A **suggested** evaluation table in ***Appendix B*** at the back of this document contains criteria that can be used to help the teacher assess team working skills.

Findings from the challenge (60%). Possibly 10% per item

A **suggested** evaluation table in ***Appendix C*** at the back of this document contains criteria that can be used to help the teacher assess technical skills.

This project has been funded with support from the European Commission.
This publication [communication] reflects the views only of the author, and the Commission cannot be held responsible for any use which may be made of the information contained therein.

cyVETsecurity

Co-funded by the Erasmus+ Programme of the European Union

Appendix A

Presentation evaluation (Team or Individual)

Criteria	Excellent	Good	Nothing to evaluate
Oral Introduction: Introduced speaker, captured audience attention	10	5	0
Body of Speech: Easy to follow and understand, information seemed accurate and complete	10	5	0
Summary: Brief, clear, and provided a wrap-up of the topic	10	5	0
Performance: Speaker showed good inflection, proper pronunciation, used expression to demonstrate points, appeared conversational and natural, made eye contact with audience, and voice was loud and clear enough to hear; reliance on notecards was limited	10	5	0
Participant's Knowledge: Participant was able to answer questions from the audience after repeating the question	10	5	0
Audience Attention: Held audience's attention for the duration	10	5	0
Sources: Sources were listed at the end of the speech	10	5	0

Appendix B

Goals						
Goals are unclear or poorly understood, resulting in little commitment to them.	1	2	3	4	5	Goals are clear, understood, and have the full commitment of team members.
Openness						

This project has been funded with support from the European Commission.
This publication [communication] reflects the views only of the author, and the Commission cannot be held responsible for any use which may be made of the information contained therein.

Members are guarded or cautious in discussions.	1	2	3	4	5	Members express thoughts, feelings, and ideas freely.
Mutual Trust						
Members are suspicious of one another's motives.	1	2	3	4	5	Members trust one another and do not fear ridicule or reprisal.
Attitudes Toward Difference						
Members smooth over differences and suppress or avoid conflict.	1	2	3	4	5	Members feel free to voice differences and work through them.
Support						
Members are reluctant to ask for or give help.	1	2	3	4	5	Members are comfortable giving and receiving help.
Participation						

This project has been funded with support from the European Commission.
This publication [communication] reflects the views only of the author, and the Commission cannot be held responsible for any use which may be made of the information contained therein.

Discussion is generally dominated by a few members.	1	2	3	4	5	All members are involved in discussion.
Decision-making						
Decisions are made by only a few members.	1	2	3	4	5	All members are involved in decision-making.
Flexibility						
The group is locked into established rules and procedures that members find difficult to change.	1	2	3	4	5	Members readily change procedures in response to new situations.
Use of Member Resources						
Individuals' abilities, knowledge and experience is not well utilized.	1	2	3	4	5	Each member's abilities, knowledge, and experience are fully utilized.

This project has been funded with support from the European Commission.
This publication [communication] reflects the views only of the author, and the Commission cannot be held responsible for any use which may be made of the information contained therein.

cyVETsecurity

Co-funded by the Erasmus+ Programme of the European Union

Appendix C

Challenge evaluation

Criteria	Excellent	Good	Nothing to evaluate
The main assets have been identified	10	5	0
Threats have been assigned for each asset.	10	5	0
The probability has been identified for each asset and threat.	10	5	0
The impact has been identified for each asset and threat.	10	5	0
The risk analysis has been done.	10	5	0
Solutions have been proposed to reduce the risk of assets.	10	5	0

This project has been funded with support from the European Commission.
This publication [communication] reflects the views only of the author, and the Commission cannot be held responsible for any use which may be made of the information contained therein.

cyVETsecurity

Co-funded by the Erasmus+ Programme of the European Union

Information Security Governance and Management

Document for students

This project has been funded with support from the European Commission.
This publication [communication] reflects the views only of the author, and the Commission cannot be held responsible for any use which may be made of the information contained therein.

cyVETsecurity

Co-funded by the Erasmus+ Programme of the European Union

Duration of the challenge

24 hours / 3 days

Your team

Student / teacher should allocate the following:

Team name:

Team member names:

Description of the situation

The challenge objective will be to manage the security of a service company in the IT sector.

To implement an Information Security Management System (ISMS), you must follow the steps of the appropriate standard.

You must perform a risk assessment on the assets of the company and propose solutions to reduce the level of risk of the company.

1. Identify at least 10 assets to protect the company.
2. Identify at least 4 possible threats for each asset.
3. Risk assessment: choose the probability and impact of each threat on each asset.

PROBABILITY	
1-Low	The threat occurs at most once each year.
2-Medium	The threat occurs at most once a month.
3-High	The threat is given at most once a week.
IMPACT	
1-Low	The damage derived from the threat has no relevant consequences for the company.
2-Medium	The damage derived from the threat has significant consequences for the company.
3-High	The damage derived from the threat has serious consequences for the company.

This project has been funded with support from the European Commission.
This publication [communication] reflects the views only of the author, and the Commission cannot be held responsible for any use which may be made of the information contained therein.

4. Develop proposals to reduce the level of potential risk that is above the stipulated limit.

RISK ACCEPTANCE CRITERIA	
Risk <= 4	The company considers the risk of little noteworthy.
Risk > 4	The company considers the notable risk and must proceed with its treatment.

Learning objectives

U10LO1. The learner knows and understands standards and safety regulations (ISO, ISACA, NIST).

U10LO2. The learner is able to implement information security governance (ISMS).

U10LO3. The learner is able to carry out a risk analysis.

U10LO4. The learner is able to work applying the regulations about personal information (RGPD).

Resources you can use

Some general resources to help you get started:

- ISO/IEC 27000: Information security management systems (ISMS): https://www.iso.org/standard/73906.html
- ISO/IEC 27001: requirements for an information security management system (ISMS): https://www.iso.org/standard/54534.html
- ISO/IEC 27002: Code of practice for information security controls: https://www.iso.org/standard/54533.html
- MAGERIT Methodology: https://administracionelectronica.gob.es/ctt/verPestanaDescargas.htm?idIniciativa=184&idioma=en#.X6hJTWhKjtQ
- RGPD: https://gdprinfo.eu/
- ISACA: https://www.isaca.org/resources/it-risk
- NIST: https://csrc.nist.gov/Projects/risk-management

This project has been funded with support from the European Commission.
This publication [communication] reflects the views only of the author, and the Commission cannot be held responsible for any use which may be made of the information contained therein.

Recommended process

In order to solve your challenge, you need to work in an organised way. We suggest you follow these steps:

1. Define the questions and activities from the challenge description
2. Look for information related to those parameters (see resources proposed, but it is suggested you use others)
3. Select which information is important to solve the challenge.
4. Write your answers and explanations in your own words.
5. You work in groups but write your own paper.
6. Share your research with each other
7. Implement the actions.
8. Present the results (following teacher´s instructions).
9. Evaluate how you carried out the challenge

Evaluation criteria

- Results presentation: 20%
- Teamwork: 20%
- Challenge: 60%
  - The main assets have been identified (10%)
  - Threats have been assigned for each asset (10%)
  - The probability has been identified for each asset and threat (10%)
  - The impact has been identified for each asset and threat (10%)
  - The risk analysis has been done (10%)
  - Solutions have been proposed to reduce the risk of assets (10%)

This project has been funded with support from the European Commission.
This publication [communication] reflects the views only of the author, and the Commission cannot be held responsible for any use which may be made of the information contained therein.

cyVETsecurity

Co-funded by the Erasmus+ Programme of the European Union

DevSecOp: Integrating security since the development phase

Document for teachers

This project has been funded with support from the European Commission. This publication [communication] reflects the views only of the author, and the Commission cannot be held responsible for any use which may be made of the information contained therein.

Duration of the challenge

40 hours / (7 days with 6h/day or 10 days with 4h/day

Description of the challenge (to present to the students)

You are developing an app for Android with Kotlin but you realise that you didn´t take into account that the data collected by the App are not encrypted and are easily accessible by a third party, outside the App.

You have to redo everything from the beginning and this is not the first time it happens. ¿What can you do to avoid this in the future?

You discuss this in your team and decide to apply the DevSecOp development methodology, taking into consideration the ASVS guidelines so security becomes something transversal to app development instead of only a final verification phase where errors where discovered at the end, affecting the whole development and making your team to start over from zero.

This way, you develop an app for Android using safe programming and in the final presentation to the client you explain how security has been integrated from the beginning of the development and which ASVS rules and directives you have followed.

The app has to be completely functional, although it is not necessary to launch it in Google Play.

Learning outcomes

U11LO1. The learner is able to identify secure programming techniques

U11LO2. The learner is able to develop apps with information delivery (certificates, protocols, signatures)

U11LO3. The learner is able to develop apps without data leakage (authorisation & access)

U11LO4. The learner is able to work according to regulations (ASVS)

Minimum requirements to carry out the challenge

Previous knowledge	Equipment/software	Training resources
Advanced knowledge in programming (particularly in Kotlin) Encryption and certificates.	A digital device with internet connection (preferably a computer and/or laptop)	• https://owasp.org/www-project-application-security-verification-standard/ • https://www.youtube.com/watch?v=H5CDiWqkAto • https://www.redhat.com/en/topics/devops/what-is-devsecops • https://owasp.org/www-pdf-archive/OWASP_SCP_Quick_Reference_Guide_v2.pdf • https://kotlinlang.org/docs/tutorials/ • https://kotlinlang.org • https://beginnersbook.com/2017/12/kotlin-tutorial/ • https://www.programiz.com/kotlin-programming/ examples • https://developer.android.comhttps://www.programiz.com/kotlin-programming/examples/guide/topics/ security/cryptography?hl=es-419 • https://www.youtube.com/watch?v=HHo_T7HlRz4 • https://www.youtube.com/watch?v=kN8hlHO8US0 • *https://www.youtube.com/watch?v=2y90l2N1l4k*

		There are a very large body of resources available for this curriculum. Teachers should use all resources available to them. *These are the resources that have been issued to the students in the challenge.*

Schedule of the challenge

This is the suggested duration of each phase of the challenge, if implementing it in a format of 4 hours/day:

Day	Activity
1	- identify the parameters of the challenge (possibly including identifying who will carry out which task (s))
2	- Look for information
3	- 1 hour to select information - 1 hour to create alternatives - 2 hours to identifiy and discuss proposals within the group
4	- Development of the APP
5	- Development of the APP
6	- Development of the APP
7	- Development of the APP
8	- Development of the APP
9	- 2 hours to discuss how to present results (following instructions given) - 2 hours to prepare the presentation of results (for instance with a PowerPoint or a simulator)
10	- 2 hours to present results and debate them in class

Presentation of results

The findings can be presented in whatever media the group decide upon. The findings must be in a form that can be retained following the challenge.
This could be a presentation of the findings, which may include but is not restricted to the following formats:

- Video
- Presentation using a simulation of the App
- Oral \ verbal (This would need to be recorded)
- Written report
- Blog / vlog /wiki
- Any other suitable medium

Note: Teachers should decide the appropriate format for the students to present their results.

Evaluation criteria

The following *guidelines* are **suggestive** only and are provided as guidance to support the teacher.

Public presentation (20%)

A ***suggested*** evaluation table in ***Appendix A*** at the back of this document which contains criteria can be used to help the teacher assess public presentation skills

Teamwork performance (20%)

A **suggested** evaluation table in ***Appendix B*** at the back of this document contains criteria that can be used to help the teacher assess team working skills.

Findings from the challenge (60%).

You can use the table in ***Appendix C*** at the end of this document which contains criteria to help you assess the competences related to this challenge.

Appendix A

Presentation evaluation (Team or Individual)

Criteria	Excellent	Very good	Good	Fair	Not Done	Comments/Suggestions:
Oral Introduction: Introduced speaker, captured audience attention	4	3	2	1	0	
Body of Speech: Easy to follow and understand, information seemed accurate and complete	4	3	2	1	0	
Summary: Brief, clear, and provided a wrap-up of the topic	4	3	2	1	0	
Performance: Speaker showed good inflection, proper pronunciation, used expression to demonstrate points, appeared conversational and natural, made eye contact with audience, and voice was loud and clear enough to hear; reliance on notecards was limited	4	3	2	1	0	
Participant's Knowledge: Participant was able to answer questions from the audience after repeating the question	4	3	2	1	0	
Audience Attention: Held audience's attention for the duration	4	3	2	1	0	
Sources: Sources were listed at the end of the speech	1	0	0	0	0	

Appendix B

Goals						
Goals are unclear or poorly understood, resulting in little commitment to them.	1	2	3	4	5	Goals are clear, understood, and have the full commitment of team members.
Openness						
Members are guarded or cautious in discussions.	1	2	3	4	5	Members express thoughts, feelings, and ideas freely.
Mutual Trust						
Members are suspicious of one another's motives.	1	2	3	4	5	Members trust one another and do not fear ridicule or reprisal.
Attitudes Toward Difference						
Members smooth over differences and suppress or avoid conflict.	1	2	3	4	5	Members feel free to voice differences and work through them.

Support						
Members are reluctant to ask for or give help.	1	2	3	4	5	Members are comfortable giving and receiving help.
Participation						
Discussion is generally dominated by a few members.	1	2	3	4	5	All members are involved in discussion.
Decision-making						
Decisions are made by only a few members.	1	2	3	4	5	All members are involved in decision-making.
Flexibility						
The group is locked into established rules and procedures that members find difficult to change.	1	2	3	4	5	Members readily change procedures in response to new situations.

Use of Member Resources						
Individuals' abilities, knowledge and experience is not well utilized.	1	2	3	4	5	Each member's abilities, knowledge, and experience are fully utilized.

Appendix C

Challenge assessment

Criteria	Excelent	Very good	Good	Suficient	Not done	Comments/suggestions:
App functionality : The app is functional and serves the purpose it was designed for:	4	3	2	1	0	
APP security: Encryption is used to code data.	4	3	2	1	0	
Secure of sensitive data. Data introduced in the app, are treated with security and privacy.	4	3	2	1	0	
Clean code: The code of the app is understandable, is not redundant and it´s clearly structured and commented.	4	3	2	1	0	
Originality: The app is innovative and it shows an unconventional and interesting idea.	4	3	2	1	0	

cyVETsecurity

Co-funded by the Erasmus+ Programme of the European Union

DevSecOp: Integrating security since the development phase

Document for students

This project has been funded with support from the European Commission.
This publication [communication] reflects the views only of the author, and the Commission cannot be held responsible for any use which may be made of the information contained therein.

cyVETsecurity

Co-funded by the Erasmus+ Programme of the European Union

Duration of the challenge

40 hours / (7 days with 6h/day or 10 days with 4h/day

Your team

Student / teacher should allocate the following:

Team name:

Team member names:

Description of the situation

You are developing an app for Android with Kotlin but you realise that you didn´t take into account that the data collected by the App are not encrypted and are easily accessible by a third party, outside the App.

You have to redo everything from the beginning and this is not the first time it happens. ¿What can you do to avoid this in the future?

You discuss this in your team and decide to apply the DevSecOp development methodology, taking into consideration the ASVS guidelines so security becomes something transversal to app development instead of only a final verification phase where errors where discovered at the end, affecting the whole development and making your team to start over from zero.

This way, you develop an app for Android using safe programming and in the final presentation to the client you explain how security has been integrated

This project has been funded with support from the European Commission.
This publication [communication] reflects the views only of the author, and the Commission cannot be held responsible for any use which may be made of the information contained therein.

from the beginning of the development and which ASVS rules and directives you have followed.

The app has to be completely functional, although it is not necessary to launch it in Google Play.

Learning outcomes

U11LO1. The learner is able to identify secure programming techniques
U11LO2. The learner is able to develop apps with information delivery (certificates, protocols, signatures)
U11LO3. The learner is able to develop apps without data leakage (authorisation & access)
U11LO4. The learner is able to work according to regulations (ASVS)

Resources that may be of help

You can use the following resources to start with. However, don´t limit to them only, you can use any other.

- https://owasp.org/www-project-application-security-verification-standard/
- https://www.youtube.com/watch?v=H5CDiWqkAto
- https://www.redhat.com/en/topics/devops/what-is-devsecops
- https://owasp.org/www-pdf-archive/OWASP_SCP_Quick_Reference_Guide_v2.pdf
- https://kotlinlang.org/docs/tutorials/
- https://kotlinlang.org
- https://beginnersbook.com/2017/12/kotlin-tutorial/
- https://www.programiz.com/kotlin-programming/
  examples
- https://developer.android.comhttps://
  www.programiz.com/kotlin-programming/examples/guide/topics/
  security/cryptography?hl=es-419

This project has been funded with support from the European Commission.
This publication [communication] reflects the views only of the author, and the Commission cannot be held responsible for any use which may be made of the information contained therein.

- https://www.youtube.com/watch?v=HHo_T7HlRz4
- https://www.youtube.com/watch?v=kN8hlHO8US0
- *https://www.youtube.com/watch?v=2y90l2N1l4k*

Recommended process

To solve the challenge you should work in a very organised way. We recommend you to follow these steps:

1. Establish which parameters you need to solve this challenge.
2. Look for information related to these parameters (see the proposed resources but also look for others you may need).
3. Select which information is important to solve the challenge.
4. Identify different proposals to solve the challenge.
5. Select the proposals which could be more effective from the team´s point of view.
6. Plan which actions you need to take to solve the challenge (once you know what you need, describe how you will do it).
7. Implement the actions.
8. Present your results and conclusions (following the teacher´s indications).
9. Evaluate how you have solved the challenge.

Evaluation criteria

This project has been funded with support from the European Commission.
This publication [communication] reflects the views only of the author, and the Commission cannot be held responsible for any use which may be made of the information contained therein.

Solution of the challenge (60%):

- **App functionality :** The app is functional and serves the purpose it was designed for:
- **APP security:** Encryption is used to code data.
- **Secure of sensitive data.** Data introduced in the app, are treated with security and privacy.
- **Clean code:** The code of the app is understandable, is not redundant and it´s clearly structured and commented.
- **Originality:** The app is innovative and it shows an unconventional and interesting idea.

Teamwork (20%):

- All team members participate actively in the challenge.
- Team members look for solutions through dialogue and explaining different points of view being flexible.
- Good working atmosphere is promoted within the team.
- If there are problems, solutions are found through agreement.

Presentation of results (20%):

- The presentation is clear and concrete.
- Knowledge about the topic is shown.
- The working app is shown.
- The team keeps the public connected with the presentation.

This project has been funded with support from the European Commission.
This publication [communication] reflects the views only of the author, and the Commission cannot be held responsible for any use which may be made of the information contained therein.

cyVETsecurity

Co-funded by the Erasmus+ Programme of the European Union

DIGITAL FORENSICS IN AN UNSAFE DIGITAL WORLD

Document for teachers

This project has been funded with support from the European Commission.
This publication [communication] reflects the views only of the author, and the Commission cannot be held responsible for any use which may be made of the information contained therein.

cyVETsecurity

Co-funded by the Erasmus+ Programme of the European Union

Duration of the challenge

48 hours / 6 days (Guidance in Appendix C section (i))

Description of the situation

You are a digital forensics investigator, and you have been hired by a business, wishing to carry out an investigation into some of their employees, and their suspicion that they are selling company design secrets to competitors.

Your engagement will be in multiple stages:-

Stage 1: As part of the engagement process. You require to present, to the business management, what the digital forensics process is. You should also present to the organisation relevant legislations that they, and you, should be fully aware of while carrying out the investigation. You should also identify at this presentation what you would anticipate you will require access to, during the investigation.

Stage 2: You will be presented with a suspect's computer; you will be expected to clone the digital evidence that may reside within the computer. The cloned data should be managed properly during the investigation. You should devise and demonstrate a suitable process to ensure the integrity of the cloned data during the investigation. Network data should also be used, and it is likely that this data will have been provided by the business in the form of a network capture file(s).

Stage 3: You will be required to carry out analysis of the cloned data, this will require the investigation and use of multiple applications/tools that will allow you to analyse the cloned data. This analysis

Stage 4: You should now review your findings and collate the evidence recovered to form an idea of what happened. You may also require to carry out additional data recovery to get more digital evidence to substantiate your original view of events.

Learning objectives

- U12LO1. The learner is able to identify and apply forensic analysis stages
- U12LO2. The learner is able to clone devices

This project has been funded with support from the European Commission.
This publication [communication] reflects the views only of the author, and the Commission cannot be held responsible for any use which may be made of the information contained therein.

- U12LO3. The learner is able to carry out diverse analysis
- U12LO4. The learner is able to recover information

This project has been funded with support from the European Commission.
This publication [communication] reflects the views only of the author, and the Commission cannot be held responsible for any use which may be made of the information contained therein.

cyVETsecurity

Co-funded by the Erasmus+ Programme of the European Union

Minimum requirements to carry out the challenge

Previous knowledge	Equipment/software	Training resources
Awareness of the need/reason for digital forensics. Understanding/Experience of Command line environments and filesystems in both windows and Linux OS. Understanding of basic Network communications models especially TCP/IP, with a knowledge of IP addressing, port Numbers, Sequence Numbers, and common protocols. Awareness of various Forensics tools and software.	**Equipment** PC/Laptop with a **recommended** minimum specification of:- CPU Intel i3 or equivalent, RAM 8GByte, SSD HDD 512GByte Various non-volatile storage devices Write Blockers **Software** Digital Forensics Software: - Caine https://www.caine-live.net/ FTK Imager https://accessdata.com/product-download Wireshark https://www.wireshark.org/	Some general resources to help you get started: Using internet searching, review appropriate local legislations that relate to digital security, Forensics process: Example text:- The Basics of Digital Forensics: The Primer for Getting Started in Digital Forensics ISBN-10: 0128016353 ISBN-13: 978-0128016350 Author John Sammons Digital Forensics and Incident Response: Incident response techniques and procedures to respond to modern cyber threats, 2nd Edition Paperback ISBN-10: 183864900X ISBN-13: 978-1838649005 Author: Gerard Johansen **Other useful Resources** https://accessdata.com/assets/pdfs/Conversational_Digital_Forensics_Analysis-Mini_Edition.pdf http://marketing.accessdata.com/l/46432/2018-04-06/5d6nfm **Legislations/Forensics Process**

This project has been funded with support from the European Commission.
This publication [communication] reflects the views only of the author, and the Commission cannot be held responsible for any use which may be made of the information contained therein.

Awareness of booting from non-default sources. This may require an understanding of booting/mounting a real/VM computer from an .ISO file Installation of Software. Virtualisation Software	Autopsy https://www.autopsy.com/ Case Notes https://first-response.co.uk/case notes/ Virtualisation Software Oracle Virtual Box: https://www.virtualbox.org/wiki/Downloads VMware (trial) https://www.vmware.com/products/workstation-pro/workstation-pro-evaluation.html Vmware Player https://my.vmware.com/en/web/vmware/downloads/details?downloadGroup=PLAYER-1600&productId=1039&rPId=51984 Hyper-V(Windows Systems only)	https://ec.europa.eu/digital-single-market/en/news/cybersecurity-act-strengthens-europes-cybersecurity https://ec.europa.eu/anti-fraud/investigations/digital-forensics_en https://www.enisa.europa.eu/topics/trainings-for-cybersecurity-specialists/online-training-material/documents/digital-forensics-handbook This list is not exhaustive, and is only provided to point you in the correct direction. Please note: Which legislations are relevant will be highly dependent on where you are performing this challenge, as legislations may differ between countries. *Resources for sample image files to allow analysis work to be carried out: -* https://www.cfreds.nist.gov/ *https://digitalcorpora.org/ and more specifically* https://digitalcorpora.org/corpora/scenarios/national-gallery-dc-2012-attack *Note: The image files and answer files may require a password, these can be obtained from digital corpora, via email, free of charge to academic institutions.* *There are a very large body of resources available for this curriculum. Teachers should use all resources available to them.*

This project has been funded with support from the European Commission.
This publication [communication] reflects the views only of the author, and the Commission cannot be held responsible for any use which may be made of the information contained therein.

	How to enable on Windows 10:- https://www.altaro.com/hyper-v/install-disable-hyper-v-windows-10/	*These are the resources that have been issued to the students in the challenge.*

This project has been funded with support from the European Commission.
This publication [communication] reflects the views only of the author, and the Commission cannot be held responsible for any use which may be made of the information contained therein.

cyVETsecurity

Co-funded by the Erasmus+ Programme of the European Union

Schedule of the challenge

Suggested below are notional time allocations for the challenge:

- 4 hours to identify the parameters of the challenge (possibly including identifying who will carry out which task (s))
- 20 hours to look for information
- 12 hours to present proposals / collate findings and discuss them (within the student´s group)
- 3 hour to identify how findings will be presented (if not stipulated by teacher)
- 3 hours to prepare findings into appropriate format i.e. PowerPoint for presentation
- 3 hours to present / discuss findings
- 3 hour to evaluate / assess how you carried out the challenge and how you might make improvements for any future activities

This project has been funded with support from the European Commission.
This publication [communication] reflects the views only of the author, and the Commission cannot be held responsible for any use which may be made of the information contained therein.

Presentation of the results

The findings can be presented in whatever media the group decide upon. The findings must be in a form that can be retained following the challenge.

This could be a presentation of the findings, which may include but is not restricted to the following formats:

- Video
- Presentation using Software
- Oral \ verbal (This would need to be recorded)
- Written report
- Blog / vlog /wiki
- Any other suitable medium

Note: Teachers should decide the appropriate format for the students to present their results.

This project has been funded with support from the European Commission.
This publication [communication] reflects the views only of the author, and the Commission cannot be held responsible for any use which may be made of the information contained therein.

Evaluation criteria

The following *guidelines* are **suggestive** only and are provided as guidance to support the teacher (Guidance in Appendix C section (iii))

Public presentation (20%)

A ***suggested*** evaluation table in ***Appendix A*** at the back of this document which contains criteria can be used to help the teacher assess public presentation skills

Teamwork performance (20%)

A **suggested** evaluation table in ***Appendix B*** at the back of this document contains criteria that can be used to help the teacher assess team working skills.

Findings from the challenge (60%). Possibly 15% per item (However the bulk of the work, from a practical viewpoint would be stage 3 – Stage 3 = 30% Stage 1, 2 & 4 10% Each, how you assign marks will be dependant on the importance of the practical element for the awarding body, within which, you are utilising this challenge.

For Stage 1: Answers will vary, however the following website provides a good example of what would be expected. Please note that the stages to the forensics process will vary from document to document, for example if you look at a police forensics process there will be more stages involved due to the nature of evidence preparation and collection, while the process from an industry environment will be more basic. These processes may also vary from country to country.

https://www.open.edu/openlearn/science-maths-technology/digital-forensics/content-section-4.1

There should also be some evidence submitted that the student(s) has investigated suitable legislation and related their chosen legislations to the case study/scenario provided.

https://ec.europa.eu/anti-fraud/investigations/digital-forensics_en

The students will also be required to identify what date and it's location they will need access to during the investigation

This project has been funded with support from the European Commission.
This publication [communication] reflects the views only of the author, and the Commission cannot be held responsible for any use which may be made of the information contained therein.

Stage 2: This stage will require the student(s) to capture the image of a storage medium (e.g. pen drive/hdd, etc.), THIS CAPTURED IMAGE MAY NOT BE THE ACTUAL IMAGE THAT ANALYSIS IS CARRIED OUT ON. They should demonstrate, using suitable forensics tools, that they can capture an image of a storage medium. The following links provide guidance on how some tools can be used to create the image:-

https://medium.com/@Frauenhoffer/how-to-create-a-forensic-image-with-ftk-imager-6fb8ee07fb2d#:~:text=%20Guide%3A%20%201%20Step%201%3A%20For%20a,window.%20If%20you%20have%20connected%20a...%20More%20

https://resources.infosecinstitute.com/category/computerforensics/introduction/areas-of-study/legal-and-ethical-principles/chain-of-custody-in-computer-forensics/

Stage 3: This stage is where the student(s) will analyse the image files (Both Storage and network) they have, either created, or been provided. Their analysis should highlight digital forensics artifacts that help with substantiating whether the accusations made are valid or not.

Image files are readily available at: -

https://digitalcorpora.org/

https://www.cfreds.nist.gov/

The answers provided will vary depending on what image is being used, and what evidence is expected to be collected during the analysis.

Links to guidance information on how to analyse data are provided below: -

https://tinyurl.com/y3hmv4rw

https://tinyurl.com/y36vr9hb

https://tinyurl.com/y4jjjnlv

https://www.sans.org/blog/a-step-by-step-introduction-to-using-the-autopsy-forensic-browser/

For networking analysis, the student(s) should demonstrate that they can analyse and interpret network traffic with the aim of locating specific conversations/communications that relate to the

This project has been funded with support from the European Commission.
This publication [communication] reflects the views only of the author, and the Commission cannot be held responsible for any use which may be made of the information contained therein.

evidence being collected. Answers will vary depending on in the network traffic being analysed.

Here are some helpful links to show how to analyse using wireshark:-

how to use wireshark:
https://www.hackers-arise.com/post/2018/09/24/network-forensics-wireshark-basics-part-1

General guidance on network forenics

https://en.wikipedia.org/wiki/Network_forensics

https://resources.infosecinstitute.com/category/computerforensics/introduction/areas-of-study/digital-forensics/network-forensics-analysis-and-examination-steps/

Sample network logs can be found here:-

https://digitalcorpora.org/

Stage 4: The students should evidence that they have carried out the investigation, and analysis, this stage may be interactive, in the event that evidence is missing. However this stage , when completed may be evidenced using a report/presentation/logbook, or any other suitable means of evidence. Examples of how cases have been solved with the help of digital forensics can be found in the links below: -

https://blog.eccouncil.org/5-cases-solved-using-extensive-digital-forensic-evidence/

https://www.controlrisks.com/campaigns/compliance-and-investigations/five-case-studies-of-interest-to-corporate-investigators

Note: All links provided were valid as at date 30/9/20

This project has been funded with support from the European Commission.
This publication [communication] reflects the views only of the author, and the Commission cannot be held responsible for any use which may be made of the information contained therein.

cyVETsecurity

Co-funded by the Erasmus+ Programme of the European Union

Appendix A

Presentation evaluation (Team or Individual)

Criteria	Excellent	Very good	Good	Fair	Not Done	Comments/Suggestions:
Oral Introduction: Introduced speaker, captured audience attention	4	3	2	1	0	
Body of Speech: Easy to follow and understand, information seemed accurate and complete	4	3	2	1	0	
Summary: Brief, clear, and provided a wrap-up of the topic	4	3	2	1	0	
Performance: Speaker showed good inflection, proper pronunciation, used expression to demonstrate points, appeared conversational and natural, made eye contact with audience, and voice was loud and clear enough to hear; reliance on notecards was limited	4	3	2	1	0	
Participant's Knowledge: Participant was able to answer questions from the audience after repeating the question	4	3	2	1	0	
Audience Attention: Held audience's attention for the duration	4	3	2	1	0	
Sources: Sources were listed at the end of the speech	1	0	0	0	0	

Appendix B

Goals						
Goals are unclear or poorly understood, resulting in little commitment to them.	1	2	3	4	5	Goals are clear, understood, and have the full commitment of team members.

This project has been funded with support from the European Commission.
This publication [communication] reflects the views only of the author, and the Commission cannot be held responsible for any use which may be made of the information contained therein.

Openness						
Members are guarded or cautious in discussions.	1	2	3	4	5	Members express thoughts, feelings, and ideas freely.
Mutual Trust						
Members are suspicious of one another's motives.	1	2	3	4	5	Members trust one another and do not fear ridicule or reprisal.
Attitudes Toward Difference						
Members smooth over differences and suppress or avoid conflict.	1	2	3	4	5	Members feel free to voice differences and work through them.
Support						
Members are reluctant to ask for or give help.	1	2	3	4	5	Members are comfortable giving and receiving help.
Participation						

This project has been funded with support from the European Commission.
This publication [communication] reflects the views only of the author, and the Commission cannot be held responsible for any use which may be made of the information contained therein.

Discussion is generally dominated by a few members.	1	2	3	4	5	All members are involved in discussion.
Decision-making						
Decisions are made by only a few members.	1	2	3	4	5	All members are involved in decision-making.
Flexibility						
The group is locked into established rules and procedures that members find difficult to change.	1	2	3	4	5	Members readily change procedures in response to new situations.
Use of Member Resources						
Individuals' abilities, knowledge and experience is not well utilized.	1	2	3	4	5	Each member's abilities, knowledge, and experience are fully utilized.

This project has been funded with support from the European Commission.
This publication [communication] reflects the views only of the author, and the Commission cannot be held responsible for any use which may be made of the information contained therein.

cyVETsecurity

Co-funded by the Erasmus+ Programme of the European Union

Appendix C

Guidance for teachers on implementing the challenge

This challenge can be delivered as a standalone challenge or aligned / embedded with other appropriate qualifications / learning. It may be prudent to ensure the evidence generated from the challenge is appropriate to map to the criteria for the aligned qualification.

The delivery method for this challenge is completely at the discretion of the teacher. This teacher document is presuming the students will be issued with the student challenge document and provide findings based on this. However, for example, the teacher could issue the challenge and proposed findings and instruct the students to establish how the teacher came to these findings.

I. The time stipulated for this challenge is notional only and the time allocated should be determined by the teacher according to the knowledge and skill level of the student(s) undertaking the challenge.
II. The percentage allocated for grading the findings are suggested only and should be adjusted to suit the context / learning environment in which the challenge is being delivered. For example, if the students are not expected to be graded for team working or presentation skills, then 100% of the grades could be assigned to their findings.

This project has been funded with support from the European Commission.
This publication [communication] reflects the views only of the author, and the Commission cannot be held responsible for any use which may be made of the information contained therein.

cyVETsecurity

Co-funded by the Erasmus+ Programme of the European Union

DIGITAL FORENSICS IN AN UNSAFE DIGITAL WORLD

Document for students

This project has been funded with support from the European Commission.
This publication [communication] reflects the views only of the author, and the Commission cannot be held responsible for any use which may be made of the information contained therein.

cyVETsecurity

Co-funded by the Erasmus+ Programme of the European Union

Duration of the challenge

48 hours / 6 days

Your team

Student / teacher should allocate the following:

Team name:

Team member names:

Description of the situation

You are a digital forensics investigator, and you have been hired by a business, wishing to carry out an investigation into some of their employees, and their suspicion that they are selling company design secrets to competitors.

Your engagement will be in multiple stages:-

Stage 1: As part of the engagement process. You require to present, to the business management, what the digital forensics process is. You should also present to the organisation relevant legislations that they, and you, should be fully aware of while carrying out the investigation. You should also identify at this presentation what you would anticipate you will require access to, during the investigation.

Stage 2: You will be presented with a suspect's computer; you will be expected to clone the digital evidence that may reside within the computer. The cloned data should be managed properly during the investigation. You should devise and demonstrate a suitable process to ensure the integrity of the cloned data

This project has been funded with support from the European Commission.
This publication [communication] reflects the views only of the author, and the Commission cannot be held responsible for any use which may be made of the information contained therein.

during the investigation. Network data should also be used, and it is likely that this data will have been provided by the business in the form of a network capture file(s).

Stage 3: You will be required to carry out analysis of the cloned data, this will require the investigation and use of multiple applications/tools that will allow you to analyse the cloned data. This analysis

Stage 4: You should now review your findings and collate the evidence recovered to form an idea of what happened. You may also require to carry out additional data recovery to get more digital evidence to substantiate your original view of events.

Learning objectives

- **U12LO1. The learner is able to identify and apply forensic analysis stages**
- **U12LO2. The learner is able to clone devices**
- **U12LO3. The learner is able to carry out diverse analysis**
- **U12LO4. The learner is able to recover information**

Resources you can use

Some general resources to help you get started:

Using internet searching, review appropriate local legislations that relate to digital security,

Forensics process: Example text:-

The Basics of Digital Forensics: The Primer for Getting Started in Digital Forensics

ISBN-10: 0128016353

ISBN-13: 978-0128016350

Author John Sammons

Digital Forensics and Incident Response: Incident response techniques and procedures to respond to modern cyber threats, 2nd Edition Paperback

This project has been funded with support from the European Commission.
This publication [communication] reflects the views only of the author, and the Commission cannot be held responsible for any use which may be made of the information contained therein.

ISBN-10: 183864900X

ISBN-13: 978-1838649005

Author: Gerard Johansen

Legislations

eg. https://ec.europa.eu/digital-single-market/en/news/cybersecurity-act-strengthens-europes-cybersecurity

This list is not exhaustive, and is only provided to point you in the correct direction.

Please note: Which legislations are relevant will be highly dependent on where you are performing this challenge, as legislations may differ between countries.

Recommended process

In order to solve your challenge, you need to work in an organised way. We suggest you follow these steps:

1. Establish the parameters you need to solve the challenge. For example, in this case these could be: recognised industry regulations/laws/guidelines that impact your chosen organisation.
2. Look for information related to those parameters (see resources proposed, but it is suggested you use others)
3. Select which information is important to solve the challenge.
4. Come up with different proposals to solve the challenge.
5. Select the proposal/proposals which are more effective from your group´s point of view.
6. Plan which actions you need to solve the challenge (once you know what you need to do, describe how you will do it).
7. Implement the actions.
8. Present the results (following teacher´s instructions).
9. Evaluate how you carried out the challenge

This project has been funded with support from the European Commission.
This publication [communication] reflects the views only of the author, and the Commission cannot be held responsible for any use which may be made of the information contained therein.

Evaluation criteria

- Stages are identified and followed when applying a forensic analysis.
  Findings are provided in accordance with established reporting procedures.
  Suitable identification and justification of legislations.
  Identification of access requirements and scope of investigation.

- Sound duplicates and management of digital devices, to ensure integrity of evidence

- Analysis is carried out on both system data as well as network data.
  For example analysis of log files, evidence and other information to determine best methods for identifying the perpetrators of a network intrusion.
  Network traffic associated with malicious activities is captured and analysed.

- Recovered data are examined to define the relevance of the intrusion.
  Data are extracted using data carving techniques (Forensic Tool Kit, Foremost…)
  Seized data are decrypted, this may require the request of passwords or decryption keys based upon valid reasons identified during the investigation.

- Suitable reflection/evaluation and improvement suggestions should be evident.

This project has been funded with support from the European Commission.
This publication [communication] reflects the views only of the author, and the Commission cannot be held responsible for any use which may be made of the information contained therein.

cyVETsecurity

Co-funded by the Erasmus+ Programme of the European Union

Perimetral security

Document for teachers

This project has been funded with support from the European Commission.
This publication [communication] reflects the views only of the author, and the Commission cannot be held responsible for any use which may be made of the information contained therein.

cyVETsecurity

Co-funded by the Erasmus+ Programme of the European Union

Duration of the challenge

24 hours / 3 days

Description of the situation

You are working in a small (or medium) company as an IT specialist and you are responsible of the perimetral security (student can choose the topic, also the teacher can recommend).

Your task is to understand, are there security gaps in this company? You must perform an internal and external security assessment to determine whether you have vulnerabilities and determine what measures should be taken in place but are not. This can include:

- implementing stronger security policies,
- strengthen password policy,
- monitor company's network for suspicious activities,
- check data backup system,
- conduct security trainings for employees:
    - how to avoid phishing?
    - cyberattacks from social engineering,
    - what is malware?
    - how to understand and report possible security threats?
    - explain the company's IT policies and best practices.

Your task is to work out different solutions and choose the best solution matching the company's needs and budget.

Learning objectives

U13LO1. The learner is able to implement communication security techniques

This project has been funded with support from the European Commission.
This publication [communication] reflects the views only of the author, and the Commission cannot be held responsible for any use which may be made of the information contained therein.

U13LO2. The learner is able to design and implement a network according to the security model

U13LO3. The learner is able to identify authentication and identity management systems (SSO)

U13LO4. The learner is able to identify event management solutions

Minimum requirements to carry out the challenge

Previous knowledge	Equipment/software	Training resources
Is able to work with laptop, PC and smartphone. Is familiar with network/internet. Understands perimetral security.	An internet connected device, such as: PC Laptop Smartphone	• Penetration testing tools https://www.csoonline.com/article/2943524/11-penetration-testing-tools-the-pros-use.html • Software Testing Tools https://www.softwaretestinghelp.com/penetration-testing-tools/ • Hacking tools https://www.concise-courses.com/hacking-tools/top-ten/ • 5 penetration test tools to secure your network https://www.computerweekly.com/tip/5-penetration-test-tools-to-secure-your-network • Tools for small businesses https://www.comparitech.com/blog/information-security/small-business-cybersecurity-free-tools/ • Security solutions for Small Business https://www.businessnewsdaily.com/6020-cybersecurity-solutions.html • Teacher chooses the company or simulates - it can also be the school environment.

This project has been funded with support from the European Commission.
This publication [communication] reflects the views only of the author, and the Commission cannot be held responsible for any use which may be made of the information contained therein.

		• Help students to choose the focus topic and collect the data: ○ Network monitoring ○ Suspicious activity detection ○ Data Backup Solution ○ Security Incident Management and Tracking *There are a very large body of resources available for this curriculum. Teachers should use all resources available to them.* *These are the resources that have been issued to the students in the challenge.*

This project has been funded with support from the European Commission.
This publication [communication] reflects the views only of the author, and the Commission cannot be held responsible for any use which may be made of the information contained therein.

Schedule of the challenge

Suggested below are notional time allocations for the challenge:

1 hour to explain the challenge

4 hours to collect data (evidences)

6 hours to analyse information

6 hours to work out initial solutions

2 hours for team discussion

4 hours to write report

1 hours to make final adjustments and to present to teacher

Presentation of the results

The students deliver their challenge to the teacher. Teacher will evaluate their solution and can ask questions to check what the student learned.

As the students work together, they must deliver their own solution.

The solution that must be delivered are:

- Short overview of the situation and the main security gaps
- Written report about the measures that should be taken
- Verbal substantiation of the teacher's questions

This project has been funded with support from the European Commission.
This publication [communication] reflects the views only of the author, and the Commission cannot be held responsible for any use which may be made of the information contained therein.

Evaluation criteria

The following *guidelines* are **suggestive** only and are provided as guidance to support the teacher.

Teamwork performance (10%)

A **suggested** evaluation table in ***Appendix A*** at the back of this document contains criteria that can be used to help the teacher assess team working skills

Challenges:

Short overview of the situation and the main security gaps (30%)

Written report about the measures that should be taken (50%)

Verbal substantiation of the teacher's questions (10%)

Teachers are free to determine their own graduation.

This project has been funded with support from the European Commission.
This publication [communication] reflects the views only of the author, and the Commission cannot be held responsible for any use which may be made of the information contained therein.

cyVETsecurity

Co-funded by the Erasmus+ Programme of the European Union

Appendix A

Goals						
Goals are unclear or poorly understood, resulting in little commitment to them.	1	2	3	4	5	Goals are clear, understood, and have the full commitment of team members.
Openness						
Members are guarded or cautious in discussions.	1	2	3	4	5	Members express thoughts, feelings, and ideas freely.
Mutual Trust						
Members are suspicious of one another's motives.	1	2	3	4	5	Members trust one another and do not fear ridicule or reprisal.
Attitudes Toward Difference						
Members smooth over differences and suppress or avoid conflict.	1	2	3	4	5	Members feel free to voice differences and work through them.

This project has been funded with support from the European Commission.
This publication [communication] reflects the views only of the author, and the Commission cannot be held responsible for any use which may be made of the information contained therein.

Support						
Members are reluctant to ask for or give help.	1	2	3	4	5	Members are comfortable giving and receiving help.
Participation						
Discussion is generally dominated by a few members.	1	2	3	4	5	All members are involved in discussion.
Decision-making						
Decisions are made by only a few members.	1	2	3	4	5	All members are involved in decision-making.
Flexibility						
The group is locked into established rules and procedures that members find difficult to change.	1	2	3	4	5	Members readily change procedures in response to new situations.

This project has been funded with support from the European Commission.
This publication [communication] reflects the views only of the author, and the Commission cannot be held responsible for any use which may be made of the information contained therein.

Use of Member Resources						
Individuals' abilities, knowledge and experience is not well utilized.	1	2	3	4	5	Each member's abilities, knowledge, and experience are fully utilized.

This project has been funded with support from the European Commission.
This publication [communication] reflects the views only of the author, and the Commission cannot be held responsible for any use which may be made of the information contained therein.

cyVETsecurity

Co-funded by the Erasmus+ Programme of the European Union

Appendix B

Guidance for teachers on implementing the challenge

This challenge can be delivered as a standalone challenge or aligned / embedded with other appropriate qualifications / learning. It may be prudent to ensure the evidence generated from the challenge is appropriate to map to the criteria for the aligned qualification.

The delivery method for this challenge is completely at the discretion of the teacher. This teacher document is presuming the students will be issued with the student challenge document and provide findings based on this. However, for example, the teacher could issue the challenge and proposed findings and instruct the students to establish how the teacher came to these findings.

I. The time stipulated for this challenge is notional only and the time allocated should be determined by the teacher according to the knowledge and skill level of the student(s) undertaking the challenge.

II. The percentage allocated for grading the findings are suggested only and should be adjusted to suit the context / learning environment in which the challenge is being delivered. For example, if the students are not expected to be graded for team working or presentation skills, then 100% of the grades could be assigned to their findings.

This project has been funded with support from the European Commission.
This publication [communication] reflects the views only of the author, and the Commission cannot be held responsible for any use which may be made of the information contained therein.

cyVETsecurity

Co-funded by the Erasmus+ Programme of the European Union

Perimetral security

Document for students

This project has been funded with support from the European Commission.
This publication [communication] reflects the views only of the author, and the Commission cannot be held responsible for any use which may be made of the information contained therein.

cyVETsecurity

Co-funded by the Erasmus+ Programme of the European Union

Duration of the challenge

24 hours / 3 days

Your team

Student / teacher should allocate the following:

Team name:

Team member names:

Description of the situation

You are working in a small (or medium) company as an IT specialist and you are responsible of the perimetral security.

Are there security gaps in this company? You must perform an internal and external security assessment to determine whether you have vulnerabilities and determine what measures should be taken in place but are not. This can include:

- implementing stronger security policies,
- strengthen password policy,
- monitor company's network for suspicious activities,
- check data backup system,
- conduct security trainings for employees:
    - how to avoid phishing?
    - cyberattacks from social engineering,
    - what is malware?
    - how to understand and report possible security threats?

This project has been funded with support from the European Commission.
This publication [communication] reflects the views only of the author, and the Commission cannot be held responsible for any use which may be made of the information contained therein.

- explain the company's IT policies and best practices.

Your task is to work out different solutions and choose the best solution matching the company's needs and budget.

Learning objectives

U5LO1. The learner is able to implement communication security techniques
U5LO2. The learner is able to design and implement a network according to the security model
U5LO3. The learner is able to identify authentication and identity management systems (SSO)
U5LO4. The learner is able to identify event management solutions

Resources you can use

Some general resources to help you get started:

- Choose the focus topic and collect the data:
  - Network monitoring
  - Suspicious activity detection
  - Data Backup Solution
  - Security Incident Management and Tracking

Recommended process

In order to solve your challenge, you need to work in an organised way. We suggest you follow these steps:

1. Define the questions and activities from the challenge description
2. Select which information is important to solve the challenge
3. Collect data (evidences)

This project has been funded with support from the European Commission.
This publication [communication] reflects the views only of the author, and the Commission cannot be held responsible for any use which may be made of the information contained therein.

4. Analyse gathered information and work out some initial solutions
5. Discuss about the solutions with your team
6. You work in groups but write your own paper
7. Share your report with each other
8. Present the initial solution (following teacher´s instructions)
9. Evaluate how you carried out the challenge

Evaluation criteria

- Check if all learning objectives are covered
- Check if you can explain what you did in the challenge
- You have worked out at least two solutions

This project has been funded with support from the European Commission.
This publication [communication] reflects the views only of the author, and the Commission cannot be held responsible for any use which may be made of the information contained therein.