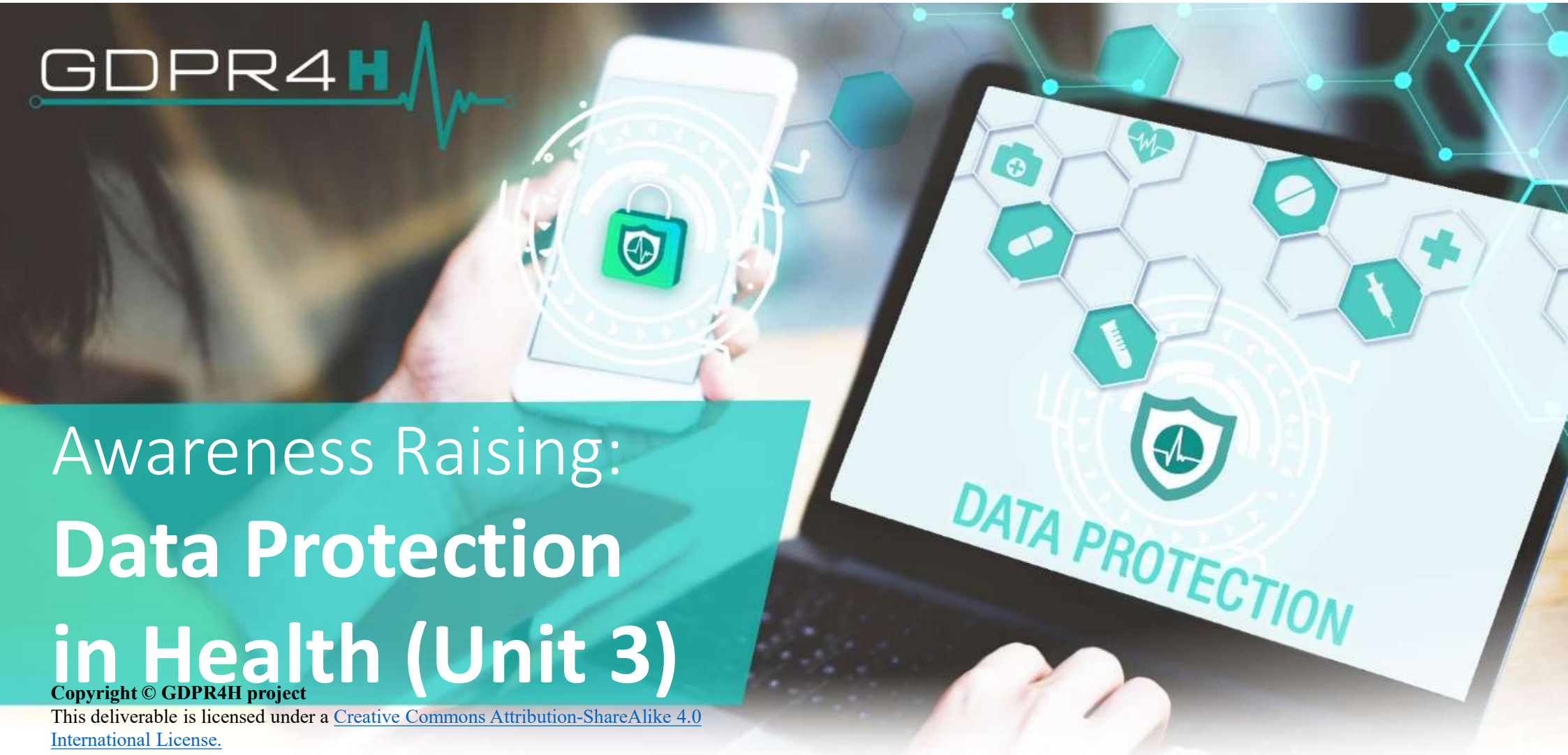



# Awareness Raising:
# Data Protection in Health (Unit 3)



Steinbeis HOCHSCHULE · ACQUIN · METROPOLITAN COLLEGE CENTRE OF EXCELLENCE · PEF · Skybridge partners · crefop · arps · EMA European Medical Association

Erasmus+

The European Commission's support for the production of this publication does not constitute endorsement of the content, which reflects the views only of the authors, and the Commission and the EACEA cannot be held responsible for any use which may be made of the information contained therein.

# Table of contents



Image by Pettycon from Pixabay


Erasmus+ The European Commission's support for the production of this publication does not constitute endorsement of the content, which reflects the views only of the authors, and the Commission and the EACEA cannot be held responsible for any use which may be made of the information contained therein.

# Table of contents



Image by Pettycon from Pixabay


The European Commission's support for the production of this publication does not constitute endorsement of the content, which reflects the views only of the authors, and the Commission and the EACEA cannot be held responsible for any use which may be made of the information contained therein.

GDPR4H

# Aims & Objectives

- Description of the basic IT security tools
- Description of the typical barriers to digitalization
- Analysis of the E-Health diverse types

Steinbeis HOCHSCHULE ACQUIN METROPOLITAN COLLEGE CENTRE OF EXCELLENCE PEF PANHELLENIC UNION OF PHARMACEUTICAL INDUSTRY Skybridge partners crefop arps EMA European Medical Association

Erasmus+ The European Commission's support for the production of this publication does not constitute endorsement of the content, which reflects the views only of the authors, and the Commission and the EACEA cannot be held responsible for any use which may be made of the information contained therein.

# Learning Outcomes

- *List at least 3 types of  E-health services*
- *List at least 3 barriers to the digitalization of healthcare*
- *List the 4 core IT security tools*
- *Describe the advantages of IT Security tools*
- *Analyze the barriers that inhibit the digitalization of healthcare sector*

Erasmus+ The European Commission's support for the production of this publication does not constitute endorsement of the content, which reflects the views only of the authors, and the Commission and the EACEA cannot be held responsible for any use which may be made of the information contained therein.

# Terms and Keywords

**-IT security tools**
**-E-Health**
**-Digitalization**
**-Threat**
**-Cybersecurity**

Image by Gerd Altmann from Pixabay

The European Commission's support for the production of this publication does not constitute endorsement of the content, which reflects the views only of the authors, and the Commission and the EACEA cannot be held responsible for any use which may be made of the information contained therein.

# Threats

1. “A threat is a potential cause of an incident, which may result in harm of systems and organization.”
2. A threat has the potential to harm amongst others information, processes and systems and therefore organizations. Threats may be of natural or human origin, and could be accidental or deliberate. A threat may arise from within or from outside the organization.
3. Threats may be deliberate, accidental or environmental (natural) and may result, for example, in damage or loss of essential services, information and others. Threats may be divided into types e.g. Physical damage, Natural events, loss of essential services and others. This grouping of threats can help organizations during Risk Identification (completeness check).

Erasmus+ The European Commission’s support for the production of this publication does not constitute endorsement of the content, which reflects the views only of the authors, and the Commission and the EACEA cannot be held responsible for any use which may be made of the information contained therein.

GDPR4H

# Threats

| Top Threats 2017 | Assessed Trends 2017 | Top Threats 2018 | Assessed Trends 2018 | Change in ranking |
|---|---|---|---|---|
| 1. Malware | ⊃ | 1. Malware | ⊃ | → |
| 2. Web Based Attacks | ↑ | 2. Web Based Attacks | ↑ | → |
| 3. Web Application Attacks | ↑ | 3. Web Application Attacks | ⊃ | → |
| 4. Phishing | ↑ | 4. Phishing | ↑ | → |
| 5. Spam | ↑ | 5. Denial of Service | ↑ | ↑ |
| 6. Denial of Service | ↑ | 6. Spam | ⊃ | ↓ |
| 7. Ransomware | ↑ | 7. Botnets | ↑ | ↑ |
| 8. Botnets | ↑ | 8. Data Breaches | ↑ | ↑ |
| 9. Insider threat | ⊃ | 9. Insider Threat | ↓ | → |
| 10. Physical manipulation/ damage/ theft/loss | ⊃ | 10. Physical manipulation/ damage/ theft/loss | ⊃ | → |
| 11. Data Breaches | ↑ | 11. Information Leakage | ↑ | ↑ |
| 12. Identity Theft | ↑ | 12. Identity Theft | ↑ | → |
| 13. Information Leakage | ↑ | 13. Cryptojacking | ↑ | NEW |
| 14. Exploit Kits | ↓ | 14. Ransomware | ↓ | ↓ |
| 15. Cyber Espionage | ↑ | 15. Cyber Espionage | ↓ | → |

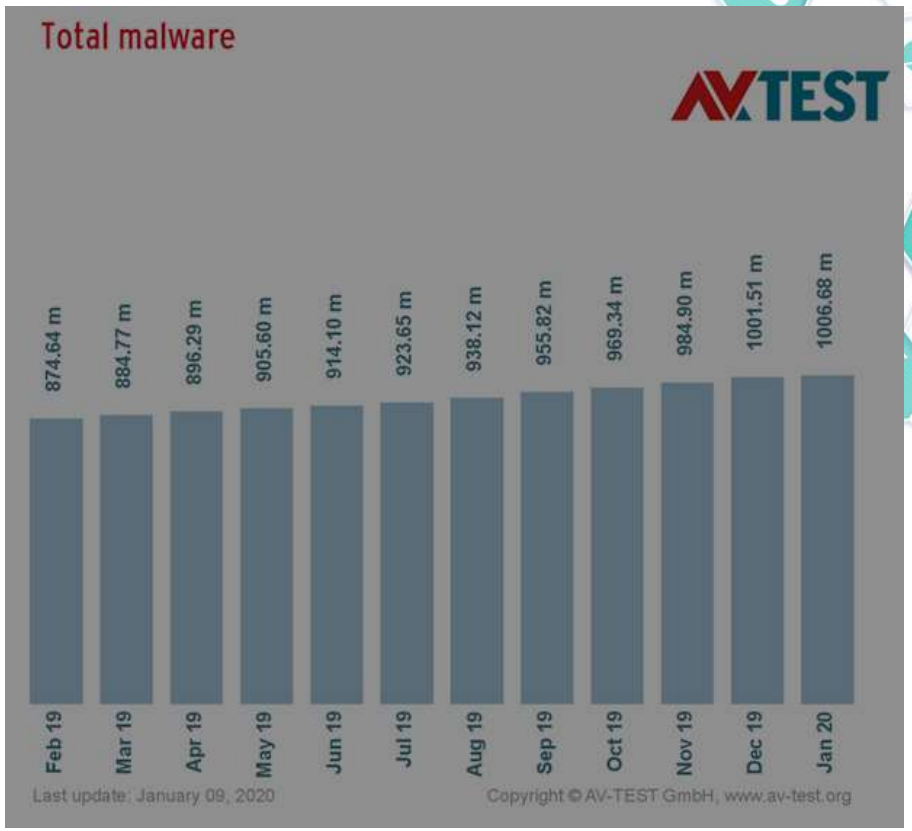
Legend: Trends: ↓ Declining, ⊃ Stable, ↑ Increasing
Ranking: ↑ Going up, → Same, ↓ Going down

Steinbeis HOCHSCHULE ACQUIN METROPOLITAN COLLEGE CENTRE OF EXCELLENCE PEF PANHELLENIC UNION OF PHARMACEUTICAL INDUSTRY Skybridge partners crefop arps EMA European Medical Association

Erasmus+ The European Commission's support for the production of this publication does not constitute endorsement of the content, which reflects the views only of the authors, and the Commission and the EACEA cannot be held responsible for any use which may be made of the information contained therein.

# Malware

"Software or firmware which performs an unauthorized process that will have adverse impact on the confidentiality, integrity, or availability of an information system. A virus, worm, Trojan horse, or other code-based entity that infects a host. Spyware and some forms of adware are also examples of malicious code."




Erasmus+ The European Commission's support for the production of this publication does not constitute endorsement of the content, which reflects the views only of the authors, and the Commission and the EACEA cannot be held responsible for any use which may be made of the information contained therein.

# Cyber extortion

1. “Cyber extortion is defined as an online crime in which hackers hold your data, website, computer systems, or other sensitive information hostage until you meet their demands for payment”.
2. One example is ransomware which is a type of malware and when the attacker gain access to a device or a system, malware locks the screen or encrypts the data stored on the disk. It then presents a ransom payment requirement with detailed payment details.


Image by methodshop from Pixabay

Erasmus+ The European Commission’s support for the production of this publication does not constitute endorsement of the content, which reflects the views only of the authors, and the Commission and the EACEA cannot be held responsible for any use which may be made of the information contained therein.

# Infected with Ransomware…

Indicators of a ransomware attack could include:

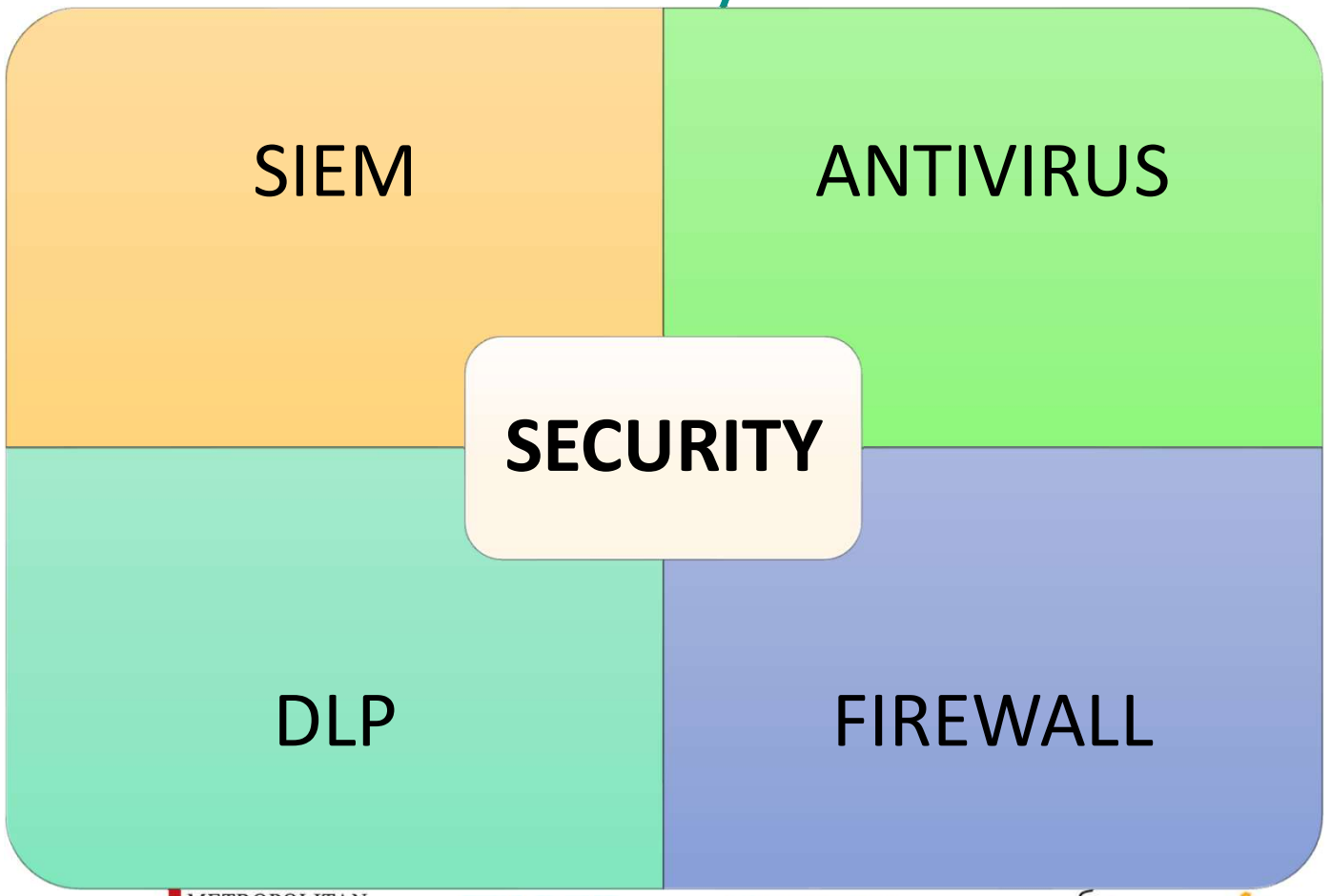
- When the user realizes that a link that was clicked on, a file attachment opened, or a website visited may have been malicious
- When there is a notable increase in activity in the central processing unit (CPU) of a computer and disk activity for no apparent reason
- When there is a difficulty or unavailability to access certain files as the ransomware encrypts, deletes and re-names and/or relocates data; and
- When somebody can detect possible suspicious network communications between the ransomware and the attackers' command


Image by methodshop from Pixabay

The European Commission's support for the production of this publication does not constitute endorsement of the content, which reflects the views only of the authors, and the Commission and the EACEA cannot be held responsible for any use which may be made of the information contained therein.

GDPR4H

# IT security tools




Steinbeis HOCHSCHULE ACQUIN METROPOLITAN COLLEGE CENTRE OF EXCELLENCE PEF PANHELLENIC UNION OF PHARMACEUTICAL INDUSTRY Skybridge partners crefop arps EMA European Medical Association

Erasmus+ The European Commission's support for the production of this publication does not constitute endorsement of the content, which reflects the views only of the authors, and the Commission and the EACEA cannot be held responsible for any use which may be made of the information contained therein.

# IT Tool 1: SIEM

1. Security Information and Event Management (SIEM) functions as a system for monitoring, recording, as well as analyzing in real time all the data in an IT infrastructure, allowing the connection of events and creating reports on the critical functions of the infrastructure systems.

2. The following image from Esecurityplanet, depicts a comparison between various SIEM vendors according to specific characteristics (e.g. threats blocked, sources ingested, value, performance, management, implementation and others).


Steinbeis HOCHSCHULE ACQUIN METROPOLITAN COLLEGE CENTRE OF EXCELLENCE PEF PANHELLENIC UNION OF PHARMACEUTICAL INDUSTRY Skybridge partners crefop arps EMA European Medical Association

Erasmus+ The European Commission's support for the production of this publication does not constitute endorsement of the content, which reflects the views only of the authors, and the Commission and the EACEA cannot be held responsible for any use which may be made of the information contained therein.

# IT Tool 1: SIEM and its advantages

Data aggregation and normalization

Compliance

Threat detection

Steinbeis HOCHSCHULE ACQUIN METROPOLITAN COLLEGE CENTRE OF EXCELLENCE PEF PANHELLENIC UNION OF PHARMACEUTICAL INDUSTRY Skybridge partners crefop arps EMA European Medical Association

Erasmus+ The European Commission's support for the production of this publication does not constitute endorsement of the content, which reflects the views only of the authors, and the Commission and the EACEA cannot be held responsible for any use which may be made of the information contained therein.

# SIEM and its advantages: Definitions

Log management aggregates data from a variety of resources. Moreover, SIEM is able to provide consolidation of monitored data

SIEM it can be used to gather compliance data and produce reports that adjust security and auditing processes

SIEM is able to search across logs, as well as provides automated analysis on correlated events

The European Commission's support for the production of this publication does not constitute endorsement of the content, which reflects the views only of the authors, and the Commission and the EACEA cannot be held responsible for any use which may be made of the information contained therein.

# IT Tool 2: Antivirus

Antivirus software is the most commonly used technical control for malware threat mitigation. There are many brands of antivirus software, with most providing similar protection through the following recommended capabilities:

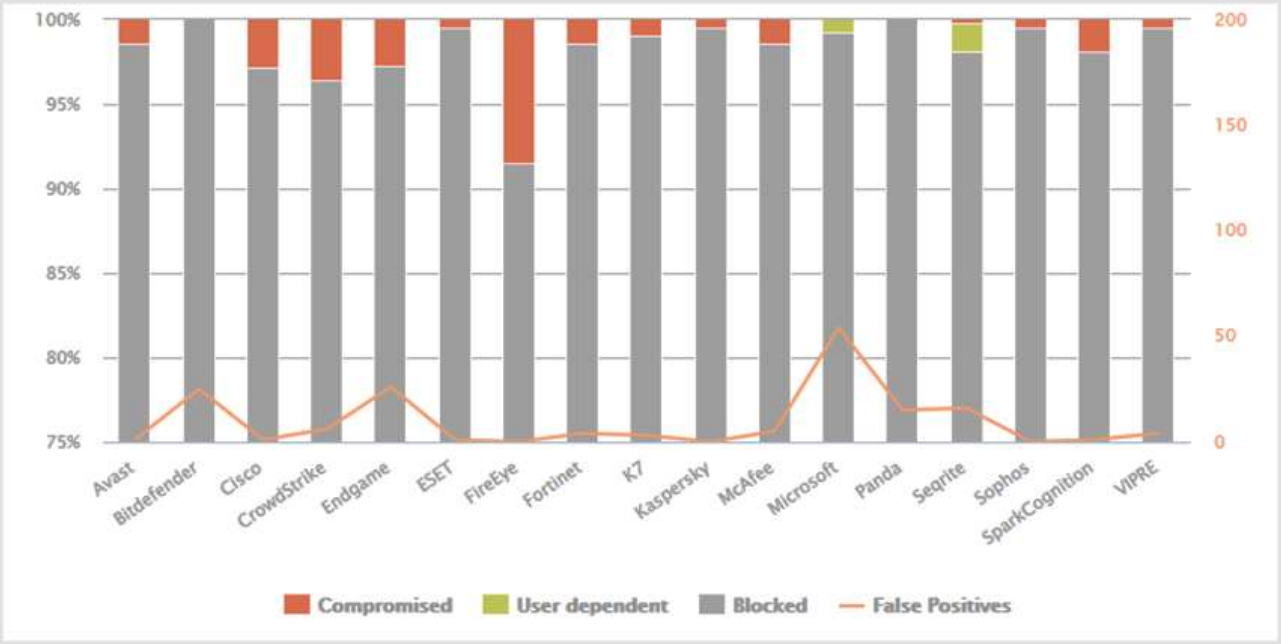
- Scanning critical host components
- Overviewing suspicious activity.
- Monitoring the behavior of common applications, such as email clients, web browsers, and instant messaging software.
- Identifying common types of malware as well as attacker tools.
- Disinfecting files, which refers to removing malware from within a file.

The European Commission's support for the production of this publication does not constitute endorsement of the content, which reflects the views only of the authors, and the Commission and the EACEA cannot be held responsible for any use which may be made of the information contained therein.

# IT Tool 2: Antivirus

**Real-World Protection Test (August-November)**

The results below are based on a test set consisting of **844** test cases (such as malicious URLs), tested from the beginning of August 2019 till the end of November 2019.




| | Blocked | User dependent | Compromised | PROTECTION RATE [Blocked % + (User dependent %)/2]* | False Alarms |
|---|---|---|---|---|---|
| Panda | 844 | - | - | 100% | 15 |
| Bitdefender | 844 | - | - | 100% | 25 |
| Microsoft | 837 | 7 | - | 99.6% | 45 |
| Kaspersky, Sophos | 840 | - | 4 | 99.5% | 0 |
| ESET | 840 | - | 4 | 99.5% | 1 |
| VIPRE | 840 | - | 4 | 99.5% | 4 |
| K7 | 836 | - | 8 | 99.1% | 3 |
| Seqrite | 828 | 14 | 2 | 98.9% | 16 |
| Avast | 832 | - | 12 | 98.6% | 1 |
| Fortinet | 832 | - | 12 | 98.6% | 4 |
| McAfee | 832 | - | 12 | 98.6% | 5 |
| SparkCognition | 828 | - | 16 | 98.1% | 1 |
| Endgame | 821 | - | 23 | 97.3% | 26 |
| Cisco | 820 | - | 24 | 97.2% | 1 |
| CrowdStrike | 814 | - | 30 | 96.4% | 6 |
| FireEye | 772 | - | 72 | 91.5% | 0 |

Erasmus+

The European Commission's support for the production of this publication does not constitute endorsement of the content, which reflects the views only of the authors, and the Commission and the EACEA cannot be held responsible for any use which may be made of the information contained therein.

# IT Tool 3: DLP

Data Loss Prevention (DLP) solutions cover three primary states of information:

- DLP solutions should be able to log where various file types are stored.
- Data in transit refers to data traveling through the network. Deep packet inspection (DPI) is used to analyze the data for sensitive content.
- Data in use refers to data movement at the user workstation level. This includes information sent to printers, thumb drives and the copy-and-paste clipboard.

DLP software products use business rules to classify and protect confidential and critical information so that unauthorized end users cannot accidentally or maliciously share data whose disclosure could put the organization at risk. For example, if an employee tried to forward a business email outside the corporate domain or upload a corporate file to a consumer cloud storage service like Dropbox, the employee would be denied permission.

# IT Tool 4: Firewall

A firewall software or hardware monitors incoming and outgoing network traffic and decides whether specific traffic needs to be allowed or blocked based on a defined set of security rules that each organization applies in accordance with their security level.

**Types of networks**:

- WAN: The interface which connects the internal network to the Internet
- LAN: Is the internal network of the company. All the assets included PCs, Printers, Access Points, Servers etc. are part of the LAN
- DMZ (demilitarized zone): Separates the internal network from other untrusted networks, usually the Internet. It is usually used for Webservers, DNS, FTP.

Erasmus+ The European Commission's support for the production of this publication does not constitute endorsement of the content, which reflects the views only of the authors, and the Commission and the EACEA cannot be held responsible for any use which may be made of the information contained therein.

# IT Tool 4: Firewall

- **Firewall features**

Most of firewalls include extra features such as AV, IPS, Antispam, Content filter, etc.

-IDPS: Intrusion detection prevention system acts as a technology that identifies suspicious activities which finds and also prevents from unwanted requests to the internal network.

-Content filter: The procedure of monitoring communications such as email and Web pages, analyzing them for suspicious content, and detecting the delivery of suspicious content to users

Erasmus+ The European Commission's support for the production of this publication does not constitute endorsement of the content, which reflects the views only of the authors, and the Commission and the EACEA cannot be held responsible for any use which may be made of the information contained therein.

# E-Health

**Types:**

- **Electronic medical record (EMR):** It functions as an electronic replacement of paper-based health records, and can be considered as the basic IT system for healthcare. It contains:

1. history of the patient
2. It sends notifications for specific actions that have to take place (i.e tests, screenings, medical visits etc.)

- **Electronic Health Record (EHR):** It is a more specified tool, since it allows the review of the patient's history and the presentation of results of examinations.

The European Commission's support for the production of this publication does not constitute endorsement of the content, which reflects the views only of the authors, and the Commission and the EACEA cannot be held responsible for any use which may be made of the information contained therein.

# E-Health

According to “ISO TR 205149” they are provided the two following definitions:

- **EHR**: “A repository of information regarding the health status of a subject of care, in computer processable form. An EHR provides the ability to share patient health information between authorized users of the HER and the primary role of the EHR is supporting continuing, efficient and quality integrated health care.”
- **EHR system**: “The set of components that form the mechanism by which electronic health records are created, used, stored, and retrieved. It includes people, data, rules and procedures, processing and storage devices, and communication and support facilities.”
- **Patient Healthcare Record**: A PHR functions as the interface between the EMR/EHR and the patient. It allows the accessibility of data not only from the hospital/clinic/doctor, but also from the patient.
- **Scheduling systems:** These function as electronic platforms for booking appointments with doctors, for tests or for simple medical procedures.

The European Commission’s support for the production of this publication does not constitute endorsement of the content, which reflects the views only of the authors, and the Commission and the EACEA cannot be held responsible for any use which may be made of the information contained therein.

# E-Health

- **e-Prescription:** This system serves the patient's need on the prescription of medicine and optimize the process. The first step is the patient visiting a physician, and the second step is the patient visiting a pharmacy, which provides him/her with the medicine.
- **Health Information System – HIS:** This is the basic IT system of every clinic or hospital, allowing management of every day operations. It is also in connection with other IT systems in hospitals.
- **Internet Medical of Things**: It includes the smart infrastructure and various medical devices connecting over the network. More specifically, its types are:

❑smart wearable devices, which for instance are monitors of heart rate,

❑home-used medical devices, which for instance are blood pressure meters

❑implantable devices, which for instance are heart pacemakers

The European Commission's support for the production of this publication does not constitute endorsement of the content, which reflects the views only of the authors, and the Commission and the EACEA cannot be held responsible for any use which may be made of the information contained therein.

# E-Health

- point-of-care kits, such as diagnostic tests
- Kiosks, which can provide clients with medical products (see e-Prescriptions)
- sensors (RFID) which are offered through pharmaceutical packages
- mobile applications for healthcare
- emergency response systems
- virtual home assistants, such as overviewing tools of adherence to prescriptions

The market value of the Internet of Medical Things is very important, since it will reach 140 billion EUR by 2022, as a study of Deloitte has stated.

Erasmus+ The European Commission's support for the production of this publication does not constitute endorsement of the content, which reflects the views only of the authors, and the Commission and the EACEA cannot be held responsible for any use which may be made of the information contained therein.

# Healthcare standards

When referring to ICT security standards related to the healthcare sector, it's important to underline that it is not a holistic era. Standards Developing Organizations are connecting with standards related directly or indirectly to ICT security in the area of healthcare. The following work is being carried out by the bodies recognized by the Regulation 1025/2012 on European standardization:

- **International Standards Organisation:** ISO has established a technical committee TC 215 – Health informatics. It is connected with the standardization in the field of health informatics, to facilitate capture, interchange and use of health-related data.
- **CEN-CENELEC:** There are various technical committees related to medical devices, mainly from the safety point of view (covering a wide variety of topics, ranging from electrical medical equipment, syringes and ophthalmic optics). A technical committee at CEN has been established to develop European standards consistent with the existing international framework - TC 251, "Health informatics". It includes Electronic Health Records architecture and Health Informatics Service Architecture, as well as Detailed Clinical Modelling
- **International Telecommunication Union – ITU**: The ITU is related to several items in connection with eHealth applications – identification of users' requirements, multimedia framework (in particular for telemedicine, roadmap for e-health standards).

The European Commission's support for the production of this publication does not constitute endorsement of the content, which reflects the views only of the authors, and the Commission and the EACEA cannot be held responsible for any use which may be made of the information contained therein.

# Tackling the barriers of digital transformation

- **Transforming skills and attitudes**:

1. By reforming both initial training

2. By offering continued professional education and supporting health workers in acquiring new digital skills.

3. By facilitating the integration of new professions and roles in health systems related to the IT sector

- **Updated ethical frameworks**: At the new digital era, a growing number of health care activities will be performed by humans and robots. How do health workers can collaborate with AI?

1. Principles for responsible AI (i.e inclusivity, sustainability and human-centric values)

Erasmus+ The European Commission's support for the production of this publication does not constitute endorsement of the content, which reflects the views only of the authors, and the Commission and the EACEA cannot be held responsible for any use which may be made of the information contained therein.

# Tackling the barriers of digital transformation

2. Data ownership challenge:

- 1st: The selling of health data, with entities acquiring and on-selling personal data for commercial purposes. While these data are typically, but not always, de-identified this should raise questions about individuals' data ownership and about who should gain profit from them. On the other hand, by excluding companies with the expertise and resources from make use of health data to develop improved diagnostic tools, may put a barrier to potential advances to human health and welfare.
- 2nd: Individuals are the 'owners' of their data, is another view which opens the room for discussion. Ownership values can be debated based on who pay for the activities that generate the data. If paid by a third party (typically the taxpayer) data may be a subject of public good.

- **No one is left behind**: According to OECD, in 2017, 3.7 billion health related smartphone apps were downloaded globally, up from 1.7 billion in 2013. Digital transformation may be considered as a promise to 'democratise' health.

Erasmus+ The European Commission's support for the production of this publication does not constitute endorsement of the content, which reflects the views only of the authors, and the Commission and the EACEA cannot be held responsible for any use which may be made of the information contained therein.

# Tackling the barriers of digital transformation

In this framework, the related actions should take place:

-Helping patients access and use effectively their own medical records

-Improving digital literacy

-Offering benefits to those that may be left behind

- **Opening data:**

1. Improving the preparedness for EHR data to be used for research→ The required operational, policy and governance levers include:

o A national plan that underlines the secondary uses of these data.

o Having a legal framework that enables data to be securely extracted

o Building the capacity analysis for data to generate meaningful information

o Ensuring minimum data specifications and common data terminology standards

Erasmus+ The European Commission's support for the production of this publication does not constitute endorsement of the content, which reflects the views only of the authors, and the Commission and the EACEA cannot be held responsible for any use which may be made of the information contained therein.

# Synopsis

In this unit, the learner will be able to get insight on the basic IT tools of data protection in general. Moreover, the learner will be able recognize the importance of tackling barriers that inhibit the digitalization of Healthcare. Based on these, you have to remember that:

- “A threat is a potential cause of an incident, which may result in harm of systems and organization.”
- “Cyber extortion is defined as an online crime in which hackers hold your data, website, computer systems, or other sensitive information hostage until you meet their demands for payment”.
- Data Loss Prevention (DLP) solutions cover three primary states of information:

-DLP solutions should be able to log where various file types are stored.

-Data in transit refers to data traveling through the network. Deep packet inspection (DPI) is used to analyze the data for sensitive content.

-Data in use refers to data movement at the user workstation level. This includes information sent to printers, thumb drives and the copy-and-paste clipboard.

The European Commission’s support for the production of this publication does not constitute endorsement of the content, which reflects the views only of the authors, and the Commission and the EACEA cannot be held responsible for any use which may be made of the information contained therein.

# Bibliography


- OECD Health Policy Studies. (2019). "Health in the 21st Century: PUTTING DATA TO WORK FOR STRONGER HEALTH SYSTEMS". Available on: https://www.oecd-ilibrary.org/docserver/e3b23f8e-en.pdf?expires=1588756674&id=id&accname=guest&checksum=05C0259E79E6C6CB82064EC413C7594B
- Anderson, A. et al. (2016), "Electronic health record phenotyping improves detection and screening of type 2 diabetes in the general United States population: A cross-sectional, unselected, retrospective study", Journal of Biomedical Informatics 60, pp. 162-68. Available on: http://dx.doi.org/10.1016/j.jbi.2015.12.006
- Blackwood, N. (2018), "The Promis of Healthtech: How Digital Innovators are Transforming NHS". Available on: http://www.public.io/wp-content/uploads/2018/04/PUBLIC-The-Promise-ofHealthTech.pdf
- ISO/IEC 27005:2018 Information Technology — Security Techniques — Information Security Risk Management
- ENISA. (2018). "ENISA Threat Landscape Report". Available on: https://www.enisa.europa.eu/publications/enisa-threat-landscape-report-2018
- ENISA. (2018). "IT security certification opportunities in the healthcare sector"



Erasmus+ The European Commission's support for the production of this publication does not constitute endorsement of the content, which reflects the views only of the authors, and the Commission and the EACEA cannot be held responsible for any use which may be made of the information contained therein.

# Thank you for your attention!

The European Commission's support for the production of this publication does not constitute endorsement of the content, which reflects the views only of the authors, and the Commission and the EACEA cannot be held responsible for any use which may be made of the information contained therein.