cyVETsecurity

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

O1. Joint VET curriculum in cybersecurity

A tool to identify cybersecurity competences for different learning 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

1. Introduction

According to a recent report released by Intel Security, called “Hacking the Skills Shortage” (https://www.mcafee.com/content/dam/enterprise/en-us/assets/reports/rp-hacking-skills-shortage.pdf), there will be 1 million to 2 million unfilled cyber-security jobs worldwide by 2019. The report includes the results of a survey of 775 IT decision-makers involved with security, 82% of whom reported a lack of cyber-security skills within their business.

In the same line, ESG´s (Enterprise Strategy Group) research shows that 45% of organisations report having a problematic shortage of cybersecurity skills in 2017 (https://www.esg-global.com/blog/esg-research-suggests-cybersecurity-skills-shortage-is-getting-worse). Of course, this applies to all areas of cybersecurity but recent ESG research shows that the skills shortage has a direct impact on security analytics and operations.

In view of a dynamically evolving threat landscape and building on the review of the 2013 EU cybersecurity strategy, tackling the cybersecurity perils together was one of the three challenges identified in the mid-term review of the Digital Single Market. Thus, on 13 September 2017 the Commission adopted a cybersecurity package.

The package builds upon existing instruments and presents new initiatives to further improve EU cyber resilience and response. It is in the EU's strategic interest to ensure that the technological tools of cybersecurity are developed in a way that allows the digital economy to flourish, while also protecting our security, society and democracy. This includes the protection of critical hardware and software. To reinforce the EU's cybersecurity capacity, the Commission and the High Representative are proposing, among other priorities and actions to address the skills gap in cyber defence. With this objective, the EU will create a cyber defence training and education platform in 2018.

These are just some data and initiatives which represent the reality of the IT world as cybersecurity is concerned and the CyVETsecurity project feeds from this momentum cybersecurity is having in the European and global agenda by producing two intellectual outputs that pretend to contribute to make smaller the gap between existing cybersecurity competences (and awareness) and the real needs (not only from companies but from society itself).

The first one of these 2 intellectual outputs is this “joint VET curriculum in cybersecurity”, which is a selection of the main knowledge, skills and competences related to cybersecurity from a comprehensive research carried out by the project team, which has included the following sources:

- The **SANS Institute** (Escal Institute of Advanced Technologies), a US company specialised in security and cybersecurity training and certification.
- The **National Institute of Standards and Technology (NIST),** a non regulatory agency from the US which has developed the certification NIST 800-53 cybersecurity framework.
- The **International Organisation for Standardization (ISO**), which provides a family of standards regarding information security under the ISO/IEC 27000 .
- The **DigiComp Framework** (European Digital Competence Framework for Citizens), which offers a comprehensive description of the knowledge, skills and attitudes that people need in 5 key areas, being security one of them.

During the research, we found that knowledge, skills and competences related to cybersecurity can be grouped as follows (according to the SANS Institute) in these fields of expertise:

- **Intrusion detection.** It involves discovering potentially harmful activity that could compromise the confidentiality, integrity, or availability of information. There are a few common types of intrusion detection. Network-based detection attempts to detect unauthorized behaviour based on network traffic. Host-based detection tries to find illicit activity on a specific device. Physical detection involves finding threats on physical systems.
- **Secure software development.** Most data breaches are successful because of vulnerabilities or flaws in software code, and commercial software needs to be patched on a regular basis.

- **Risk mitigation.** Involves tracking identified risks, discovering new risks, and keeping track of risk throughout a project. First, it's necessary to understand that data needs to be protected and why. Businesses must identify their most valuable assets and the threats putting them at risk. Knowing how the information is stored, who has access, and how the data is protected are three critical questions to ask for optimal data protection.
- **Cloud security.** There are several threats particular to cloud security. Some of the top dangers include data breaches, system vulnerability exploits, hijacked accounts, inadequate diligence, and malicious insiders.
- **Network monitoring and access management.** Organisations also need professionals who know what they're looking for and can make quick decisions when suspicious behaviour is detected.
- **Security analysis.** To build innovative solutions to prevent hackers from entering corporate networks and stealing sensitive data.
- **Data security.** Especially important for organisations in vulnerable fields, such as healthcare and financial services.

What will you find in this document?

Taking those fields of expertise as basis, we have defined different units of competences and learning outcomes and assessment criteria associated. We have done that taking also into account different professional profiles.

In the next chapter we explain which methodology we used to do that and build our joint VET curriculum in cybersecurity, but first, we want you to understand how you can use this document:

- If you are a VET teacher, you can use the complete curriculum or just parts of it. Depending of who you are addressing and your objectives, you will find that you need only some units, most of them or even all of them! Whatever the number of units, you can use them to introduce cybersecurity and information security pills and practices in an existing VET programme and/or you can design new training programmes taking our curriculum (totally or partially) as it is or adapting it, completing it with any other content you may find relevant. As for the delivery of the curriculum, we have also produced some training materials, covering the different units of competence, which is our output number 2 “O2. cybersecurity challenges”. You can use both documents together or separately but bear in mind that O2 has been built upon O1.

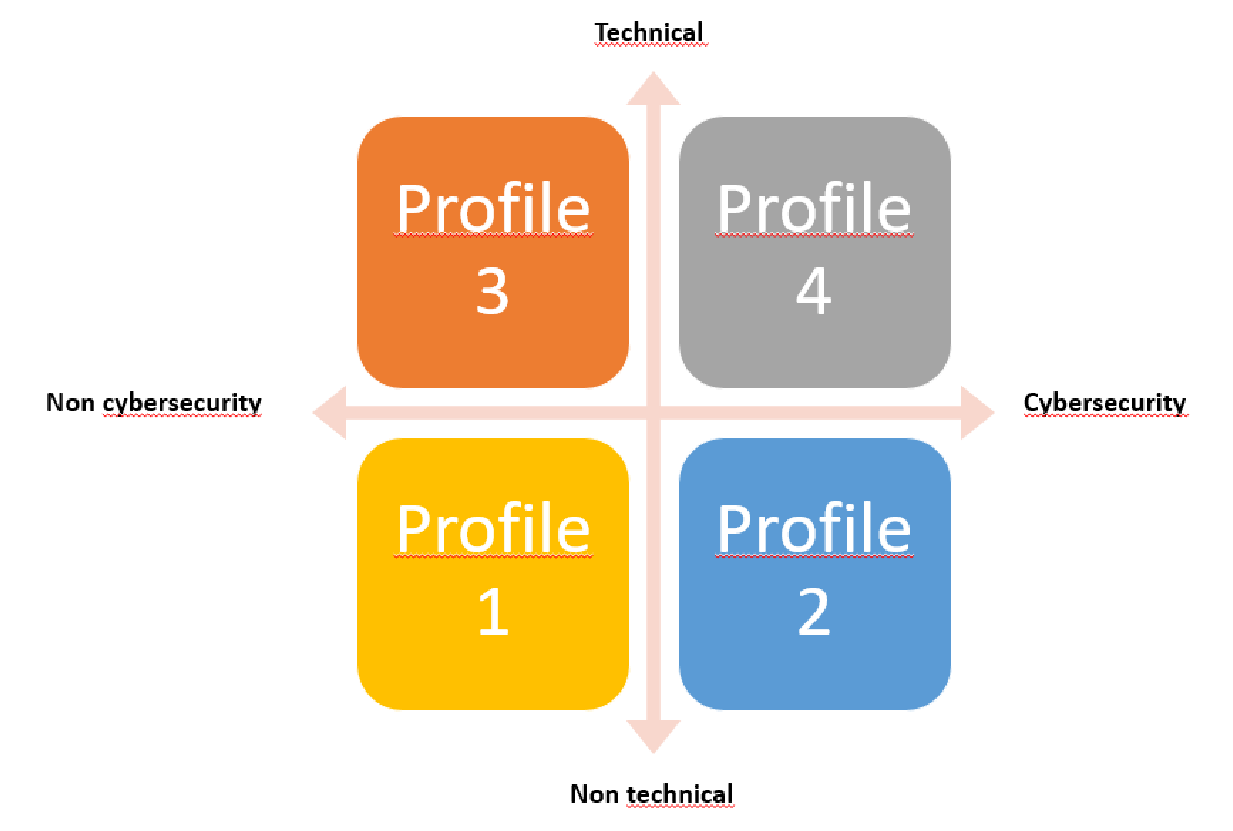
- If you are a company, you can use both outputs for internal training of your employees or even only O1, to ask to a training provider to design a training covering certain units important for your organisation, or even as a support to define the profile of a future worker during a recruitment process.
- If you are an education authority in charge of curriculum design, you may find this output interesting to look at and see which possible units could be implemented in a variety of VET programmes or even in a specialization programme dedicated entirely to cybersecurity. The bibliography we used, referenced in the last chapter, can also be useful.

Constructed following a modular structure (LO grouped in units to be trained together or independently) in the form of a matrix, being lines the units of competence and columns the learning outcomes associated to each unit.

2. Methodology

Taking as basis the fields of expertise described in the previous chapter the next step we took was to characterise different professional profiles and their relation to cybersecurity.

We defined 4 types of profiles:



- **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 cooker, 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.

- **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.

- **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.

These 4 profiles were defined and described during the first meeting of the project in Tallinn. A clarification deserves to be mentioned: The profiles are not addressed to any particular EQF level. It will be the definition of the learning outcomes together with the assessment criteria which will provide guidance to the user in order to decide if it is feasible to apply to a certain target group. However, when designing the curriculum we did bear the following in mind:

- Units related to profile 1 were defined having in mind any level or any VET programme as they cover very basic aspects of cybersecurity to be applicable both at the professional and the personal level. Let´s say they are focused on cyber hygiene and awareness which, however, is not taught in VET programmes and which cover basic digital skills that most of people, however, do not have (see https://ec.europa.eu/jrc/en/digcomp/digital-competence-framework and http://publications.jrc.ec.europa.eu/repository/bitstream/JRC110624/dc_guide_may18.pdf)
- Units related to profile 2 were defined having in mind an EQF level from 3-5. We were thinking of VET programmes such as business administration, finance, health care or e-business and retail.
- Units related to profile 3 were defined having in mind an EQF level from 3-5, aiming specially at industrial fields such as CNC programming, robotics, electricity, electronics or automation.
- Units related to profile 4 were defined having in mind an EQF level 4-5 with an IT background like app development, programming or IT networks management.

The definition of learning outcomes and assessment criteria identified for each unit was one of the most challenging parts of this document. The information available was really extensive so defining specific units was also difficult but bearing in mind the profiles defined by us and the fields of expertise in cybersecurity defined by the SANS Institute made it easier. Simplifying that amount of information in the definition of specific learning outcomes was a more complicated process, which went through different steps where we started with 12-20 learning outcomes per unit (and even more assessment criteria!) to the group of learning outcomes so it could be more manageable, joining and simplifying some of them. Here an example of this, from this:

UNITS OF COMPETENCE	LEARNING OUTCOMES
Unit 1. Penetration test (This unit is based on the work roles described for: "system test and evaluation specialist" and "Information systems security developer" in the NICE	U1LO1. The learner is able to determine the level of assurance of developed capabilities based on test results.
	U1LO2. The learner is able to test plans to address specifications and requirements.
	U1LO3. The learner is able to install and maintain network infraestructure device operating system software (e.g., IOS, firmware)
	U1LO4. The learner is able to make recommendations based on test results.
	U1LO5. The learner is able to determine scope, infrastructure, resources, and data sample size to ensure system requirements are adequately demonstrated
	U1LO6. The learner is able to validate specifications and requirements for testability.
	U1LO7. The learner is able to analyze the results of software, hardware or interoperability testing.
	U1LO8. The learner is able to perform developmental testing on systems under development.
	U1LO9. The learner is able to perform interoperability testin on systems exchanging eletronic information with other systems.
	U1LO10. The learner is able to perform operational testing.
	U1LO11. The learner is able to test, evaluate and verify hardware and/or software to determine compliance with defined specifications and requirements.
	U1LO12. The learner is able to record and manage test data.
	U1LO13. The learner is able to develop and direct system testing and validation procedures and documentation.
	U1LO14. The learner is able to identify and direct the remediation of technical problems encountered during testing and implementaion of new systems
	U1LO15. The learner is able to identify, assess and recommend cybersecurity or cybersecurity-enabled products for use within a system and ensure that recommended products are in compliance with organization´s evaluation and validation requirements.
	U1LO16. The learner is able to perform risk analysis (e.g. threat, vulnerability and probability of occurrence) whenevar an application or system undergoes a major change.
	U1LO17. The learner is able to utilize models and simulations to analyze or predict system performance under different operating conditions
	U1LO18. The learner is able to test and evaluate secure interfaces between information systems, physical systems and/or embedded technologies.
	U1LO19. The learner is able to perform an information security risk assessment.
	U1LO20. The learner is able to perform security reviews and identify security gaps in architecture.

To this:

UNITS OF COMPETENCE	LEARNING OUTCOMES
Unit 1. Penetration test	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

In some cases, we carried out this simplification process by ourselves, but in the case of the profiles 3 and 4 (more complicated in terms of content) we counted with the help of our associated partners in Spain and the Netherlands.

One last question to bear in mind is that profiles are not necessarily exclusive, i.e; even if we defined different units for different profiles, you can exchange units at your convenience and give someone from profile 3 an activity from profile 2 or vice versa. That will depend on your target group and your aims. In the design of the challenges we have taken this into account and we define which previous knowledge or background a person needs to carry out a specific challenge. Or…you could even go crazy and mix profiles to have a more multidisciplinary approach!

As you can see, the design of our curriculum is flexible enough as to be adapted to different VET programmes and levels and to different types of professionals. Just go and take a look to the units more suitable to your objectives!

3. The CyVETsecurity curriculum

	UNITS	LEARNING OUTCOMES	EVALUATION CRITERIA
Profile 1	**Unit 1. Protection of devices and digital content**	**U1LO1**. The learner is able to identify physical and virtual risks associated with technology	The learner groups multiple risks into 3 physical and 3 virtual.
		U1LO2. The learner is able to implement the strategies to prevent risks and updates him/herself in this matter	The learner describes a strategy to prevent being compromised
		U1LO3. The learner is able to install an antivirus	The learner installs an anti-virus on a virtual machine
		U1LO4. The learner is able to protect him/herself from fraud by using secure passwords.	The learner identifies the secure passwords from a list of many passwords
		U1LO5. The learner is able to protect different vulnerable devices from digital threats (malwares, virus…)	The learner identifies which are vulnerable devices and the mechanisms for their protection
		U1LO6. The learner is able to identify sensitive/valuable information and sectors prone to attack	The learner identifies sensitive data and variations of attacks depending on sectors
	Unit 2. Protection of personal data and digital identity	**U2LO1**. The learner is able to adequate behaviour in the digital world and manage his/her digital trace properly	The learner knows GDPR The learner describes how google analytics work The learner understands and explains the concept of a digital footprint
		U2LO2. The learner is able to identify the perils of getting stolen or missused his/her digital identity by others.	The learner identifies scenarios where their data could be mis-used The learner describes the term "identity theft" and values the risk of it happening
		U2LO3. The learner is able to protect information relative to other people from his/her environment (as a worker, as a friend…)	The learner identifies techniques used to protect PII
		U2LO4. The learner is able to find, erase and/or modify information on-line about him/herself.	The learner explains how to erase/modify PII being kept with an organisation The learner collates his/her digital footprint.
		U2LO5. The learner is able to manage his/her own digital trace.	The learner manages his/her digital footprint
		U2LO6.The learner is able to act in a critical way when sharing information on-line about him/herself.	The learner demonstrates appropriate audit techniques when sharing PII on-line
		U2LO7.The learner is able to make use of multiple digital identities, addressed to different objectives.	The Learner creates multiple social media accounts, and differentiate them for work versus personal.

Profile 2	Unit 3. Information security management and regulations	**U3LO1**. The learner is able to understand the importance of information security and its significance for the organisation	The learner explains clearly which the organisation's information security guidelines are. The learner suggests improvements to provided guidelines.
		U3LO2. The learner is able to identify basic laws, regulations and ethic principles of cybersecurity and information security instructions (for example GDPR and ISO 27 000)	The learner identifies core concepts, regulations and procedures of information security and cybersecurity. The learner applies regulations related to information security.
		U3LO3. The learner is able to plan his / her own work based on work place information security instructions	The learner works applying information security instructions
		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 learner explains the possible consequences of breaking confidenciality.
		U3LO5. The learner is able to implement staff safety training: security guidelines, control and monitoring	The learner prepares a short set of instructions on information security for an organisation or a group of organisations' personnel.
	Unit 4. Information security as part of organisations' security practices	**U4LO1.** The learner is able to observe, assess, prevent and report information risks in work place	The learner names the data security threats and risks faced in his/her daily work. The learner applies measures to ensure data protection.
		U4LO2. The learner is able to utilise organisation's security systems in relation with information security	The learner uses organisation's security systems in relation with information security.
		U4LO3. The learner is able to manage physical security in the premises	The learner identifies different physical security situations in the organisation.
		U4LO4. The learner is able to work safely in mobile and cloud services	The learner applies measures to work safely in a virtual environment
		U4LO5. The learner is able to ensure material and data storage and protection	The learner stores and protect material and data.
		U4LO6. The learner is able to apply basics of software safety: operating systems, applications	The learner uses safely personal devices and applications
	Unit 5. Introduction to cyber security defense	**U5LO1**. The learner is able to identify critical information from different media	The learner compares and analyses critically information acquired from different media, identifying that most vulnerable
		U5LO2. The learner is able to assess the vulnerability of critical infrastructure for society	The learner identifies vulnerabilities of the critical infrastructure in the society
		U5LO3. The learner is able to identify cyber attacks and threats	The learner lists common cyber attacks and threats that are prone to happen taking into consideration the information managed at his/er work

Profile 3	**Unit 6. Basic knowledge of the relation between IT & OT**	**U6LO1.** The learner is able to differentiate IT versus OT	The learner distinguishes IT and OT in terms of availability, integrity and confidenciality
		U6LO2. The learner is able to understand basic knowledge of networking (cisco,hp)	The learner defines basic networking, what is routing/switching or portforwarding.
		U6LO3. The learner is able to identify the main threats and effects of a cyber attack in an industrial environment.	The learner identifies at least 3 threats and their possible effects and consequences in an industrial environment.
		U6LO4. The learner is able to describe the main Information Security Standards in IT	The learner identifies and briefly describes at least these standards: ISO 27001, COBIT, NIST and SANS
		U6LO5. The learner identifies the main security standards related to OT	The learner identifies and briefly describes at least 3 of these standards: IEC 62443/ISA99, NIST 800 82, NIST 800 53, NERC CIP, CyberEssentials, NISTIR7228
		U6LO6. The learner is able to identify some security measures in industrial processes	The learner describes what segmentation is and identify at least 2 industrial firewalls
		U6LO7. The learner is able to identify which are the main components and common protocols in OT	The learner identifies and describes at least 3 of these protocols: PLC, SCADA, HMI, MES, MODBUS, PROFINET
	Unit 7. Company procedures and machines	**U7LO1.** The learner is able to name and describe the levels in the industrial process.	The learner names and describes the levels in the industrial process in a given scenario.
		U7LO2. The learner is able to apply company procedures, detecting possible problems and informing a specialist about any security issues.	The learner applies the procedure when a breach in security is detected. The learner communicates with a specialist in IT with clarity and in an understandable way.
		U7LO3. The learner is able to detect malfunction in the machine or breaches in the machine security.	The learner explains 3 examples of possible breaches in machine security and how to act.
		U7LO4. The learner is able to identify the risks of plugging in random USB in a company network/machines/computers	The learner explains why you must not plug in random usb sticks the risks of plugging in usb sticks and how to prevent it.
		U7LO5. The learner is able to read out a network monitoring tool to detect unusual network traffic.	The learner uses a monitoring tool (like wireshark) to read out a network traffic list, assessing if there are any abnormalities. The learner communicates possible threads to a security specialist in a clear way and applying the company´s protocol.
		U7LO6. The learner is able to understand networking protocols routing/vpn/PF/etc..	The learner explains the basics of networking, not on a ICT level but on a lower level.
	Unit 8. GDPR and data protection	**U8LO1.** The learner is able to identify which are the data protection regulations in his/her country and in Europe.	The learner gives a small summary of the GDPR in his/her own country. The learner looks for relevant information regarding data protection applied to his/her activity, using the right sources.
		U8LO2. The learner is able to work in a secure way with data connected to the diferent kind of machines used at work.	The learner identifies sensitive information which might be susceptible of being affected by data protection regulations.

Profile 4	Unit 9. Penetration test	**U9LO1**. The learner is able to identify and apply the phases of the Audit Process	The phases of the audit process are clearly identified The test is carried out following the phases of the audit process, evaluating and verfying hardware and/or software to determine compliance with defined specifications or requirements
		U9LO2. The learner is able to collect evidences	Scope, infrastructure, resources and data sample size to ensure system requirements are adequately demonstrated. Test data are properly recorded and managed.
		U9LO3. The learner is able to search and exploit vulnerability	Models and simulations to analyse or predict system performance are used. Results of software, hardware or interoperability testing results are correctly analysed. Evaluation of secure interfaces between information systems, physical systems and/or embedded technologies is carried out to search for vulnerability
		U9LO4. The learner is able to do a vulnerability report	Information vulnerabilities and security gaps in architecture are correctly identified. Recommendations based on test results are given in a concrete and clear way
	Unit 10. Management and governance of security	**U10LO1.** The learner knows and understands standards and safety regulations (ISO, ISACA, NIST)	Best practices of IT management by using some well-known framework (e.g. ITIL) are explained. Information security management standards (e.g. ISO/IEC 27001/27002) are applied.
		U10LO2. The learner is able to implement information security governance (ISMS)	The role of information from the strategic viewpoint is explained. Roles & stakeholders in information technology are identified. Business and ICT strategy are aligned. Recommendations on how data is to be managed in the organisation according to its security documentation are given.
		U10LO3. The learner is able to carry out a risk analysis	Vulnerability and threat assessment as part of business impact analysis are carried out. Security documentation based on monitoring results is updated.
		U10LO4. The learner is able to work applying the regulations about personal information (RGPD)	National and international regulations regarding data protection are taken into account
	Unit 11. Security development	**U11LO1**. The learner is able to identify secure programming techniques	Cybersecurity designs for systems and networks are developed or integrated. Secure configuration management processes are employed. Programming is carried out taken into account protection means to minimise intrusion
		U11LO2. The learner is able to develop apps with information delivery (certificates, protocols, signatures)	Apps are developed applying signature-based permissions Access to apps´ content providers is disabled. Apps are developed adding a network security configuration.
		U11LO3. The learner is able to develop apps without data leakage (authorisation & access)	Apps are developed storing private data within internal storage Validity of data is checked
		U11LO4. The learner is able to work according to regulations (ASVS)	The design, development and test of web applications is done observing the Application Security Verification Standards (ASVS)

	regulations (ASVS)	the Application Security Verification Standards (ASVS)
Unit 12. Forensic analysis	**U12LO1**. The learner is able to identify and apply forensic analysis stages	Stages are identified and followed when applying a forensic analysis. Findings are provided in accordance with established reporting procedures.
	U12LO2. The learner is able to clone devices	Sound duplicates of hard drives, floppy diskettes, CDs mobile phones or GPS are created.
	U12LO3. The learner is able to carry out diverse analysis	Analysis of log files, evidence and other information to determine best methods for identifying the perpetrators of a network intrusion is conducted. Information accessed after an intrusion is identified. Network traffic associated with malicious activities is captured and analysed.
	U12LO4. The learner is able to recover information	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.
Unit 13. Perimetral security	**U13LO1**. The learner is able to implement communication security techniques	E-mail and web servers are secured. Firewall for server security is configured. DNS and DHCP server protection is ensured. Security requirements are communicated to other departments in the organisation.
	U13LO2. The learner is able to design and implement a network according to the security model	Potential critical component failures are identified. Actions to mitigate effects of failure are taken. Network connections are encrypted. Wireless networks are protected with encryption and password systems Backup file storing is automated in local or global network and protected from unauthorised use.
	U13LO3. The learner is able to identify authentication and identity management systems (SSO)	The AAA model (authentication, authorisation and accounting) is implemented. VPN policy is managed. Single sing-on systems are integrated to Web and mobile apps.
	U13LO4. The learner is able to identify event management solutions	Main providers of SIEM systems are identified. The best solution matching the organisation needs and budget efficiency is selected.

4. Bibliography

- International Organisation of Standardization. *ISO/IEC 27000:2018* https://standards.iso.org/ittf/PubliclyAvailableStandards/c073906_ISO_IEC_27000_2018_E.zip
- European Digital Competence Framework for Citizens. *DigComp into Action. A user guide to the European Digital Competence Framework.* http://publications.jrc.ec.europa.eu/repository/bitstream/JRC110624/dc_guide_may18.pdf
- National Institute of Standards and Technology. National Initiative for Cybersecurity Education (NICE). Cybersecurity Workforce Framework. 2017. https://nvlpubs.nist.gov/nistpubs/SpecialPublications/NIST.SP.800-181.pdf
- Instituto Nacional de Tecnologías Educativas y de Formación del Profesorado (INTEF). *Marco Común de Competencia Digital Docente*. 2017. https://aprende.intef.es/sites/default/files/2018-05/2017_1020_Marco-Com%C3%BAn-de-Competencia-Digital-Docente.pdf