Stock taking of information security training needs in critical sectors

DECEMBER 2017

About ENISA

The European Union Agency for Network and Information Security (ENISA) is a centre of network and information security expertise for the EU, its member states, the private sector and Europe's citizens. ENISA works with these groups to develop advice and recommendations on good practice in information security. It assists EU member states in implementing relevant EU legislation and works to improve the resilience of Europe's critical information infrastructure and networks. ENISA seeks to enhance existing expertise in EU member states by supporting the development of cross-border communities committed to improving network and information security throughout the EU. More information about ENISA and its work can be found at www.enisa.europa.eu.

Contact

For queries in relation to this paper, please use csirt-relations@enisa.europa.eu
For media enquiries about this paper, please use press@enisa.europa.eu.

ISBN: 978-92-9204-231-8, DOI: 10.2824/521757

Table of Contents

Executive Summary

The European Union's Directive on security of network and information systems (NIS Directive[1]) asserts that "network and information systems and services play a vital role in society", and that the "magnitude, frequency and impact of security incidents are increasing, and represent a major threat". Given that urgency, the NIS Directive goes on to argue that "operators of essential services" need to identify "which services have to be considered as essential for the maintenance of critical societal and economic activities". This is in fact referring to the operators in the so-called critical sectors, with those being: energy, transport, banking, financial market infrastructures, health sector, drinking water supply and distribution, and digital infrastructure.

The protection of these seven critical sectors should have the highest priority, because when they are under threat, the functioning of society itself and the well-being of its citizens are at stake. As part of this effort, it is extremely important to increase the competences of cyber security personnel. This requires the availability of high quality trainings across the board, available to all critical sectors.

Within the critical sectors, there are significant differences regarding the maturity level of cyber security. Therefore, some of the critical infrastructure operators will not be as ready as others, to counter the risks resulting from new cyber security threats in a timely and adequate manner.

With the emphasis that the NIS Directive places on the importance of the seven critical sectors, this study aims to identify the current situation in these sectors in regard to the available cyber security trainings, and if there are any training needs specific to each of the sectors, beyond the generic needs for such trainings.

Over the past years, ENISA has developed a wide range of cyber security trainings, and also delivered the training content to several national and governmental CSIRTs (Computer Security Incident Response Teams) as well as their constituents. The next important question that this study set out to answer is if and how the ENISA training portfolio actually is useful for the seven critical sectors – and what could be done to improve the suitability of that portfolio to the existing training needs.

The main general conclusions are:

- the cyber security training field is extensive and diversified, but does not sufficiently address the issue of raising the cyber security resilience of critical infrastructure: CIP-related trainings are still a niche
- there is a shortage of specialised trainings in the field of ICS/SCADA systems cyber security – which is an essential element in countering operational threats (e.g. in the energy sector)
- there are very few trainings specialising in the specific threats encountered in the different (sub)sectors
- cyber security awareness raising trainings are lagging behind
- there is a shortage of trainings in regard to decision making as a result of data leakages or privacy incidents

[1] http://eur-lex.europa.eu/legal-content/EN/TXT/?uri=uriserv:OJ.L_.2016.194.01.0001.01.ENG&toc=OJ:L:2016:194:TOC

- there is a pressing need for trainings related to GDPR[2], since this will affect every sector, and could have an operational impact on the organization.

As for the fit of ENISA's current training offer to the needs of the seven critical sectors, the study has found that:

- ENISA should present the context of threats and risks related to each sector in the trainings. In particular, dependencies and mutual influence of infrastructures operating in different sectors should be explained, and their possible impact on cyber-security issues concerning e.g. global payments or air traffic control
- ENISA should provide trainings in more local languages
- ENISA should determine whether cyber ranges and gamification based trainings will likely provide a more effective approach than traditional trainings. On-demand training accessibility is gaining in importance.
- ENISA is advised to organise a pilot study in for instance the transport sector to further gauge the results of this study and come to implementable proposals on how to improve the training situation in that sector. This approach may be used for other sectors too.

[2] General Data Protection Regulations

1. Introduction

1.1 General Context

Quoting from the European Union's NIS Directive, "Network and information systems and services play a vital role in society. Their reliability and security are essential to economic and societal activities, and in particular to the functioning of the internal market. The magnitude, frequency and impact of security incidents are increasing, and represent a major threat to the functioning of network and information systems. Those systems may also become a target for deliberate harmful actions intended to damage or interrupt the operation of the systems. Such incidents can impede the pursuit of economic activities, generate substantial financial losses, undermine user confidence and cause major damage to the economy of the Union. Network and information systems, and primarily the internet, play an essential role in facilitating the cross- border movement of goods, services and people. Owing to that transnational nature, substantial disruptions of those systems, whether intentional or unintentional and regardless of where they occur, can affect individual Member States and the Union as a whole. The security of network and information systems is therefore essential for the smooth functioning of the internal market."

Given that urgency, the NIS Directive goes on to argue that "operators of essential services" need to be identified, "which services have to be considered as essential for the maintenance of critical societal and economic activities". This is in fact referring to the operators in so-called critical sectors. These critical sectors are identified in Annex II of the NIS Directive:

1. Energy. Subsectors: Electricity, Oil and Gas;
2. Transport. Subsectors: Air, Rail, Water and Road transport;
3. Banking;
4. Financial market infrastructures;
5. Health sector;
6. Drinking water supply and distribution;
7. Digital Infrastructure.

The protection of these critical sectors should have the highest priority, because when they are under threat, the functioning of society itself and the health and well-being of its' citizens are under threat. Many organisational and technical initiatives have been, and will be launched all over the world, to increase the state of security for these sectors, however all such attempts depend on the people carrying out the security and protection work, and how well they are equipped to do their jobs with high quality. Thus, to increase the competences of cyber security personnel is of paramount importance. This requires the availability of high quality trainings available to all critical sectors.

There is a significant difference in the maturity level of cyber security among sectors. Therefore, it is reasonable to assume that some of the critical infrastructure operators will be less prepared than others to timely and adequately counter the risks resulting from new IT/OT[3] threats. This has been illustrated by:

[3] Information Technology/Operation Technology

- WannaCry (impacted the health sector, but was also spread widely)
- NotPetya (not sector specific)
- Attacks on power plants in the energy sector
- Ongoing attacks on the banking sector using phishing and Trojan Horses
- The increasing number of leakages of sensitive data in the health sector.

With the emphasis that the NIS Directive rightfully places on the importance of the identified critical sectors, it is therefore relevant to find out what the situation is in regard to available cyber security trainings, and if there are any training needs specific to each of the sectors, beyond the generic need for such trainings.

ENISA has developed a wide range of cyber security trainings, with emphasis on cyber security incident response teams (CSIRTs), offering training courses where the commercial market may fail to provide them. The full set of training material and supporting tools are freely available for download on ENISA's website. Once the market comes up to speed with the training being offered, ENISA focuses on other 'untapped' trainings. Moreover, ENISA uses a 'train the trainer' approach in order to be able to provide a more scalable solution. This study asks to what extent is cyber security training available to various sectorial players and to what extent ENISA's training portfolio meeting to the critical sectors' demand – and what could be done to improve on the identified shortcomings of the present portfolio.

1.2 Objective and Scope

The primary objective of this project is to provide a mapping of ENISA's training program and a strategy to adapt it in the light of the recently adopted EU NIS Directive, catering for the needs of the identified critical sectors.

The project provides a structured report based on relevant training/education initiatives, stakeholders' input, ENISA reports, and other relevant material.

The primary target audience is ENISA and the NIS Directive sectors. The secondary target audience are decision making bodies in Member States and EU organisations, responsible for the cyber security agenda for the sectors impacted by the NIS Directive.

1.3 Methodology

In order to achieve the objectives, the following methodology was adopted:

1. Stock taking by means of desktop research of existing cyber security initiatives (public and private) in all seven critical sectors, and see what specificity there is in relation to the sectors
2. Identify training needs for each of the seven critical sectors, by means of reaching out to relevant stakeholders, starting from IT/OT threats that are relevant for these sectors
3. Finally, by means of desktop research:
    a. Map ENISA's portfolio of cyber security trainings to the identified sectoral needs
    b. Identify gaps in ENISA's portfolio compared with the critical sectors
    c. Propose ways how ENISA's portfolio can better help all seven critical sectors to increase their cyber security training level.

2. Overview of Cyber Security Training Initiatives

2.1 Information Sources

The approach to take stock of existing cyber security initiatives in the seven critical sectors identified in the NIS Directive was as follows. The first step of the research process was the preparation of a list of public and private institutions together with CSIRT teams that offer cyber security training. In this context, more than 50 institutions and 15 CSIRTs providing trainings were identified, and their training information was harvested mostly by means of web research, and additionally by means of e-mail queries and an online questionnaire.

To identify which cyber security trainings from the offer could more specifically address sectoral needs, web research was used. However, when checking the websites of these organisations, two impressions emerged:

- the number of trainings offered by renowned training institutions was often very high, without any clear specificity as to target audience or scope being offered – so it is in many cases not straight forward to determine to what extent the trainings are useful for specific sectors
- in a number of cases, the information found on training organisations' websites seemed to be either not regularly updated or incomplete. In these cases, training vendors and CSIRTs were contacted via e-mail, to obtain more accurate and up-to-date information.

Thus, queries were sent to vendors and CSIRTs asking them individually about their cyber security related trainings, and to provide some specificity inasmuch as specific trainings meet the needs of the 7 critical sectors. An online questionnaire was put at their disposal in order to facilitate the information acquisition process. The training offer of those organizations who did not respond to the queries sent out, was harvested based only on the information available on the web.

2.2 Results of Taking Stock of Trainings

This section presents a summary of the results from the stock taking of existing training initiatives. The collection of cyber security training include two inputs: from questionnaires and from desktop research. It should be noted that it is not exhaustive of all available trainings/institutions in the market. The obtained trainings collection is presented in two tables (see Appendix B) that contain the detailed information about trainings as in Table 1. training list is non-exhaustive. The structure of this table reflects the information that was collected using a questionnaire.

Table 1: Contents of the Training Tables (from questionnaires/desktop research)

#	ITEM	DESCRIPTION
1	Organizer (Ownership)	Name of the training organiser with information about its origin (public / private)
2	Training Title	Name of a training
3	General Description	Short description of a training, including information about its content and scope
4	Skills Level	Level of required skills before signing up for a training (Beginner / Intermediate / Advanced)
5	Training Method	Information about trainings methods (more hands-on / more theoretical)

6	Target Audience	A type of a participant for which a training is dedicated (Non-technical Employees / OT Security Specialists / IT Security Specialists / Security Managers / Top Management)
7	Cyber Range Simulator	Information whether a training is supported with a Cyber Range Platform
8	Topic Relevance	Information on how much a training is relevant to a particular topic (e.g. IDS, Mobile Security, Data Privacy, ICS/SCADA Security)
9	Sector Relevance	Information on how much a training is relevant for a particular critical sector
10	Availability	Information on how training is available (online / live - on vendor's /or client's side)
11	Accessibility	Information on how training is accessible (on demand / on register)
12	Location	Place(s) where a training is organized
13	Duration	Information on how long a training takes
14	Materials	Additional materials (training manual / exercises book / presentation)
15	Certificate	Name of the training certificate (if available)
16	Training Category (Taxonomy)	Training category – see trainings taxonomy (Table 2)

From questionnaires, ENISA received 57 trainings records from 15 organisations, and from desktop research, 29 records from 16 organisations. The details for both cases can be found in Appendix B. The main findings about all the collected trainings are listed in Subsection 2.3. However, for the purpose of analysis and conclusions, it should be mentioned that information collected in the process of desktop research, is considered to be not as accurate, up-to-date and complete, as the information provided directly by vendors. Therefore, the following analysis and the resulting conclusions are based mainly on the set of trainings collected through questionnaires.

For convenience, the collected trainings are sorted in training tables according to the taxonomy presented in Table 2.

Table 2: Trainings Taxonomy

#	TYPE OF TRAINING CATEGORY	CATEGORY DESCRIPTION
1	Cyber Security Foundations	Under this category basic cyber security trainings were concerned, such as threat landscape, authentication issues, malware types, cryptography and network security.
2	Audit/Penetration Testing/Ethical Hacking	Under this category trainings related with security audits, penetration testing and ethical hacking were concerned.
3	Monitoring	Under this category trainings related with network monitoring, Intrusion Prevention & Detection systems and Security Information & Event Management (SIEM) were concerned.
4	CSIRTs/Incident Response	Under this category trainings related with Computer Security Incident Response Teams (CSIRT) activity, incident handling and management were concerned.

5	General Cyber Security	Under this category general cyber security trainings were concerned, which are not particularly connected to the specific areas of cyber security.
6	ICS/SCADA Security	Under this category trainings related to critical infrastructure protection are concerned, such as security of SCADA, ICS, PLC and other cyber-physical devices.

2.2.1 Geographical Availability of Trainings

The present study was not set-up to derive a complete list of available trainings. That being said, the following categories have been recognised in regard the geographical availability of trainings:

(i) Online, available worldwide;
(ii) On location on demand, potentially available worldwide and certainly inside the EU;
(iii) On vendor allocated locations – these can also vary if the vendor supports "training tours" (e.g. TRANSITS, SANS). These are available in many locations in the EU – and outside, of course.

Categories (i) and (ii) are available to all of the EU member states. For category (iii) the coverage of this research is the least complete, as a survey of all 28 Member States was not intended – also taking into account the language factor. Here a sample set was taken – English, Dutch, German and Polish.

In Appendix B the geographical availability of trainings is part of the listing of all trainings.

2.3 Summary of Findings

When analysing the training collection, the main findings and conclusions are as follows:

- Most of the available training initiatives are not dedicated to specific sectorial needs but apply to all sectors. Only ICS/SCADA security trainings cover specific needs for three sectors (energy, transport, drinking water supply and distribution) as they concern OT threats.
- Some of the available trainings vendors' offers, are exactly the same in sense that they are either approved or organized in partnership with renowned training centres.
- In some cases, the course material of one course may overlap with that of another, but then the appropriate information appears in the course description ("Course Content Overlap Notice").
- A majority of 44 out of 57 trainings is provided by private vendors.
- Only 19 out of 57 trainings are not available as online trainings.
- Most of the trainings can be conducted live at clients' premises.
- Vendors are cautious with implementing tools for trainings; e.g. just 14 out of 57 trainings are conducted with the support of cyber platforms.
- The majority of the training courses span over 5 days.
- A majority (40 out of 57) of the available trainings has a "hands-on" factor of at least 50%.

3. Critical Sectors Trainings Needs

3.1 Information Sources and Findings

The next step of our research aimed to identify specific trainings needs for critical sectors. A starting point included sending a survey and conducting interviews with sectorial stakeholders (included in Appendix A). Questions asked in a survey and during interviews concerned two aspects:

- Type of the sector;
- Type of training needs in that particular sector.

Stakeholders' opinions that were obtained in regard to their sectors can be summarised as follows:

- Sectors that need special trainings are especially those which use ICS/SCADA which also increasingly include Internet of Things (IoT) based solutions: energy, transport, drinking water supply and distribution.
- Energy sector (electricity): the connectedness of the grids across Europe necessitates close cooperation also on the incident response level. Relevant trainings are welcome.
- Energy sector (oil & gas): traditional focus on physical security, and cooperation inside the sector. More openness needed across the sectors. Relevant trainings are welcome.
- Transport (air): new threats emerging with the Internet-of-Things. It is not evident that this is covered adequately. The minimum requirement is for awareness trainings.
- Banking & financial markets sector: there is a significant need for malware analysis trainings.
- Banking sector: there is a need for security awareness initiatives for customers (both businesses and the general public). It is recognised that this is not easy to put into trainings.
- Health sector: there is a gap between the frontrunners – such as university hospitals are – who are advanced in cyber security and have a high level of training on the one hand – and on the other hand smaller hospitals or small practices in all countries, where the knowledge and experience in this field is often very limited.
    - As all are part of the same chain and are increasingly exchanging sensitive data, there is a dire need to close this gap. Trainings of various kinds, starting with awareness, should be part of this effort.
- Digital infrastructure: especially from the CSIRT perspective, the most needed trainings are for raising awareness and incident management.

Among more general conclusions resulted from interviews are the following:

- It is very important to adjust a training to the maturity of the participants/organisations.
- Local trainings in local languages are very important. They ensure better communication and problem understanding.

3.2 Identification of Threats Related to Critical Sectors

After consulting the critical infrastructure protection practitioners, it was decided to conduct additional research to further clarify the picture of the cyber security threat landscape of the critical infrastructures. This step assumed that the identification of specific threats related to particular sectors, by doing desktop research, to enable supplement the experts' point of view and in result more fully determine the needs for the cyber security trainings in these sectors.

The initial observation from taking stock of existing training initiatives (Section 2.2) is that very few of the available training programmes are dedicated to particular sectors. It was then confirmed when we started gathering trainings information directly from the vendors. All of the contacted vendors claimed that the trainings they have in their offers are – with a very few exceptions – relevant to all critical sectors identified in the NIS Directive. The only major difference here concerns those sectors, which uses Operation Technology systems, i.e. Energy, Transport and Water Supply sectors.

It was also found that differences in the context of cyber security among sectors actually lie in the various threats vectors. Indeed, there are threats strongly linked to some sectors and less to others. To give an example, Distributed Denial of Service (DDoS) attacks are a much bigger concern in the Digital Infrastructure sector than in some of the other sectors, due to the fact that eveb short periods of downtime can have significant business implications. However, the way the attack is executed is technically the same. On the other hand, one must also consider interdependencies among sectors and their security implications. For example, a DDoS attack in Digital Infrastructure may impact an e-Health application.

The above observations led to an approach in which for the purpose of threats identification related to sectors, the group of sectors were divided into two following subgroups:

- **ICS(Industrial Control Systems)-based** sectors: energy, transport, drinking water supply and distribution sectors,
- **Non-ICS-based** sectors: banking, financial market infrastructure, and digital infrastructure sectors.

While ENISA has developed in the past sectorial threat models, for the purpose of this study it was more efficient to use a smaller scheme, that can be correlated to specific potential training topics. All the critical sectors, ICS-based and non-ICS-based have related IT threats, but it could be assumed that OT threats are relevant only to sectors from the ICS-based sectors; thus, to provide a more structured approach, separate groups of specific OT/IT threats and shared IT threats are considered. The identified collection of IT and OT threats related to sectors are included in Table 1. The identification of a complete and comprehensive list of threats for each sector is outside the scope of this work. However, the categorisation below, even though it is non-exhaustive, should provide enough information to facilitate the mapping of threats to specific sectorial training needs.

Table 3: Threats (OT & IT) related to seven critical sectors identified in NIS Directive.

SECTOR	SPECIFIC OT & IT THREATS		SHARED IT THREATS
	OPERATIONAL TECHNOLOGY THREATS	INFORMATION TECHNOLOGY THREATS	
Energy	Vulnerabilities of ICS components (HMI, IoT, electric devices, SCADA systems) Unpatched components Utilizing of outdated and obscure components Outsourcing of the third parties to manage and maintain the ICS architecture	Smart grids security threats: Malware exploits Privacy Infringement Identity theft Compromising of communication equipment Web applications attack Vulnerabilities in Mobile Applications and payment interfaces	Unpatched & outdated software Low awareness Lack of incident reporting Lack of Information sharing Insider threats

	Remote access to the corporate network Utilizing external servers for critical infrastructure architecture Integration of IT and OT networks	Data Confidentiality, Integrity and Availability Eavesdropping and traffic analysis Distributed Denial of Service (DDoS) Social Engineering	Advanced Persistent Threats (APT) Distributed Denial of Service (DDoS)
Transport		POS intrusions Social Engineering Eavesdropping and traffic analysis Insider threats Vulnerabilities in Mobile Applications and payment interfaces Miscellaneous errors Denial of Service (DoS)	
Drinking Water Supply and Distribution		Lack of protective monitoring	
Banking		Vulnerabilities in Mobile Applications and payment interfaces	
Financial Market Infrastructures	OT not applicable	Vulnerabilities in automated machines (ATMs, cashier machines, POS intrusions) Web applications attack Data Confidentiality, Integrity and Availability Social Engineering Identity theft	
Health		Identity theft Large-scale attacks on IoT (medical devices) Malware exploits Privacy Infringement Advanced Persistent Threats (APT) Intellectual property theft Web applications attack	
Digital Infrastructure		Distributed Denial of Service (DDoS) Denial of Service (Dos) DNS Cache Poisoning DNS Spoofing Cybersquatting Typosquatting	

3.3 Mapping Threats into Trainings

Having collected the threats related to critical sectors (Table 3), the following approach for mapping identified threats into cyber security trainings is proposed. This methodology is based on the assumption that threats identified in sectors can be associated with one or more training types[4] (for training topics see Table 4). Applying the following scoring methodology identified what types of trainings are less or more needed in particular sectors. In general, this methodology assesses for each identified threat, and its' relevance to a particular training. The following examples provide a better understanding of the entire mapping process:

- if *privacy protection* threat is identified within a particular sector it scores 1 point under *General Data Protection* training and 1 point under *Data Security* training,
- if *malware exploits* threat is identified within a particular sector it scores 1 point under *Malware Analysis* training, 1 point under *Forensic Analysis* training, 1 point under *Threat Intelligence* training, 1 point under *Incident Response* training and 1 point under *Intrusion Prevention and Detection* training,
- if *vulnerabilities of ICS components* threat is identified within a particular sector (in this case it is identified within all OT sectors: energy, transport and water supply) it scores 1 point under *ICS/SCADA Security* training and 1 point under *Vulnerability Assessment* training.

After completing the above mapping process for each threat identified, the four-level scale to evaluate the need of a particular type of training in every sector was proposed. The scale is as follows:

- **0 – not relevant** – the training is very loosely related to the sectorial need,
- **1 – good to have** – the training is the part of the good practice for cyber security management process but not specifically related to the sector,
- **2 – should have** – the training is the part of the good practice for cyber security management process and an organization should not avoid it,
- **3 (3+) – must have** – the exercise is crucial for organising a proper cyber security management process. It includes specific material for the sector.

To conclude the whole above process, the more points the training received after mapping, the more emphasis should be put in the implementation of such a training in a particular sector. In some cases, for e.g. ICS/SCADA Security trainings in the energy sector, there are more points than 3 which suggests even stronger urgency regarding implementation of such a training.

The results of the above mapping process are presented in Table 4.

[4] In cases where a threat could not be associated with a certain training type, it would probably indicate the need to add appropriate training.

Table 4: Results of mapping threats related to critical sectors into cyber security trainings

TRAINNG TOPIC	ENERGY	TRANSPORT	DRINKING WATER SUPPLY AND DISTRIBUTION	BANKING AND FINANCIAL MARKET INFRASTRUCTURES	HEALTH	DIGITAL INFRASTRUCTURE
Communication (team exercises)	1	1	1	1	1	1
Awareness Raising	3	3+	2	3	2	3+
General Data Protection	2	0	0	2	3	0
Vulnerability Assessment	2	2	1	1	0	0
Identity & Access Management	1	1	1	0	0	0
Malware Analysis	1	0	2	0	1	0
Network Analysis	2	2	2	0	2	0
Web App Security	3	2	1	3	2	1
Data Security	3	2	2	3	3	1
Cloud Security	1	1	1	0	0	0
Wireless Security	2	1	1	0	0	0
Forensics Analysis	1	0	0	0	1	0
Device & Endpoint Security	2	3	2	3	1	1
ICS/SCADA Security	3+	3+	3+	0	0	0
Threat Intelligence	1	0	1	0	1	0
Intrusion Prevention & Detection	2	1	1	0	1	0
Incident Response Management	3	2	2	2	2	2
Security of the Chain Supply	1	1	0	2	0	0
Security of the Outsourcing	1	1	1	0	0	0
Protection against APT	1	1	1	1	3	2
Protection against DDoS attacks	2	2	1	1	2	3
Protection against Insider threats	1	2	1	1	1	2

3.4 Summary of Findings

The main findings from the desktop research related to sectors' trainings needs are as follows:

- The finance, digital infrastructure, and energy sectors appear to have significantly high incident costs. This can be regarded as an argument to treat these sectors with extra attention in terms of training.
- The energy, transport, drinking water supply and distribution sectors have similar Operation Technology risks. Such risks are related to cyber security threats to ICS systems and include: HMI (Human-Machine Interfaces), IoT, electric devices and SCADA (Supervisory Control and Data Acquisition) systems. This means that trainings should be available focusing on these topics.
- ICT systems increased interdependencies between all critical infrastructure sectors and in result these sectors share similar IT threats. One example is the banking and financial infrastructure sectors that share very similar threats concerning data protection and privacy.
- New security challenges arise as systems are becoming more interconnected, integrating more and more digital technologies and increasingly use data to deliver higher capacity and performance. These systems were designed to maximize efficiency and functionality, not security.
- The lack of awareness of the potential severity of malicious cyber security attacks in every sector is the gravest concern. Awareness raising trainings are thus of great importance in all sectors. It is important to notice that these kind of trainings are mainly dedicated for ordinary staff, and only partially for cyber security specialists.
- The Social Engineering threat concerns all sectors, but is particularly important in digital infrastructure sector due to the wide spectrum of this type of attacks (e.g. DNS Cache Poisoning, DNS Spoofing, cybersquatting, typosquatting).
- ICS systems are not only at risk from current vulnerabilities which target standard business networks, such as malware, denial-of-service and user error, but also from specific vulnerabilities which target the unique characteristics inherent in these systems as e.g. the use of advanced technology in transport sector, such as 4G/LTE networks mixed with legacy systems.
- New factors influence the cyber threat landscape: shadow IT, mobile and flexible working, bring own devices (e.g. infected USB drives), IoT (Internet of Things). IoT threats are becoming increasingly important, especially in the context of the health sector and smart cities – the concept increasingly applied in the transport sector.
- The risks associated with ransomware cannot be underestimated. Unfortunately, recent cases ("WannaCry", "NotPetya") have proven that this kind of malware is not always targeted to specific sectors and can paralyse a significant part of the critical infrastructure.
- Desktop research (identification of specific threats related to critical sectors) led to expanding of the training catalogue with additional trainings such as: security of the chain supply, security of the outsourcing, protection against APT, protection against DDoS attacks, protection against insider threats. Insider threats especially are a complex area, and are only partially technical in nature – psychology and how staff is treated and managed all come into play here: how to create a work environment that minimises these risks.
- Vulnerability assessment, risk and threat management are of significant importance for all critical sectors.
- Information on breaches in critical sectors is confidential and therefore often difficult to obtain. This is a significant problem as sharing information about cyber security and incidents reporting is of great importance when addressing cyber security. It is not trivial to address by means of trainings,

but one way could be to share success stories of information sharing[5] and explain how it is possible to share information without breaching confidentiality. This also includes training people in such concepts as TLP – the Traffic Light Protocol – which was designed for purposes like this.

- Trainings curricula should include for each sector context information and present direct consequences of IT/OT security threats by e.g. presenting real examples of incidents. This will improve understanding of cyber security threats in particular sectors.

[5] Like in the financial sector in some countries, or the CSIRT community, and vendors who exchange security information while competing in the commercial area.

4. Mapping ENISA CSIRT Trainings into Critical Sectors Needs

4.1 Mapping Methodology

The aim of this section is to provide an insight and evaluation of ENISA's trainings availability in the context of cyber security and critical sectors identified by the NIS Directive. The results should lead to a better adaptation of the ENISA offer to sectorial training needs. To provide such an evaluation, the methodology of mapping of ENISA's trainings material[6] to the training needs (identified in Section 3.3) of all sectors was proposed. A similar scoring methodology as above was used, but here for each cyber security topic (see Table 4), the ENISA trainings catalogue was searched, identifying any ENISA's training that is related to this topic. For example, the topic "Protection against APT" is covered by three trainings offered by ENISA and such a training type scores 3 points under "ENISA's trainings availability" column (see Table 5). The identified ENISA trainings are listed in the same column.

Having identified numbers of relevant ENISA's trainings for each cyber security topic and comparing them with the numbers of previously identified cyber security trainings needs in sectors (for both see Table 5), it is possible to make trainings gaps analysis and identification that are presented in details in the next sections.

[6] https://www.enisa.europa.eu/topics/trainings-for-cybersecurity-specialists/online-training-material

	ENISA' TRAININGS AVAILABILITY		ENERGY	TRANSPORT	DRINKING WATER SUPPLY AND DISTRIBUTION	BANKING AND FINANCIAL MARKET INFRASTRUCTURES	HEALTH	DIGITAL INFRASTRUCTURE
Communication (team exercises)	• *Incident Handling Management* • *Establishing External Contact* • Incident handling in live role playing • Cooperation with Law Enforcement Agencies - Advising in Cyber Crime Cases • Assessing and Testing Communication Channels with CERTs and all their stakeholders • Cooperation in the Area of Cybercrime	6	1	1	1	1	1	1
Awareness Raising	Lack of dedicated trainings	0	3	3+	2	3	2	3+
General Data Protection	Lack of dedicated trainings	0	1	0	0	2	2	0
Vulnerability Assessment	• *Vulnerability handling*	1	2	2	1	1	0	0
Identity & Access Management	Lack of dedicated trainings	0	1	1	1	0	0	0
Malware Analysis	• *Processing and storing artifacts* • *Artifact analysis fundamentals* • *Advanced artifact handling*	7	1	0	2	0	1	0

	• *Introduction to advanced artefact analysis* • *Dynamic analysis of artefacts* • *Common framework for artefact analysis activities* • *Static analysis of artefacts*							
Network Analysis	• *Network forensics* • *Forensic analysis: Network Incident Response* • *Digital forensics*	3	2	2	2	0	2	0
Web App Security	• *Forensic analysis: Webserver Analysis*	1	3	2	1	3	2	1
Data Security	Lack of dedicated trainings	0	3	2	2	3	3	1
Cloud Security	• *Incident handling in the cloud*	1	1	1	1	0	0	0
Wireless Security	Lack of dedicated trainings	0	2	1	1	0	0	0
Forensics Analysis	• *Forensic analysis: Local Incident Response* • *Forensic analysis: Network Incident Response* • *Forensic analysis: Webserver Analysis* • *Digital forensics* • *Network forensics*	5	1	0	0	0	1	0
Device & Endpoint Security	Lack of dedicated training	0	2	3	2	3	1	1
ICS/SCADA Security	• Incident handling during an attack on Critical Information Infrastructure	1	3+	3+	3+	0	0	0

Threat Intelligence	Lack of dedicated trainings	0	1	0	1	0	1	0
Intrusion Prevention & Detection	• *Presenting, correlating and filtering various feeds* • *Developing Countermeasures* • *Using indicators to enhance defence capabilities* • *Proactive incident detection*	4	2	1	1	0	1	0
Incident Response Management	• Automation in incident handling • Incident handling during an attack on Critical Information Infrastructure • Large scale incident handling • Incident handling management • Incident handling and cooperation during phishing campaign	5	3	2	2	2	2	2
Security of the Chain Supply	Lack of dedicated trainings	0	1	1	0	2	0	0
Security of the Outsourcing	Lack of dedicated trainings	0	1	1	1	0	0	0
Protection against APT	• Advanced Persistent Threat incident handling • Social networks used as an attack vector for targeted attacks • Incident handling during an attack on Critical Information Infrastructure	3	1	1	1	1	3	2

Protection against DDoS attacks	Lack of dedicated trainings	0	2	2	1	1	2	3
Protection against Insider threats	Lack of dedicated trainings	0	1	2	1	1	1	2
Mobile Application Security	• Mobile threats incident handling • Mobile threats incident handling (Part II)	2	2	2	1	2	1	1

Table 5: Results of mapping cyber security trainings needs in critical sectors into ENISA's trainings' catalogue

4.2 Gap Analysis and Evaluation Results

4.2.1 General Overview of ENISA's Trainings Availability Concerning Critical Sectors Needs

In this section, the outcome and conclusions from trainings gaps analysis is presented, resulting from the mapping methodology, as introduced in the previous section. Figure 1 shows the current ENISA's availability of cyber security related trainings.

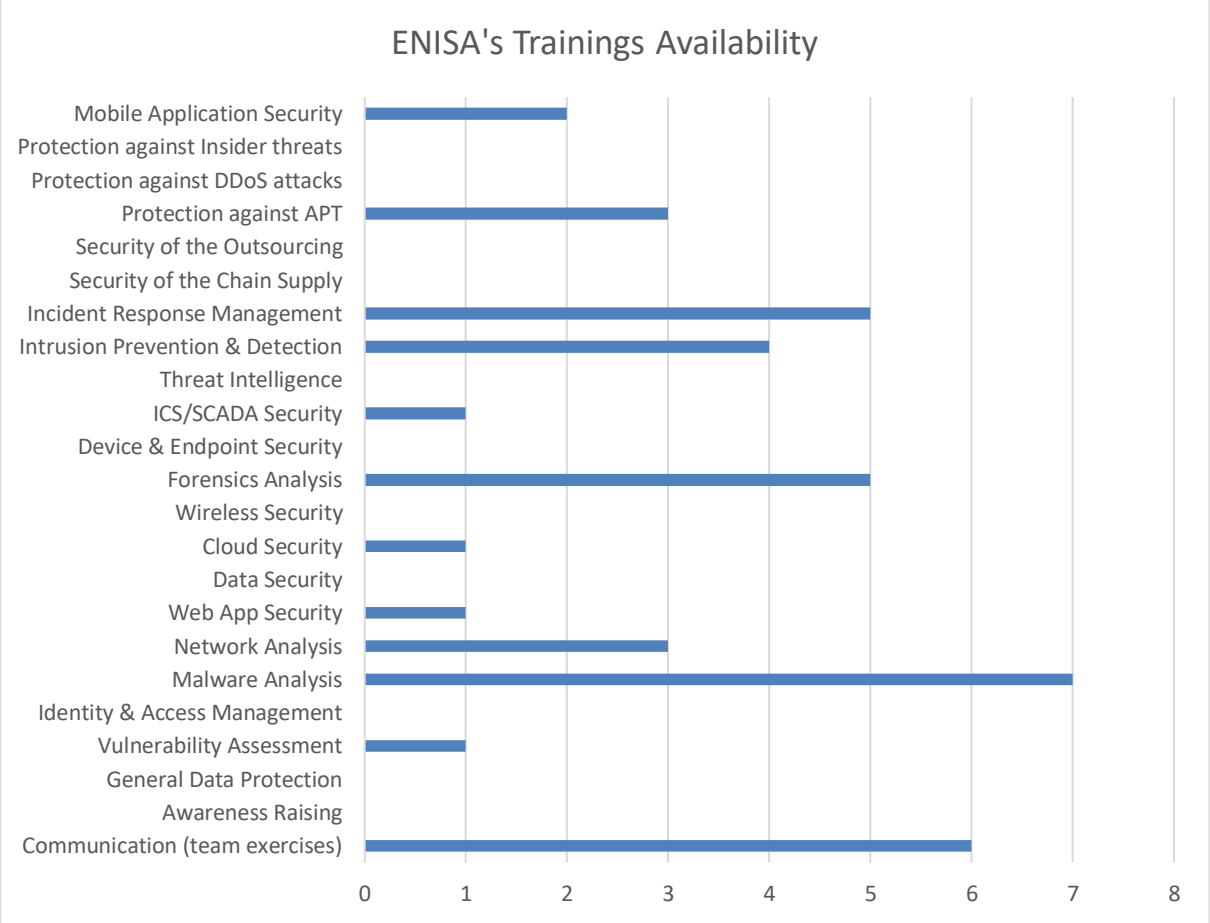

Figure 1: ENISA's trainings availability

The availability of ENISA's cyber security related trainings in the context of critical sectors needs can be summarized as follows.

- ENISA offers a wide spectrum of trainings regarding *Malware Analysis* on different levels of advancement.
- ENISA specialises in trainings relevant to *Incident Response Management* and the examples of trainings listed in Table 3 are only examples. Thus, all critical sector needs in terms of *Incident Response Management* should be met and there is no urgent need for ENISA to introduce more such trainings.
- Although, it might seem like ENISA does not provide trainings strictly dedicated to *Device & Endpoint Security* or *Data Security*, it should be noted that a part of this knowledge is provided across a number of trainings.
- When it comes to the *Communication (Team Exercises)* training, the two presented in the ENISA offer (*Incident Handling Management*, *Establishing External Contacts*) include only some of the elements

regarding communication exercises. There are no exercises specializing in communication between team members.

- The only training connected with *Vulnerability Assessment* is dedicated to the CSIRTs incident handlers and managers.
- The only training connected to the *Cloud Security* is dedicated to the CSIRTs incident handlers and managers.
- ENISA does not provide dedicated trainings concerning: *Awareness Raising, General Data Protection, Identity & Access Management, Wireless Security, Threat Intelligence, Security of the Outsourcing, Security of the Chain Supply, Protection from the DDOS attacks, Protection from the Insider Threats*. It does not mean that elements of these topics are not included in the offer at all, but the emphasis is put on other good practices, primarily: *Artefact Analysis, Incident Handling and Forensics Analysis*.
- Apart from the above-mentioned trainings, the low number of *ICS/SCADA Security* trainings (only 1, and basic) is a point of attention, especially when cyber security of critical sectors utilizing operation technologies are concerned (Energy, Transport and Water Supply sectors).

The gaps analysis and evaluation presented above provide a general overview of ENISA's trainings availability concerning critical sectors' needs. The proposed adaptation of ENISA's training material to trainings needs for a chosen sector (Transport Sector) will be analysed in detail in the following subsections.

4.2.2 Gap Analysis for the Transport Sector

The process of identification of critical sectors' needs showed a high demand of various types of cyber security trainings in these areas. Focusing on one of the sectors, the gap analysis between ENISA's trainings catalogue and this sector training needs is presented, suggesting the broadening of ENISA's existing training material to better suit the sector's needs. The chosen sector is the Transport sector. The gap analysis is presented in Figure 2 and analysed in details below.

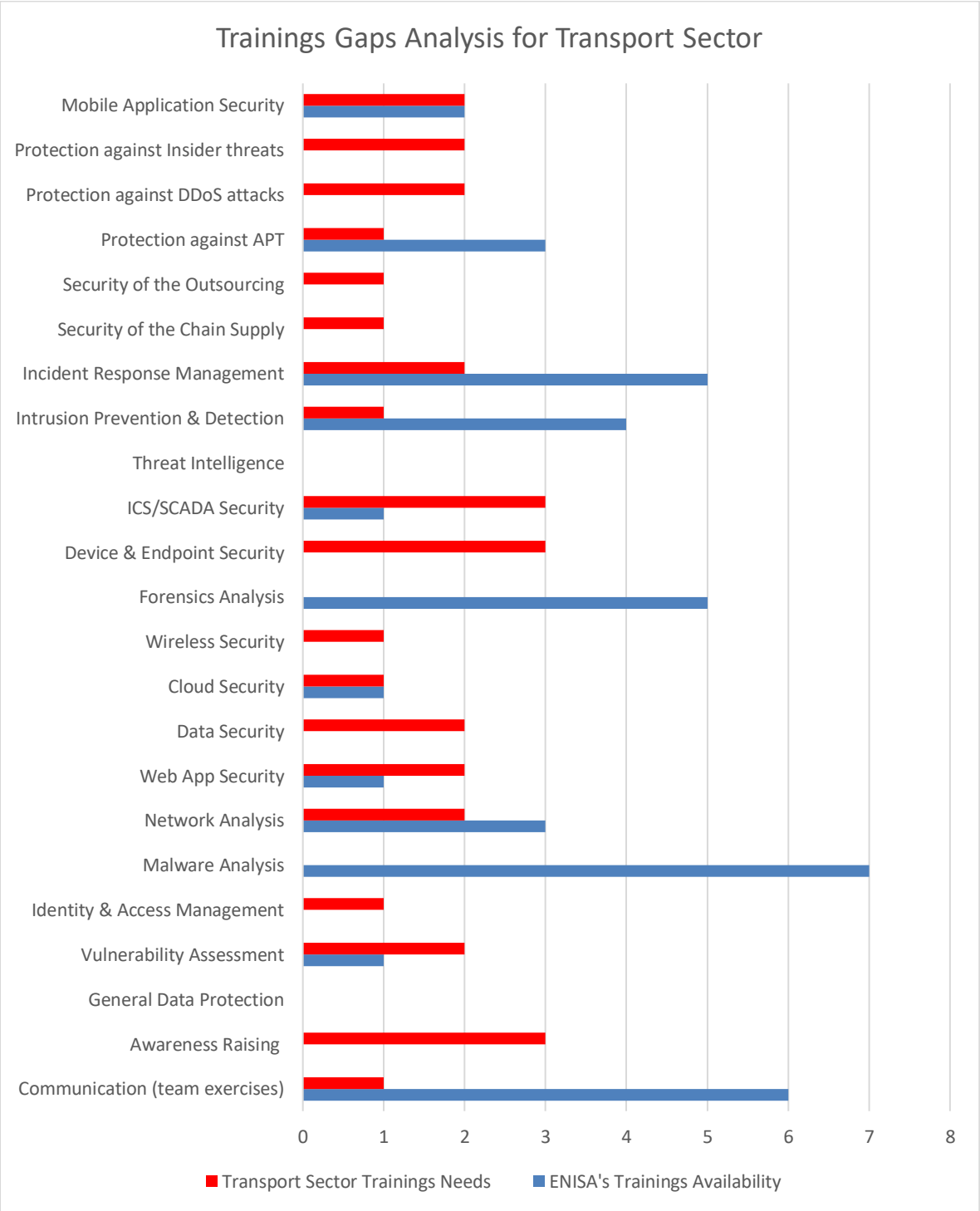

Figure 2: Trainings gaps analysis for transport sector

The results of the gap analysis for the transport sector can be summarized as follows.

- The Transport sector has a significant or urgent need for *ICS/SCADA Security* and IoT related trainings, whereas ENISA provides only one basic training dedicated to this topic. However, some elements related to *ISC/SCADA Security* can be found across a number of ENISA's training materials.
- The Transport sector has an average need for *Data Security* trainings, whereas ENISA does not provide trainings strictly dedicated to this area. However, since data security is concerned as a broad and complex topic, the issues pertaining to it are available partially in most of the available trainings.
- The Transport sector has an average need for *Awareness Raising* trainings, whereas ENISA does not provide trainings dedicated to this area nor does it offer cyber security foundations trainings for beginners (where *Awareness Rising* issue is crucial).
- The Transport sector has an average need for *Vulnerability Assessment* trainings, whereas ENISA provides only 1 training dedicated to this topic.
- The Transport sector has an average need for *Device & Endpoint Security* trainings, whereas ENISA does not provide trainings directly dedicated to this topic.
- The Transport sector has an average need for *Insider Threats* trainings, whereas ENISA does not provide trainings dedicated to this topic.

However, ENISA's trainings catalogue fully meets the following transport sector trainings needs:

- *Communication (Team exercises)*,
- *Network Analysis*,
- *Intrusion Prevention & Detection*,
- *Mobile Application Security*.

4.2.3 Covering Transport Sector Trainings Needs

Below, some findings concerning the transport sector are presented, obtained from the interview with the expert of the Polish Governmental Aviation Agency:

- There is a substantial need for cyber security trainings and exercises dedicated to aviation sector. Trainings offered by the vendors on the market are not sufficient.
- Awareness raising is often limited to the very basic aspect of cyber security. Also, it is presented in the context of physical security (e.g. misuse of USB sticks).
- On the other hand, aviation employees are trained with data protection issues (e.g: trade secrets).
- The crucial trainings needs are connected with operations continuity and maintaining land-air communication.
- Aviation is very a specific sector also because processing of information is twofold: "business" IT systems and operations.
- The main cyber security challenge of aviation IT infrastructure is securing information flow between the stakeholders. The operators are often mistakenly convinced that their networks are completely segregated, whereas in reality public-networks are commonly used.
- One of the greatest technological challenge is to provide real-time encryption between the air-land communication.
- There are several concepts of so called "Aviation CERT" in the industry, but so far there are only commercial platforms available. Not all operators can afford using them.
- Game-changer for the aviation sector might be the implementation of the NIS Directive.

5. Conclusions

The main conclusion from the conducted research is that the available cyber security training offer is large and characterized by a great diversity; however, this offering does not address raising cyber security resilience of critical infrastructure through trainings. The area of CIP-related trainings is still a niche field. There are few organizations and CSIRTs (e.g. ICS-CERT) that provide specialized trainings, in particular in the field of ICS/SCADA systems, but this is still a small fraction within the trainings that are currently available. Despite the availability of various cyber security trainings, there is a lack of cyber security training dedicated to the specific needs of critical sectors that take into account threat context and complexity of interconnections of IT/OT systems.

The emerging need in all NIS Directive sectors is related to cyber security awareness raising. Also, aspects such as e.g. decision making in cyber security management process should be covered – particularly concerning decisions-making in cases of data security incidents, data leakage, etc. Moreover, cyber security trainings should take into account various roles of employees in the cyber security management process and the level of technical advancement of the staff to adequately adjust the trainings to different audience.

There is also a need of trainings related to GDPR, in the light of the upcoming EU regulations, as this will affect every sector in such a way that any breach of personal data protection (e.g. customer data in transport sector) may result in sanctions (both financial and organizational) and could have an impact on the organization operations.

Below are some other practical findings that could assist in tailoring the existing ENISA's training material in the context of NIS Directive sectors needs resulting from the research are summarized.

- ENISA should present the context of threats and risks related to each sector in the trainings. In particular, dependencies and mutual influence of infrastructures operating in different sectors should be explained, and their possible impact on cyber-security issues concerning e.g. global payments or air traffic control.
- ENISA should provide trainings in the local languages.
- ENISA should determine whether cyber ranges and gamification based trainings will likely provide a more effective approach than traditional trainings. On-demand training accessibility is gaining in importance.
- On-demand training accessibility is gaining importance. Such an option is beneficial for the training vendor and organizations, but on the other hand can be less beneficial for the individuals enrolling for the training.

6. Bibliography

DNS: Types of attack and security techniques, AFNIC (Association française pour le nommage Internet en coopération), France 2009

Pescatore J., *Securing DNS Against Emerging Threats: A Hybrid Approach*, SANS Institute, The United States of America 2017

Security of Mobile Payments and Digital Wallets, ENISA, Greece 2016

Security Scorecard, Financial Industry Cybersecurity Report, Security Scorecard, The United States of America 2016

Masud U.T., *Incorporating Cybersecurity Into Water Utility Master Planning A Strategic, Cost-Effective Approach to Mitigate Control System Risk*, Rockwell Automation, The United States of America 2017

Van Leuven L.J., *Water/Wastewater Infrastructure Security: Threats and Vulnerabilities*, Springer, Berlin 2011

The Directive on security of network and information systems (NIS Directive), European Commission, July 2016, http://eur-lex.europa.eu/legal-content/EN/TXT/?uri=uriserv:OJ.L_.2016.194.01.0001.01.ENG&toc=OJ:L:2016:194:TOC

ENISA Threat Landscape, ENISA, February 2017, https://www.enisa.europa.eu/topics/threat-risk-management/threats-and-trends/enisa-threat-landscape

Healthcare and Public Health Sector-Specific Plan, Homeland Security, May 2016, https://www.dhs.gov/sites/default/files/publications/nipp-ssp-healthcare-public-health-2015-508.pdf

Security and Resilience in eHealth Infrastructures and Services, ENISA, December 2015, https://www.enisa.europa.eu/publications/cyber-security-and-resilience-for-smart-hospitals

Cyber security and resilience for Smart Hospitals, ENISA, November 2016, https://www.enisa.europa.eu/publications/security-and-resilience-in-ehealth-infrastructures-and-services

Cybersecurity and Hospitals, American Hospitals Association 2013, http://www.aha.org/content/13/ahaprimer-cyberandhosp.pdf

Securing Smart Airports, ENISA 2016, https://www.enisa.europa.eu/publications/securing-smart-airports

Cyber Security and Resilience of Intelligent Public Transport, Good practices and recommendations, ENISA , January 2016, https://www.enisa.europa.eu/publications/good-practices-recommendations

Cyber Security Strategy for Energy Sector, European Parliament, October 2016, http://www.europarl.europa.eu/RegData/etudes/STUD/2016/587333/IPOL_STU(2016)587333_EN.pdf

Smart Grid Threat Landscape and Good Practice Guide, ENISA, December 2013, https://www.enisa.europa.eu/publications/smart-grid-threat-landscape-and-good-practice-guide

Guidelines for Smart Grid Cyber Security, NIST September 2010, https://www.nist.gov/sites/default/files/documents/smartgrid/nistir-7628_total.pdf

Appendices

A. Lists of trainings institutions and CSIRTs contacted (questionnaires) and those which websites were viewed for desktop research

Table 6: Training institutions/CSIRTs contacted (input from questionnaires)

#	TRAININGS INSTITUTIONS/CSIRTs (QUESTIONNAIRES)
1	CERT/CC - Software Engineering Institute at Carnegie Mellon University
2	Open CSIRT Foundation / Netherlands
3	GEANT / Europe
4	Security Academy / The Netherlands, Belgium & UK
5	Offensive Security
6	MILE2
7	ISECOM (Institute for Security and Open Methodologies)
8	SANS Institute
9	Security Infrastructure Solutions
10	CompTIA
11	PGI Cyber
12	JYVSECTEC
13	Cloud Security Alliance
14	RCTS-CERT / Portugal
15	M7

Table 7: Training institutions/CSIRTs that websites were viewed (input from desktop research)

#	TRAININGS INSTITUTIONS/CSIRTs (INPUT FROM DESKTOP RESEARCH)
1	ISACA (Information Systems Audit and Control Association)
2	GIAC (Global Information Assurance Certification)
3	EC-Council (International Council of Electronic Commerce Consultants)
4	Offensive Security

5	InfoSec Institute
6	Red Tiger Security
7	ENCS
8	NetSecurity
9	Ingalls Information Security
10	IT Governance
11	ESG
12	Antago
13	ICS-CERT

B. List of trainings – based on questionnaires and desktop research

See Annex_B.xlsx for full table of results.

1. The Vendor's Name (***-filled in by Consortium)	3. Training title	11. Sector Relevance							
		Energy	*Transport*	*Banking*	*Finance*	*Health*	*Water Supply*	***Digital Market***	***Other***
SANS Institute	SEC301: Intro to Information Security	✓	✓	✓	✓	✓	✓	✓	
SANS Institute	Developers: DEV534 - Secure DevOps: A Practical Introduction	✓	✓	✓	✓	✓	✓	✓	All Sectors and Industries
CompTIA	CompTIA CyberSecure	✓	✓	✓	✓	✓	✓	✓	

SANS Institute	SEC660: Advanced Penetration Testing, Exploit Writing, and Ethical Hacking	✓	✓	✓	✓	✓	✓	✓	
SANS Institute	SEC575: Mobile Device Security and Ethical Hacking	✓	✓	✓	✓	✓	✓	✓	
SANS Institute	SEC566: Implementing and Auditing the Critical Security Controls - In-Depth	✓	✓	✓	✓	✓	✓	✓	
SANS Institute	SEC560: Network Penetration Testing and Ethical Hacking	✓	✓	✓	✓	✓	✓	✓	
Offensive Security	Penetration Testing	✓	✓	✓	✓	✓	✓	✓	
Mile2	C)PEH = Certified Professional Ethical Hacker	✓	✓	✓	✓	✓	✓	✓	
Mile2	C)PTC = Certified Penetration Testing Consultant	✓	✓	✓	✓	✓	✓	✓	
Mile2	C)PTE= Certified Penetration Testing Engineer	✓	✓	✓	✓	✓	✓	✓	
Security Academy	CISA® Preparation Course : Certified Information Security Auditor	✓	✓	✓	✓	✓	✓	✓	
MONITORING									
SANS Institute	SEC555: SIEM with Tactical Analytics	✓	✓	✓	✓	✓	✓	✓	
SANS Institute	SEC511: Continuous Monitoring and Security Operations	✓	✓	✓	✓	✓	✓	✓	
Mile2	C)NFE = Certified Network	✓	✓	✓	✓	✓	✓	✓	

	Forensics Examiner								
Security Academy	CISSP® Preparation Course : Certified Information Systems Security Professional	✓	✓	✓	✓	✓	✓	✓	
CSIRTs/INCIDENT RESPONSE									
SANS Institute	Management: MGT535 - Incident Response Team Management	✓	✓	✓	✓	✓	✓	✓	All Sectors and Industries
SANS Institute	Management: MGT517 - Managing Security Operations: Detection, Response, and Intelligence	✓	✓	✓	✓	✓	✓	✓	All Sectors and Industries
Software Engineering Institute	Advanced Incident Handling	✓	✓	✓	✓	✓	✓	✓	All sectors
Software Engineering Institute (CERT)	Fundamentals of Incident Handling	✓	✓	✓	✓	✓	✓	✓	can be used by all
Software Engineering Institute (CERT)	Managing CSIRTs	✓	✓	✓	✓	✓	✓	✓	can by used by all
Software Engineering Institute (CERT)	Creating a CSIRT	✓	✓	✓	✓	✓	✓	✓	geared for all sectors
RCTS-CERT	CSIRT-in-a-Box	×	×	×	×	×	×	×	Education and Public administration in general
Open CSIRT Foundation (OCF)	OCF CSIRT Maturity / SIM3 Assessor Training	✓	✓	✓	✓	✓	✓	✓	all sectors
Open CSIRT Foundation (OCF)	OCF Introduction to CSIRT Maturity	✓	✓	✓	✓	✓	✓	✓	All sectors
Mile2	C)IHE - Certified Incident Handling Engineer	✓	✓	✓	✓	✓	✓	✓	

JAMK University of Applied Sciences, Institute of Information Technology, JYVSECTEC Research, Development and Training center	Digital Forensics and Incident Response training/exercise	✓	✓	✓	✓	✓	✓	✓	Government
m7	CSIRT Training / Water Management	×	×	×	×	×	✓	×	Water management
m7	CSIRT Introductory Training	✓	✓	✓	✓	✓	✓	✓	
GEANT	TRANSITS-I CSIRT Introduction Trainings	✓	✓	✓	✓	✓	✓	✓	
GEANT	TRANSITS-II CSIRT Introduction Trainings	✓	✓	✓	✓	✓	✓	✓	
SANS Institute	Management: MGT512 - SANS Security Leadership Essentials For Managers w/ Knowledge Compression™	✓	✓	✓	✓	✓	✓	✓	All Sectors and Industries
GENERAL CYBER SECURITY									
SANS institute	Management: MGT414 - SANS Training Program for CISSP® Certification	✓	✓	✓	✓	✓	✓	✓	All Sectors and Industries
SANS Institute	SEC579: Virtualization and Software-Defined Security	✓	✓	✓	✓	✓	✓	✓	
Cloud Security Alliance	Cloud Control Matrix	✓	✓	✓	✓	✓	✓	✓	
Cloud Security Alliance	Certificate of Cloud Security Knowledge	✓	✓	✓	✓	✓	✓	✓	
Software Engineering Institute	Insider Threat Vulnerability Assessor	✓	✓	✓	✓	✓	✓	✓	all

Software Engineering Institute (CERT)	Insider Threat Program Manager Certificate Program: Implementation and Operations	✓	✓	✓	✓	✓	✓	✓	All sectors
CompTIA	CompTIA Advanced Security Practitioner (CASP)	✓	✓	✓	✓	✓	✓	✓	
CompTIA	CompTIA Cyber Security Analyst (CSA+)	✓	✓	✓	✓	✓	✓	✓	
CompTIA	CompTIA Security+	✓	✓	✓	✓	✓	✓	✓	
Protection Group International	Cyber Security	✓	✓	✓	✓	✓	✓	✓	Law Enforcement, Military, Government,
The Institute for Security and Open Methodologies (ISECOM)	OSSTMM Professional Security Analyst (OPSA)	✓	✓	✓	✓	✓	✓	✓	Appropriate for anything requiring security, online and offline
The Institute for Security and Open Methodologies (ISECOM)	OSSTMM Professional Security Testing	✓	✓	✓	✓	✓	✓	✓	Any onlie systems or processes
Mile2	C)SLO = Certified Security Leadership Officer	✓	✓	✓	✓	✓	✓	✓	
Mile2	C)VA = Certified Vulnerability Assessor	✓	✓	✓	✓	✓	✓	✓	
Mile2	C)SAP = Certified Security Awareness Principles	✓	✓	✓	✓	✓	✓	✓	
Mile2	C)SWAE = Certified Secure Web Applications Engineer	✓	✓	✓	✓	✓	✓	✓	
Mile2	C)DFE = Certified Digital Forensics Examiner	✓	✓	✓	✓	✓	✓	✓	
Mile2	C)DRE = Certified Disaster	✓	✓	✓	✓	✓	✓	✓	

	Recovery Engineer								
Mile2	C)ISSO = Certified Information Systems Security Officer	✓	✓	✓	✓	✓	✓	✓	
JAMK University of Applied Sciences, Institute of Information Technology, JYVSECTEC research, development and training center	Versatile and high quality training in various fields of information and cyber security	✓	✓	✓	✓	✓	✓	✓	Government
Security Academy	CCSP® Preparation Course : Certified Cloud Security Professionak	✓	✓	✓	✓	✓	✓	✓	
Security Academy	CISM® Preparation Course : Certified Information Security Manager	✓	✓	✓	✓	✓	✓	✓	
ICS/SCADA SECURITY									
SANS Institute	Industrial Control Systems: ICS Active Defense and Incident Response	✓	✓	×	×	×	✓	×	Control Systems - All Sectors: F&B,Metals /mining,Chem,Pharma ,Manufact., Auto,Aero, BAS
SANS Institute	Industrial Control Systems: ICS/SCADA Security Essentials	✓	✓	×	×	×	✓	×	Control Systems - All Sectors: F&B,Metals /Mining,Chem,Pharma ,Manufact., Auto,Aero, BAS
Security Infrastructure Solutions	Industrial Control Systems Security	✓	✓	×	×	×	✓	×	

C. List of tables and figures

ENISA

European Union Agency for Network
and Information Security
Science and Technology Park of Crete (ITE)
Vassilika Vouton, 700 13, Heraklion, Greece

Athens Office

1 Vasilissis Sofias
Marousi 151 24, Attiki, Greece

TP-04-17-945-EN-N

PO Box 1309, 710 01 Heraklion, Greece
Tel: +30 28 14 40 9710
info@enisa.europa.eu
www.enisa.europa.eu

ISBN: 978-92-9204-231-8
DOI: 10.2824/521757