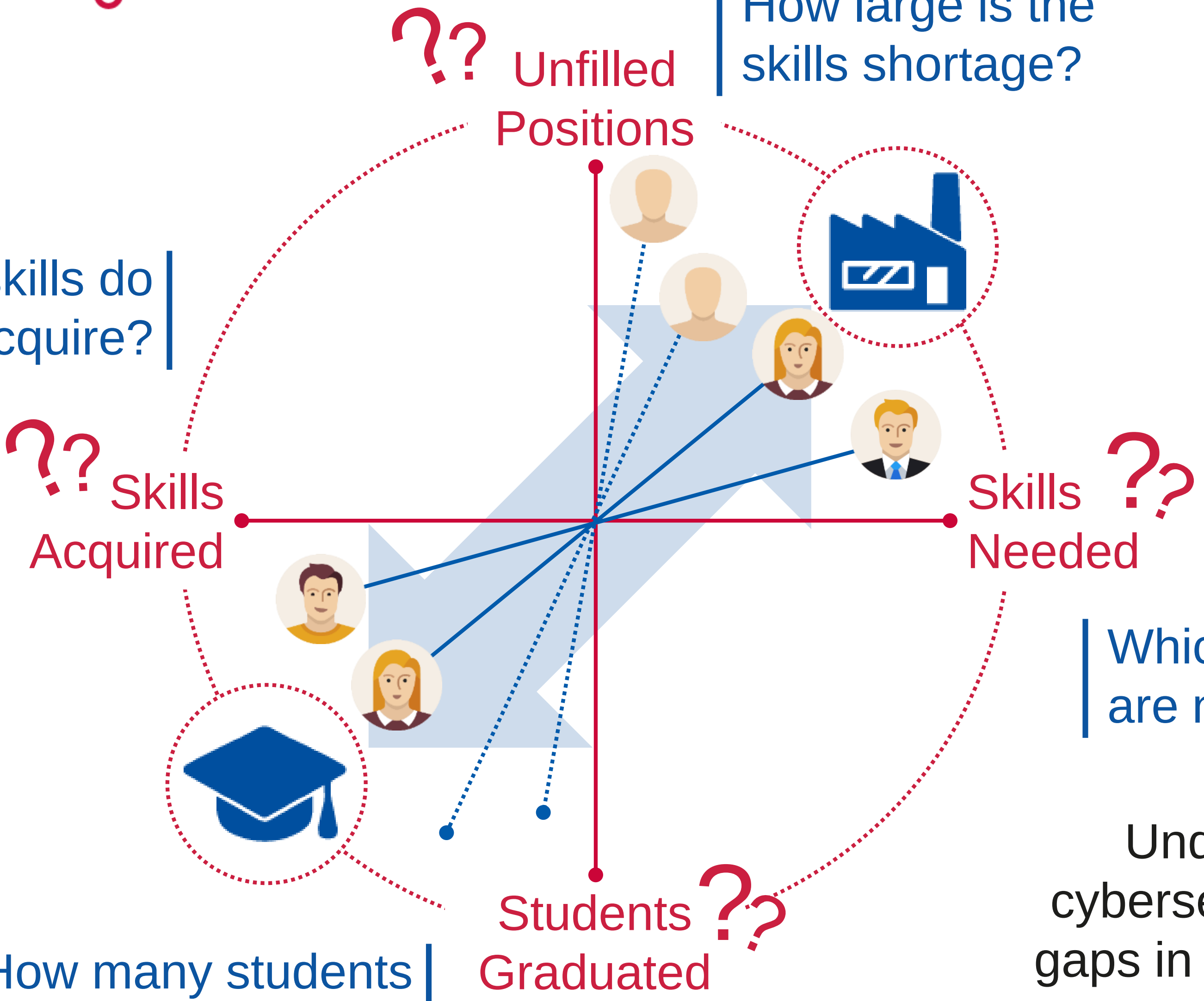
EUROPEAN UNION AGENCY
FOR CYBERSECURITY

# TRAININGS AND SKILLS: ENISA EXPERIENCE

Dr. Fabio Di Franco
Capacity Building Unit - ENISA

25 | 03 | 2021

# Cybersecurity skills gap and shortage



Unfilled Positions

Skills Needed

Students Graduated

Skills Acquired

How large is the skills shortage?

What skills do students acquire?

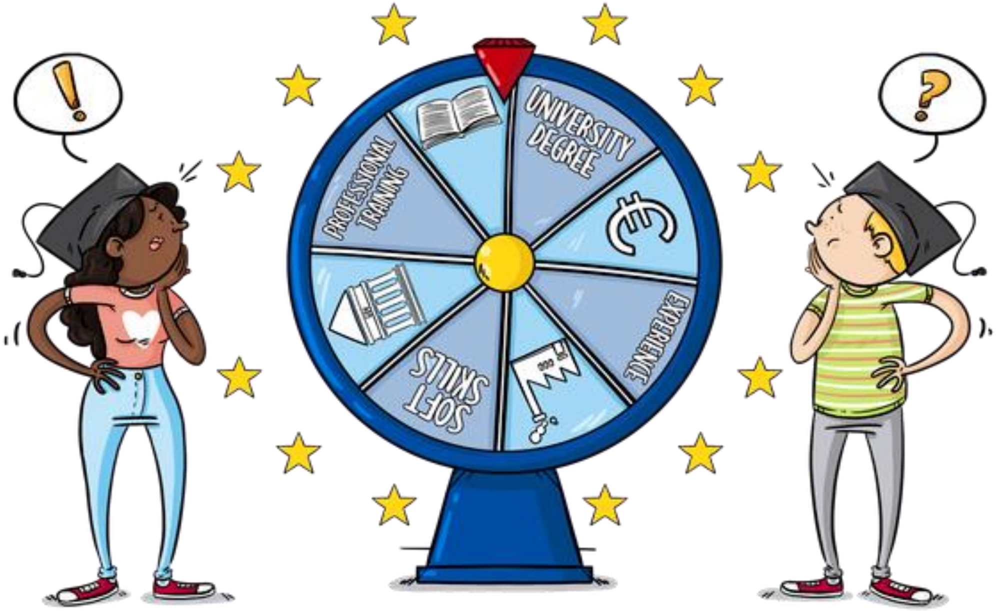
Which skills are needed?

How many students graduate yearly?

Understand the cybersecurity skills gaps in the Europe.

# AN EUROPEAN CYBERSECURITY SKILLS FRAMEWORK IS ON THE WAY

- Promote harmonization in the ecosystem of cybersecurity education, training, and workforce development
- Develop of a common European language in the cybersecurity skills and competencies context.



# CYBERSECURITY HIGHER EDUCATION DATABASE

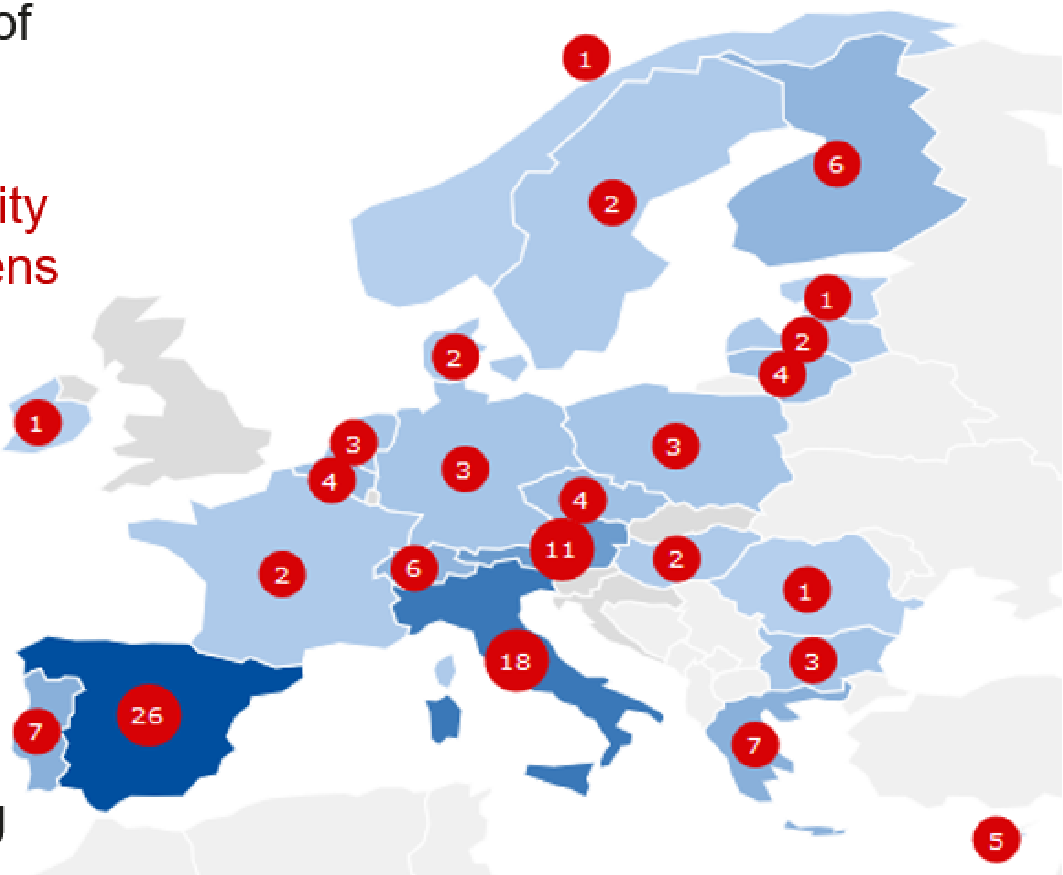
CYBERHEAD

CYBERSECURITY HIGHER EDUCATION DATABASE

Crowd-sourced database of cybersecurity related education programmes: it is the largest cybersecurity point of reference for citizens looking to upskill their knowledge in the cybersecurity field

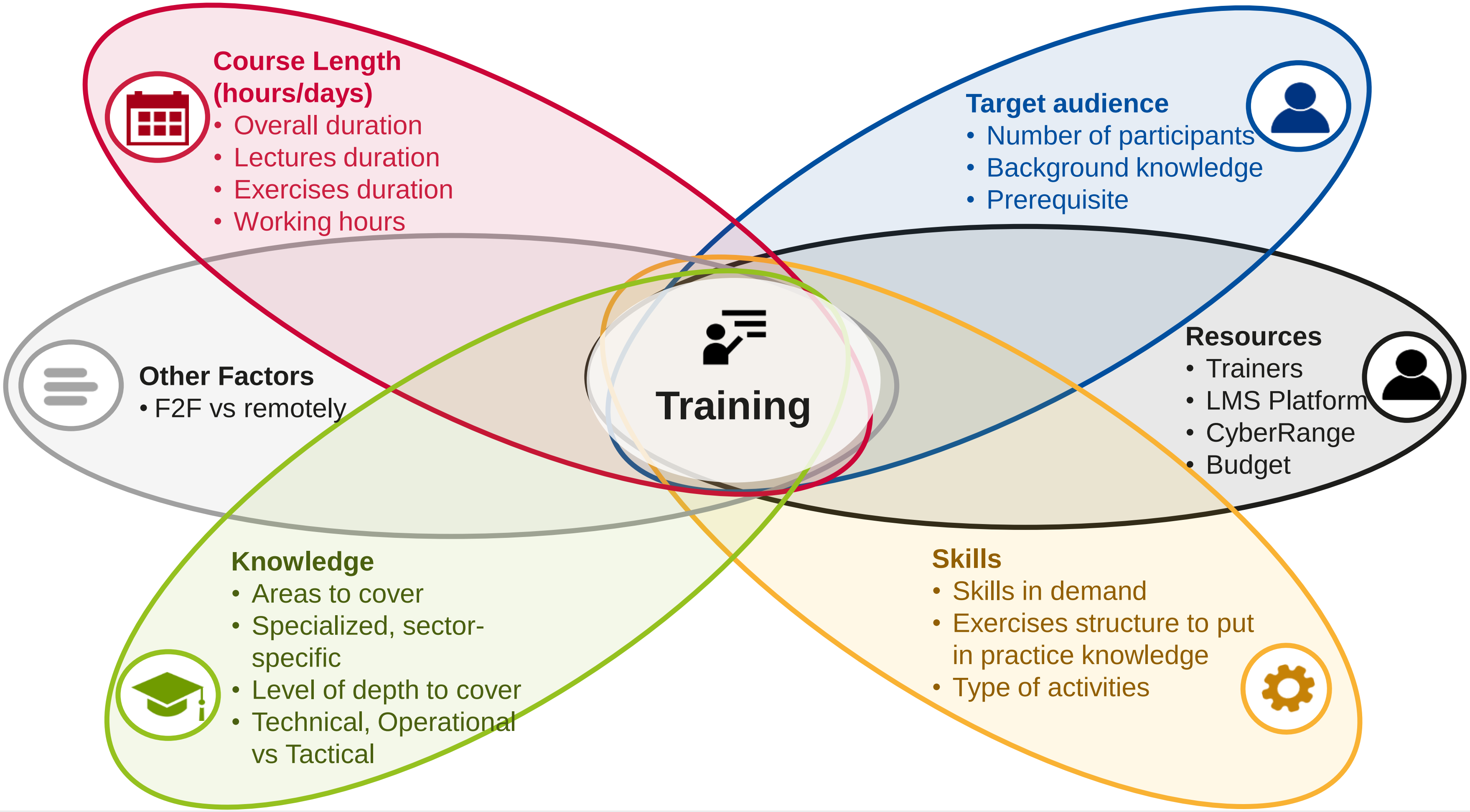
120+ cybersecurity programmes

Collaboration with the pilots of CCCN is on-going



# ENISA EXPERIENCE IN TRAININGS

# FACTORS TO CONSIDER



**Training**

**Course Length (hours/days)**
- Overall duration
- Lectures duration
- Exercises duration
- Working hours

**Target audience**
- Number of participants
- Background knowledge
- Prerequisite

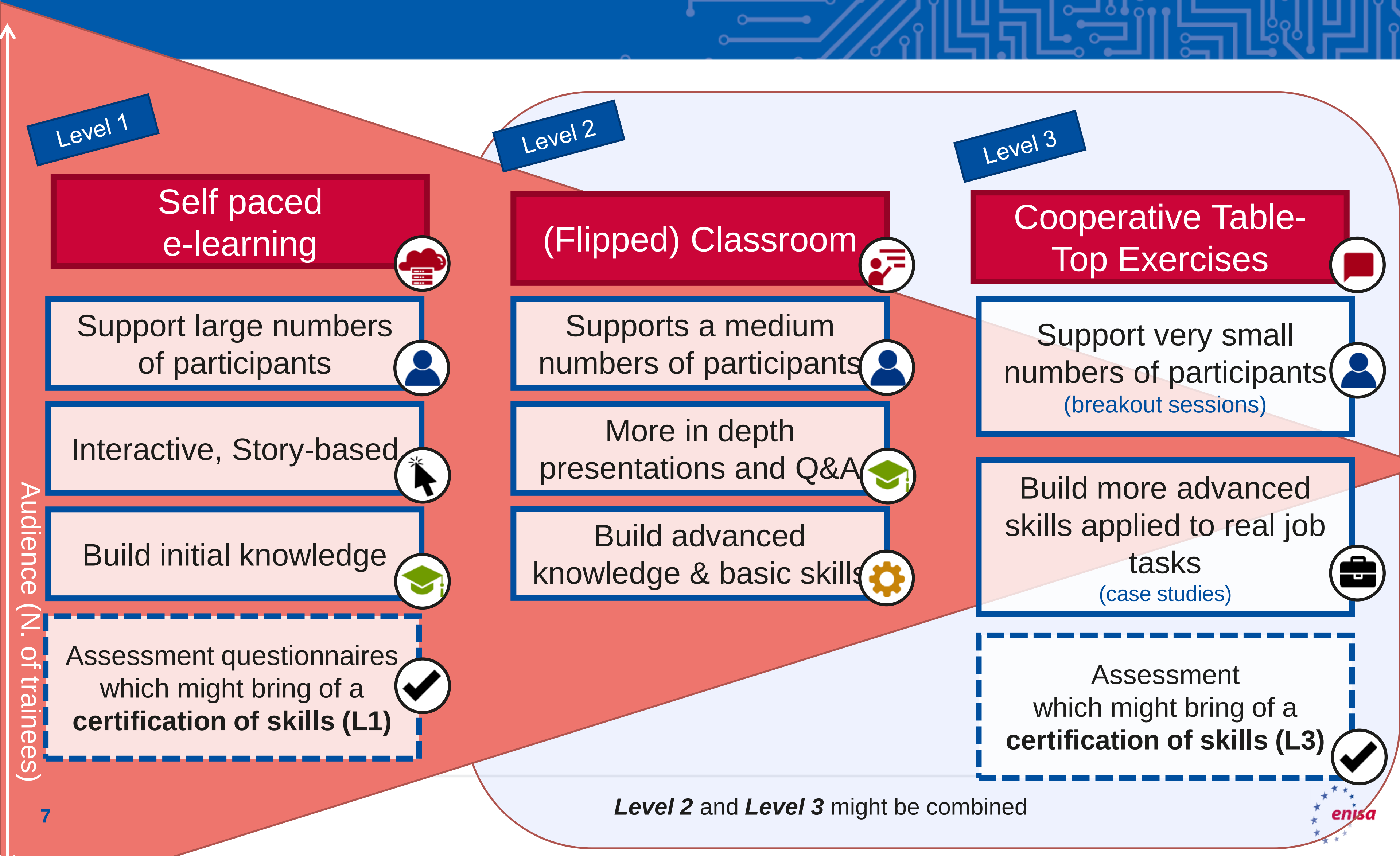
**Other Factors**
- F2F vs remotely

**Resources**
- Trainers
- LMS Platform
- CyberRange
- Budget

**Knowledge**
- Areas to cover
- Specialized, sector-specific
- Level of depth to cover
- Technical, Operational vs Tactical

**Skills**
- Skills in demand
- Exercises structure to put in practice knowledge
- Type of activities

# A PLAN FOR TRAININGS



Audience (N. of trainees)

Level 1

Self paced e-learning

Support large numbers of participants

Interactive, Story-based

Build initial knowledge

Assessment questionnaires which might bring of a **certification of skills (L1)**

Level 2

(Flipped) Classroom

Supports a medium numbers of participants

More in depth presentations and Q&A

Build advanced knowledge & basic skills

Level 3

Cooperative Table-Top Exercises

Support very small numbers of participants
(breakout sessions)

Build more advanced skills applied to real job tasks
(case studies)

Assessment which might bring of a **certification of skills (L3)**

***Level 2*** and ***Level 3*** might be combined

# BENEFITS

## Flexibility

Trainees have the ability to effectively use their time (use the elearning at their own pace in order to gain enough knowledge ).

## Engagement

Strong connections between pre-class preparation and in-class sessions ensure that trainees are engaged in both the material and the discussions. They are given more time to discuss and question aspects of the lecture. They become active participants instead of passive listeners.

## Peer-Learning and Collaboration

Collaboration among team members and across teams allow knowledge transfer between learners. Activities are be trainees-led, and the teacher’s role will be the one of a facilitator.

# Self paced e-learning

Example - ENISA e-learning

## Paul’s Success

### ✓ 1. Understand the Organization

Colleagues with key roles and responsibilities.

### ✓ 2. Learn about Information Security

Information Security Definitions and Terms, Best Practices, and Legal and Regulatory requirements.

### 3. Experience a security incident

Follow the established incident handling procedure starting from reporting to incident analysis and communication.

### 4. Understand the Security Organization

Get to know the Organizational Structure, Roles and Responsibilities and the Organization’s RASCI model.

### 5. Introduction to Risk Management

Learn about the Organization’s Risk Management process (assets identification, threats and vulnerabilities assessment,  risk treatment).

### 6. Conduct Risk Assessment

Interview key personnel to identify assets, existing security controls, threats, vulnerabilities and the associated risks.

### 7. Risk Treatment

Make a decision about risk treatment and establish an action plan for risk reduction.

### 8. Review Organizational Controls

Revise security policies and deploy a targeted awareness program.

### 9. Review Technical Controls

Audit technical controls and enhance protection with additional technical measures.

### 10. IT Security Risk Management Methodology - ITSRM

Conduct Risk Assessment based on EU ITSRM Methodology.

Ministry’s IT Security Department

# Self paced e-learning

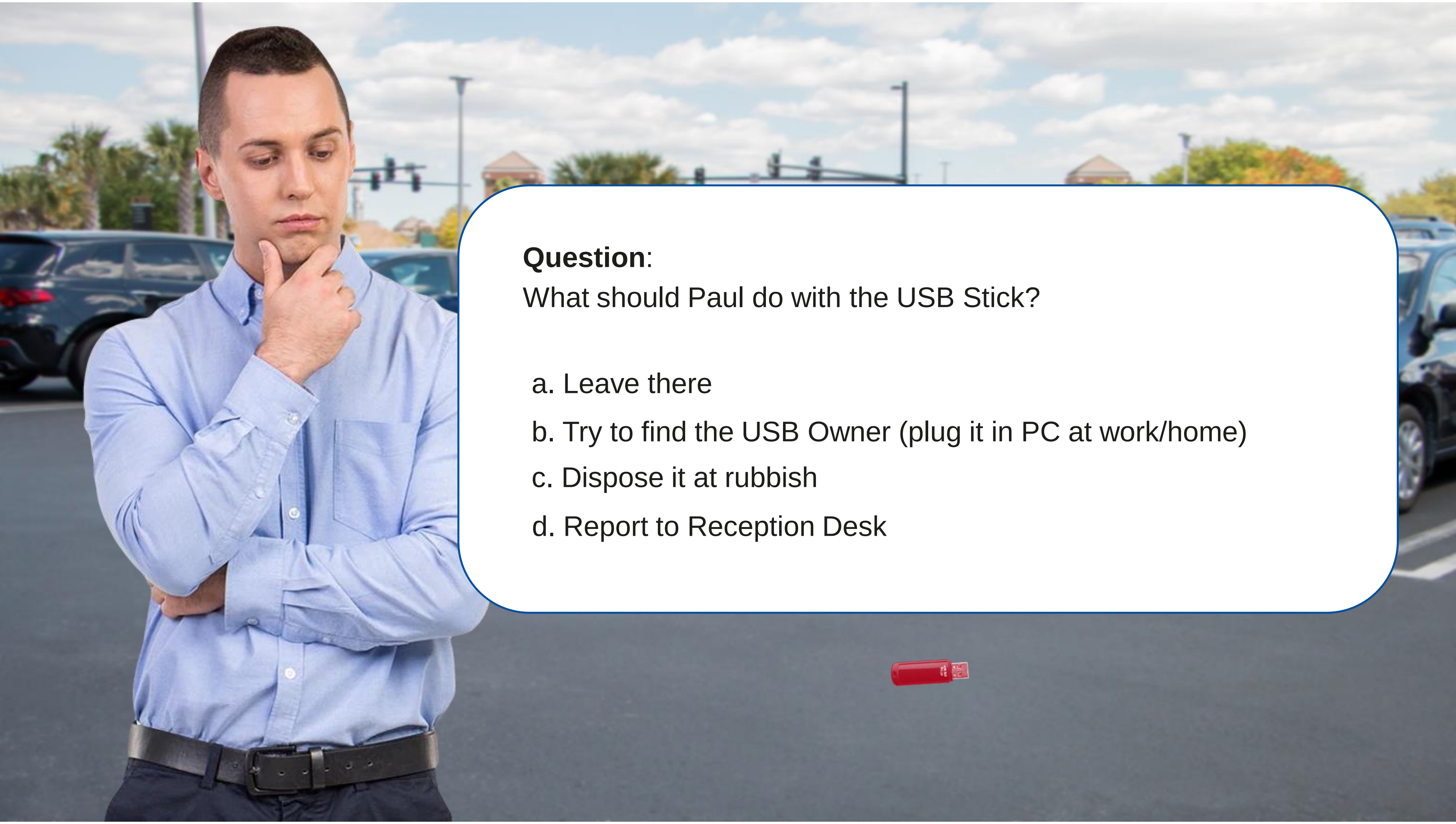
Example - ENISA e-learning

**Story Overview**

The following day Paul arrives at the Ministry's Car Park. He finds a USB stick close to the place he parked his car. He must decide what to do with the USB stick.

# Self paced e-learning

Example - ENISA e-learning



**Question**:
What should Paul do with the USB Stick?

a. Leave there

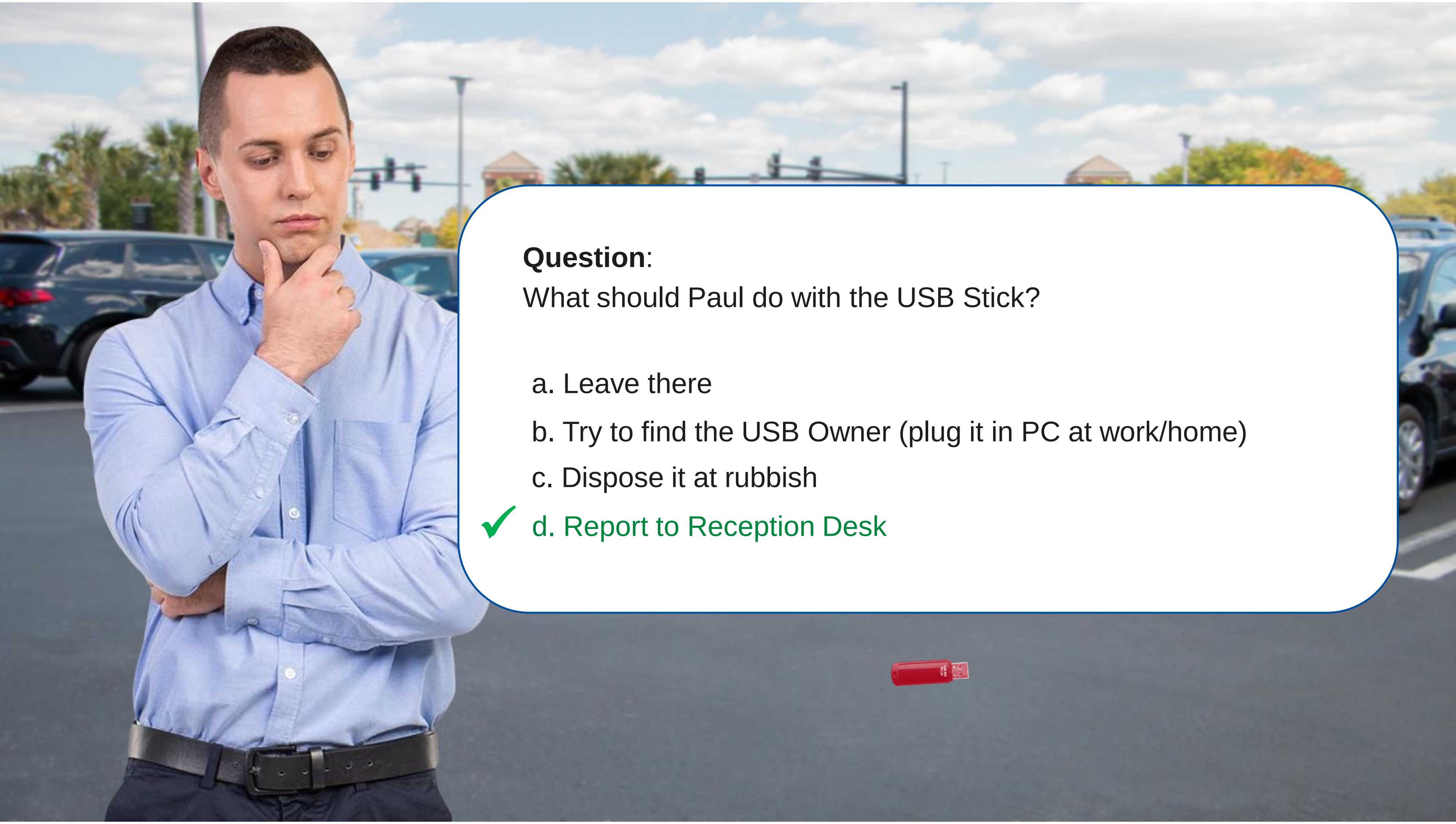
b. Try to find the USB Owner (plug it in PC at work/home)

c. Dispose it at rubbish

d. Report to Reception Desk

# Self paced e-learning

Example - ENISA e-learning



**Question**:
What should Paul do with the USB Stick?

a. Leave there

b. Try to find the USB Owner (plug it in PC at work/home)

c. Dispose it at rubbish

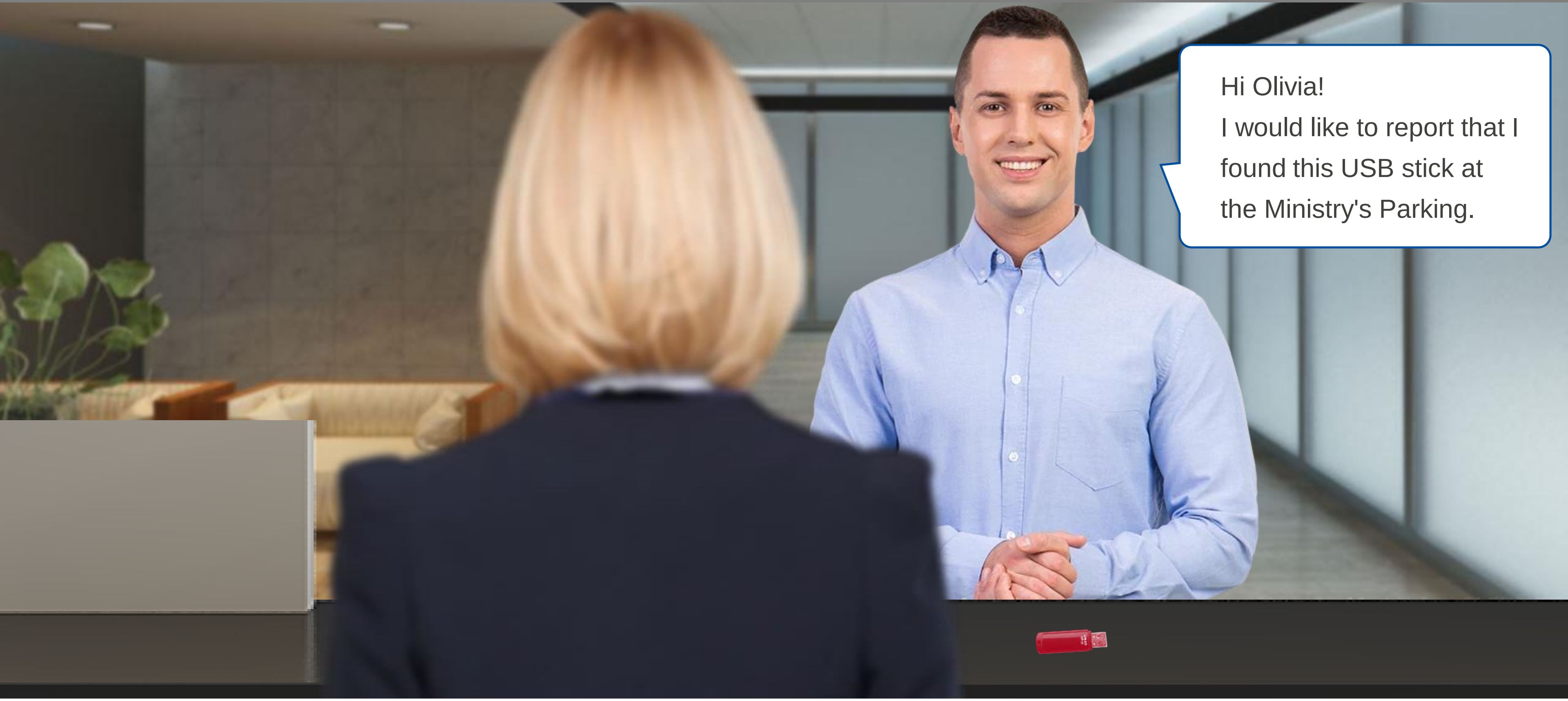
✓ d. Report to Reception Desk

# Self paced e-learning

Example - ENISA e-learning

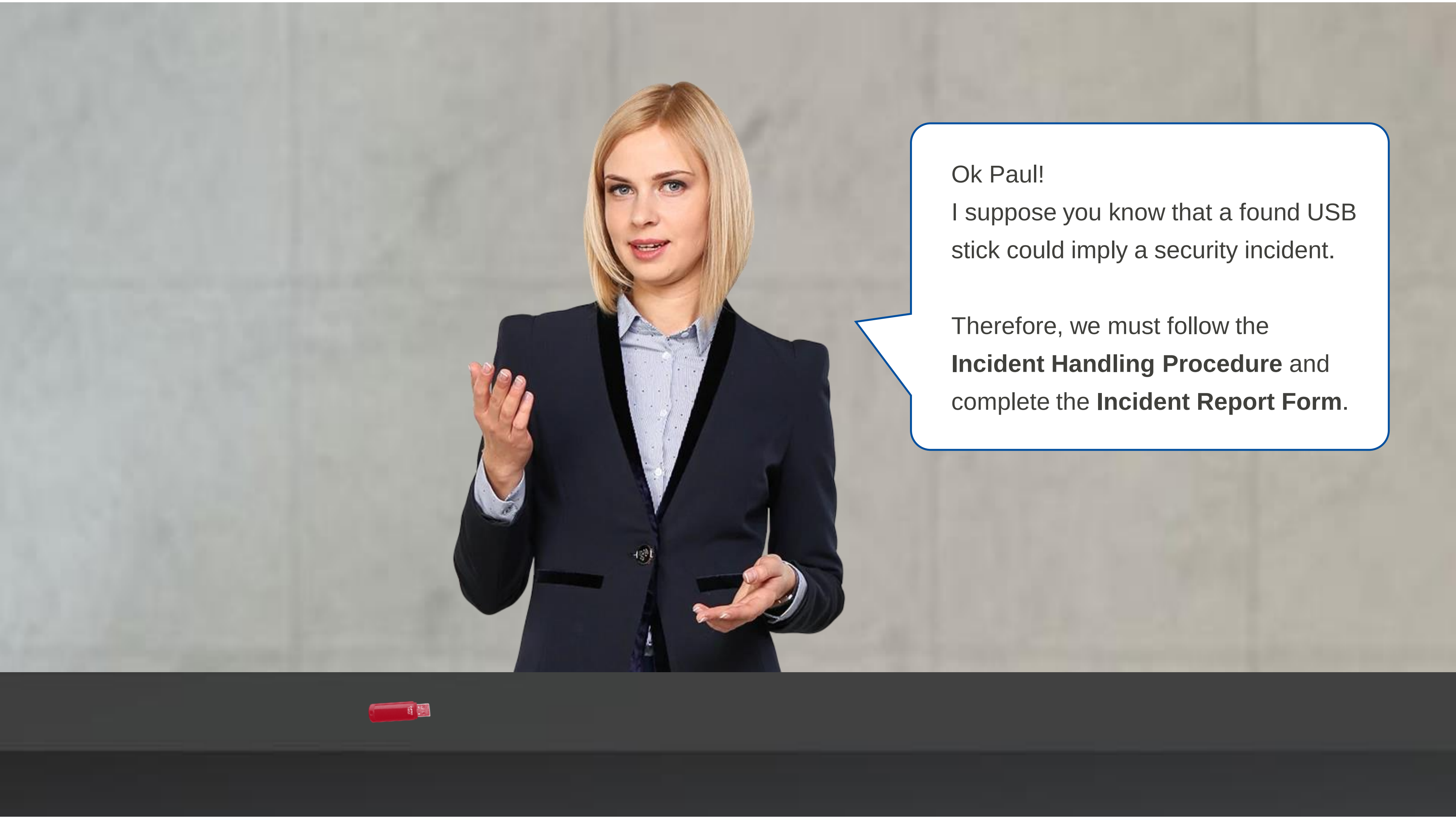
**Story Overview**

The following day Paul arrives at the Ministry’s Car Park. He finds a USB stick close to the place he parked his car. He must decide what to do with the USB stick.


Hi Olivia!
I would like to report that I found this USB stick at the Ministry's Parking.

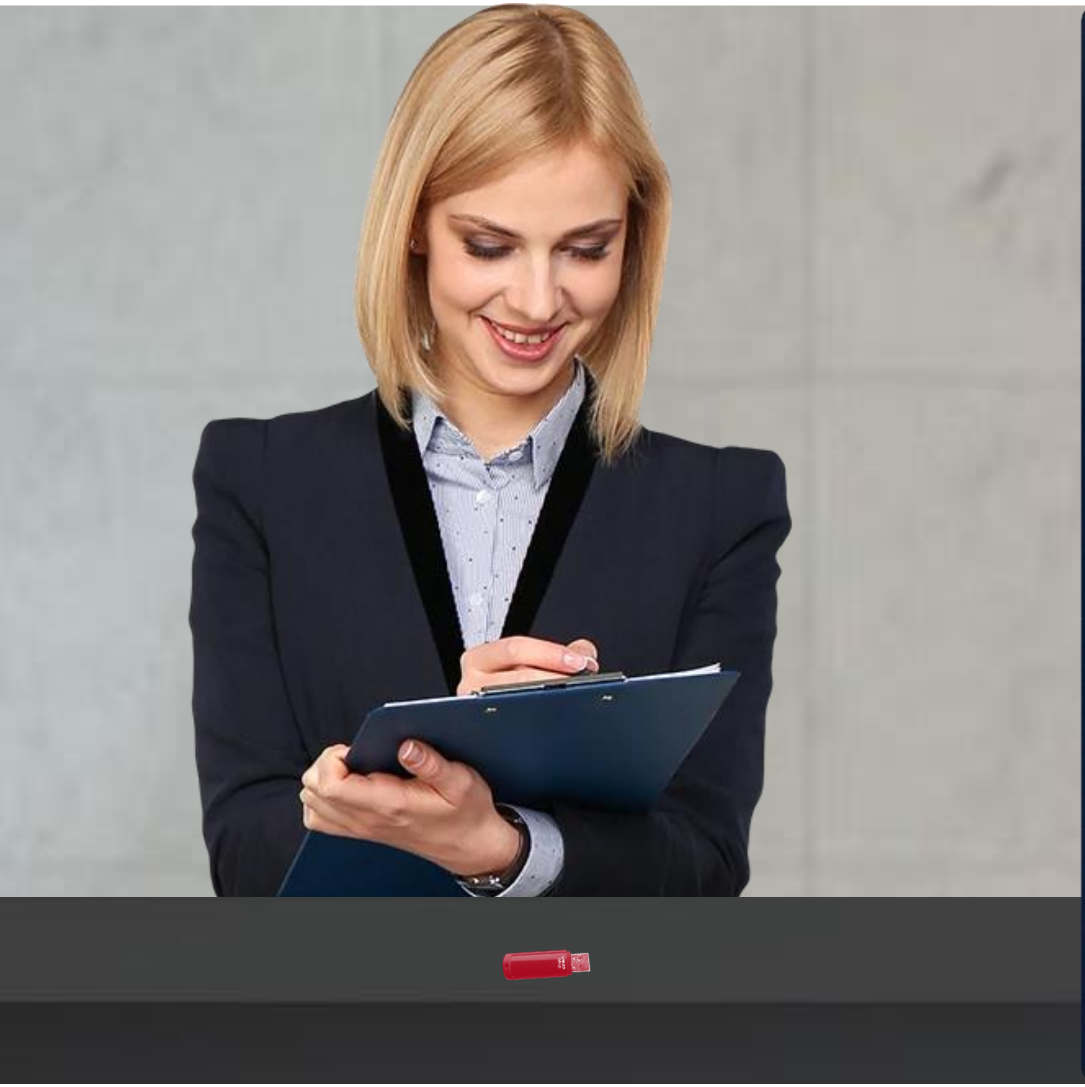
# Self paced e-learning

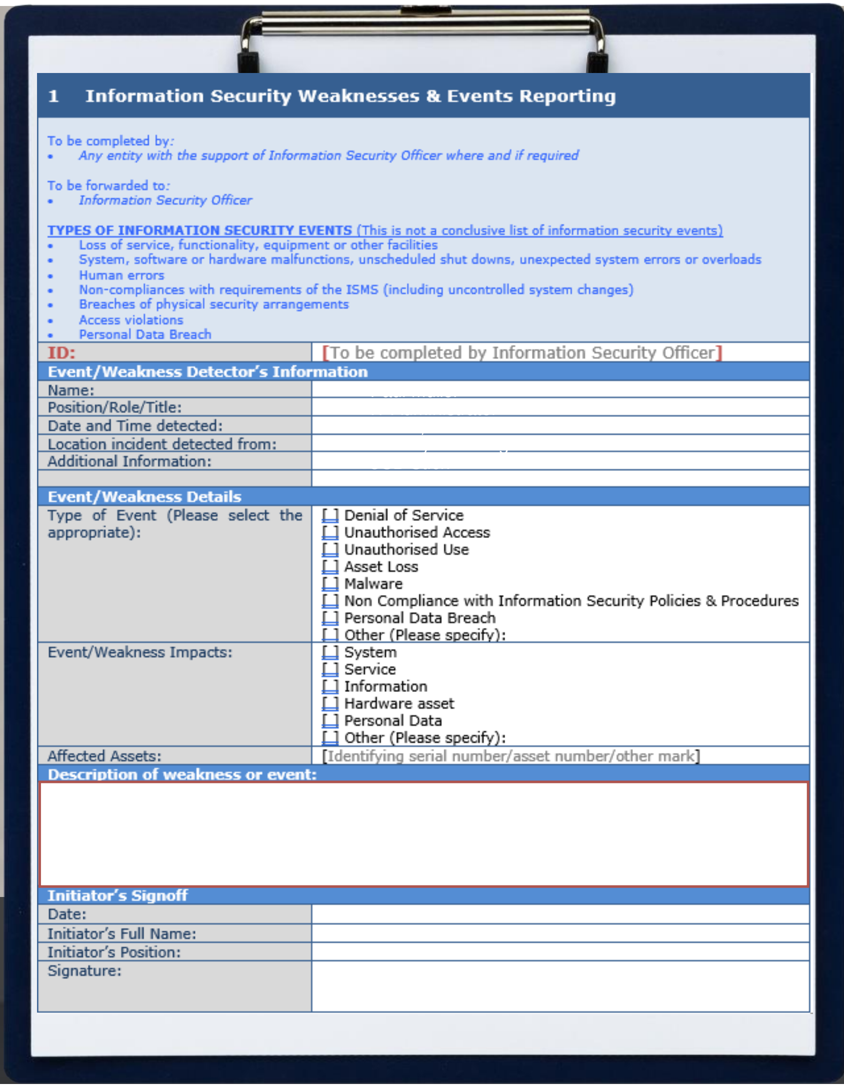
Example - ENISA e-learning



Ok Paul!
I suppose you know that a found USB stick could imply a security incident.

Therefore, we must follow the **Incident Handling Procedure** and complete the **Incident Report Form**.





## 1 Information Security Weaknesses & Events Reporting

To be completed by:

- *Any entity with the support of Information Security Officer where and if required*

To be forwarded to:

- *Information Security Officer*

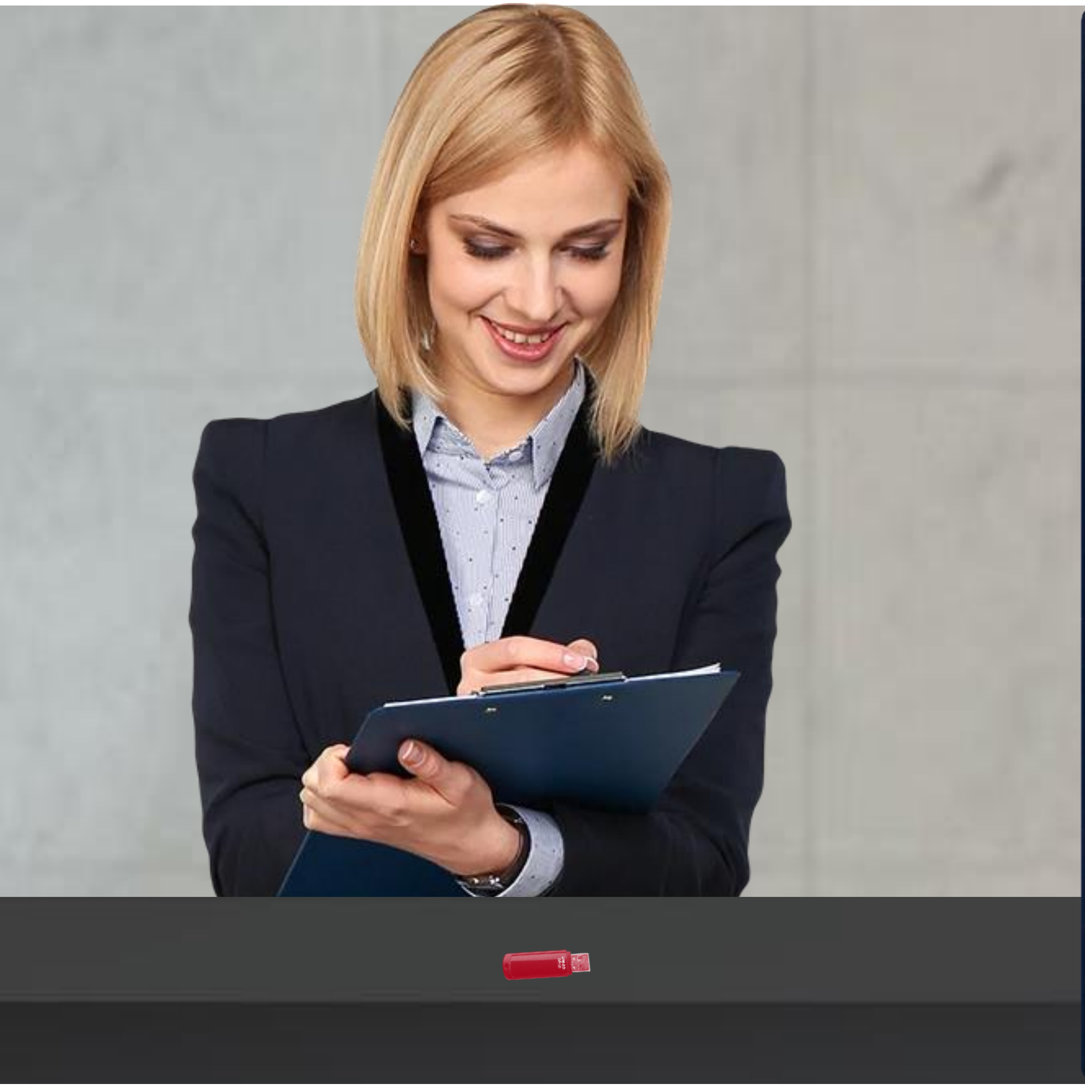
**TYPES OF INFORMATION SECURITY EVENTS** (This is not a conclusive list of information security events)

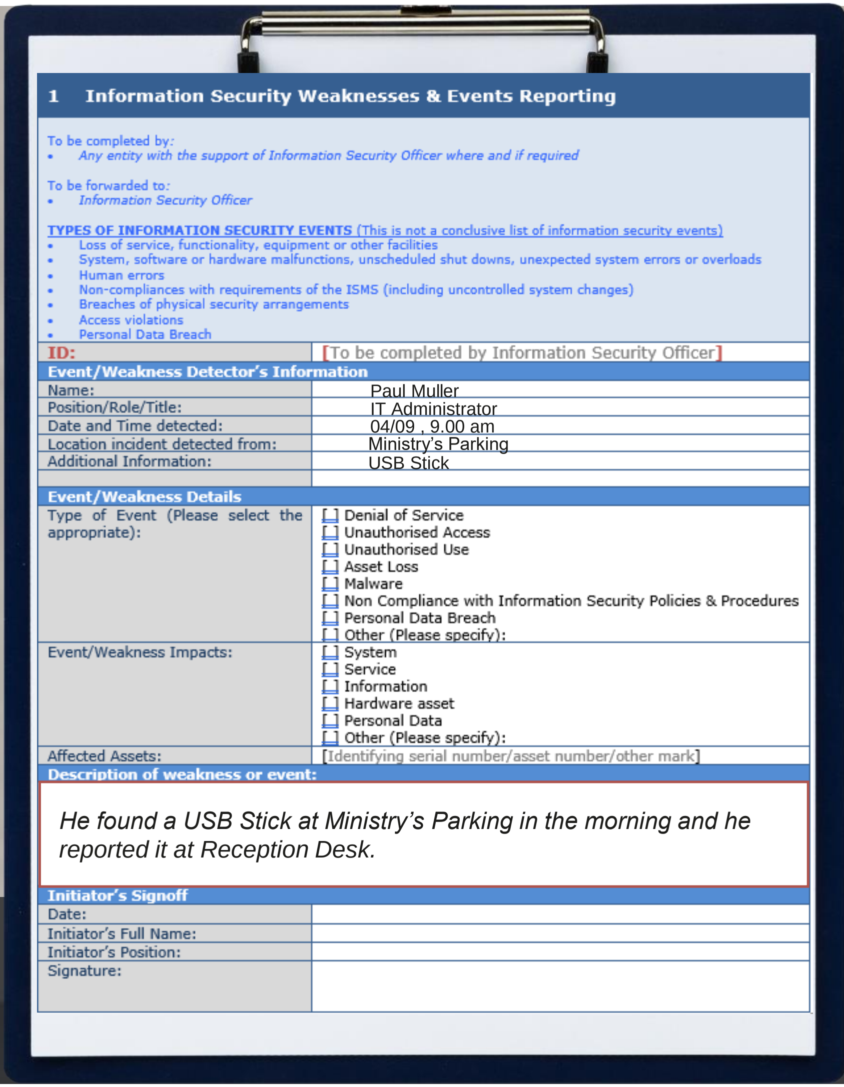
- Loss of service, functionality, equipment or other facilities
- System, software or hardware malfunctions, unscheduled shut downs, unexpected system errors or overloads
- Human errors
- Non-compliances with requirements of the ISMS (including uncontrolled system changes)
- Breaches of physical security arrangements
- Access violations
- Personal Data Breach

| | |
|---|---|
| **ID:** | [To be completed by Information Security Officer] |
| **Event/Weakness Detector's Information** | |
| Name: | |
| Position/Role/Title: | |
| Date and Time detected: | |
| Location incident detected from: | |
| Additional Information: | |
| **Event/Weakness Details** | |
| Type of Event (Please select the appropriate): | □ Denial of Service<br>□ Unauthorised Access<br>□ Unauthorised Use<br>□ Asset Loss<br>□ Malware<br>□ Non Compliance with Information Security Policies & Procedures<br>□ Personal Data Breach<br>□ Other (Please specify): |
| Event/Weakness Impacts: | □ System<br>□ Service<br>□ Information<br>□ Hardware asset<br>□ Personal Data<br>□ Other (Please specify): |
| Affected Assets: | [Identifying serial number/asset number/other mark] |
| **Description of weakness or event:** | |
| | |
| **Initiator's Signoff** | |
| Date: | |
| Initiator's Full Name: | |
| Initiator's Position: | |
| Signature: | |

# Self paced e-learning

Example - ENISA e-learning





## 1 Information Security Weaknesses & Events Reporting

To be completed by:

- *Any entity with the support of Information Security Officer where and if required*

To be forwarded to:

- *Information Security Officer*

**TYPES OF INFORMATION SECURITY EVENTS** (This is not a conclusive list of information security events)

- Loss of service, functionality, equipment or other facilities
- System, software or hardware malfunctions, unscheduled shut downs, unexpected system errors or overloads
- Human errors
- Non-compliances with requirements of the ISMS (including uncontrolled system changes)
- Breaches of physical security arrangements
- Access violations
- Personal Data Breach

| | |
|---|---|
| **ID:** | [To be completed by Information Security Officer] |
| **Event/Weakness Detector's Information** | |
| Name: | Paul Muller |
| Position/Role/Title: | IT Administrator |
| Date and Time detected: | 04/09 , 9.00 am |
| Location incident detected from: | Ministry's Parking |
| Additional Information: | USB Stick |
| **Event/Weakness Details** | |
| Type of Event (Please select the appropriate): | □ Denial of Service<br>□ Unauthorised Access<br>□ Unauthorised Use<br>□ Asset Loss<br>□ Malware<br>□ Non Compliance with Information Security Policies & Procedures<br>□ Personal Data Breach<br>□ Other (Please specify): |
| Event/Weakness Impacts: | □ System<br>□ Service<br>□ Information<br>□ Hardware asset<br>□ Personal Data<br>□ Other (Please specify): |
| Affected Assets: | [Identifying serial number/asset number/other mark] |
| **Description of weakness or event:** | |
| *He found a USB Stick at Ministry's Parking in the morning and he reported it at Reception Desk.* | |
| **Initiator's Signoff** | |
| Date: | |
| Initiator's Full Name: | |
| Initiator's Position: | |
| Signature: | |

# Self paced e-learning

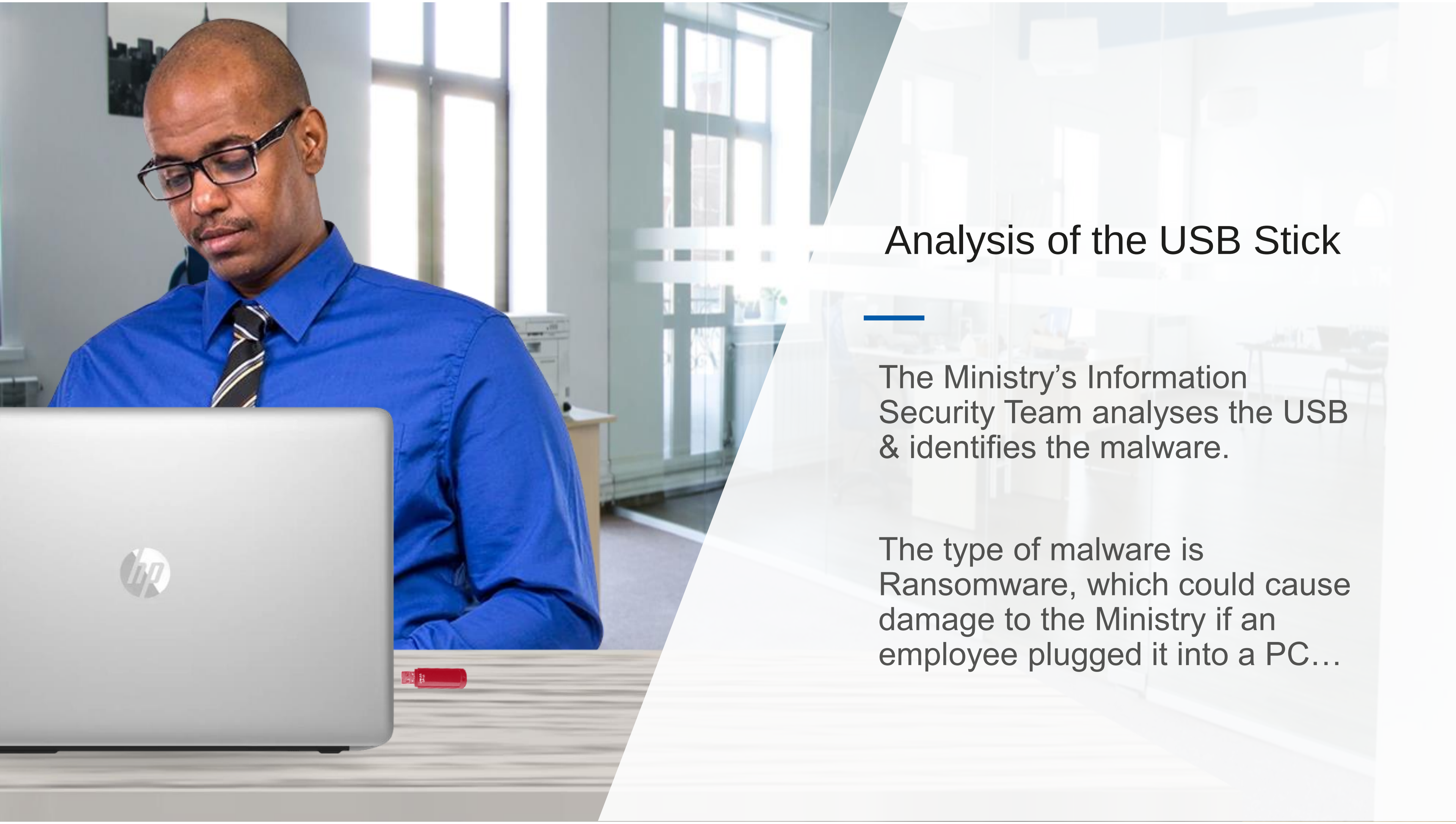
**Story Overview**

Olivia contacts the Security Team and delivers the USB Stick to Mr. Frank, who is responsible of evaluating the potential security incident.

Hi Mr. Frank!
This morning, a colleague of ours, Mr. Paul Muller, found this device at the Ministry’s Car Park.
Thank you, Olivia!
Our Security Team will analyze the device.

# Self paced e-learning

Example - ENISA e-learning



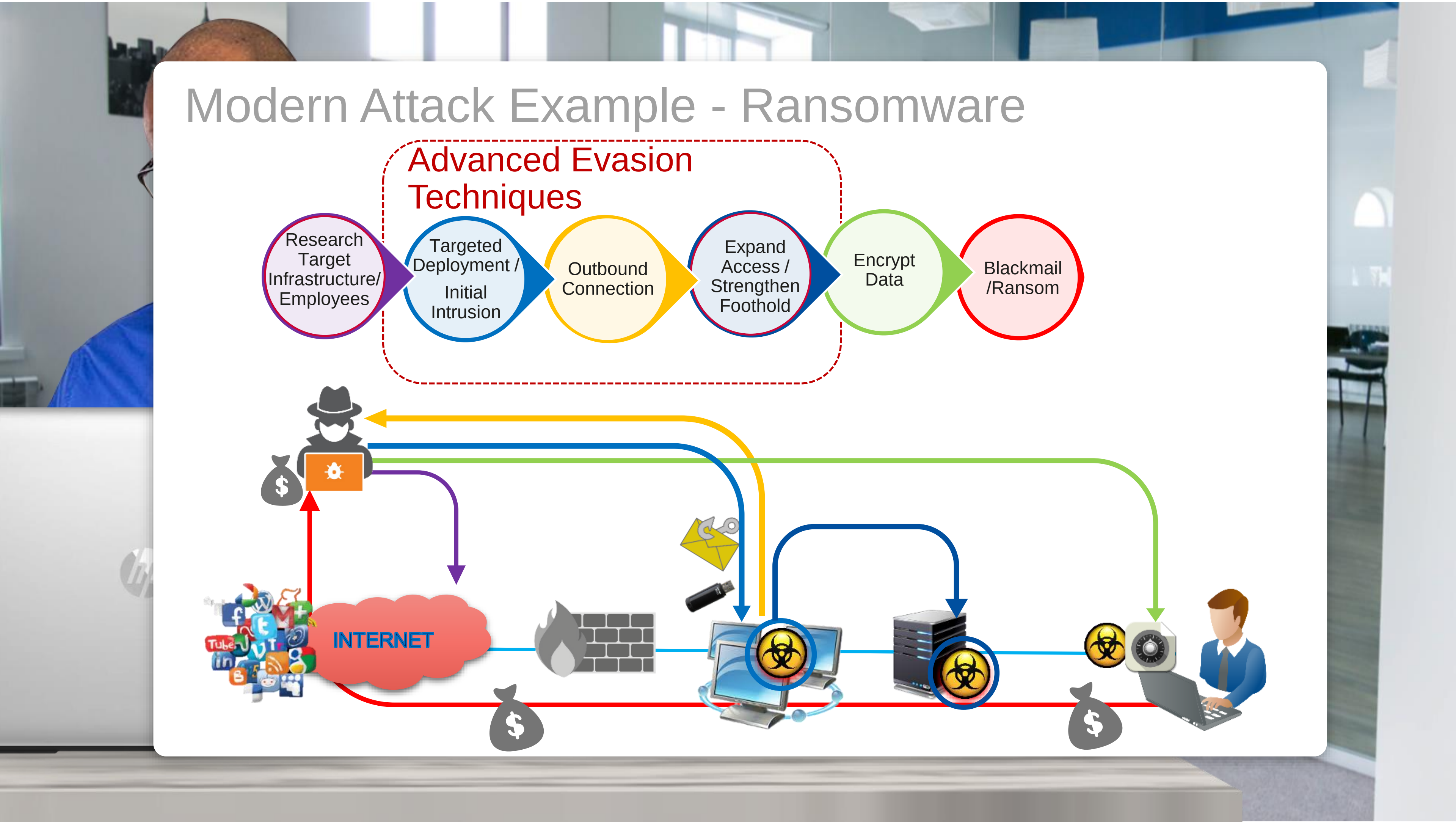
## Analysis of the USB Stick

The Ministry’s Information Security Team analyses the USB & identifies the malware.

The type of malware is Ransomware, which could cause damage to the Ministry if an employee plugged it into a PC…

# Self paced e-learning

Example - ENISA e-learning



## Modern Attack Example - Ransomware

Advanced Evasion Techniques

Research Target Infrastructure/ Employees

Targeted Deployment / Initial Intrusion

Outbound Connection

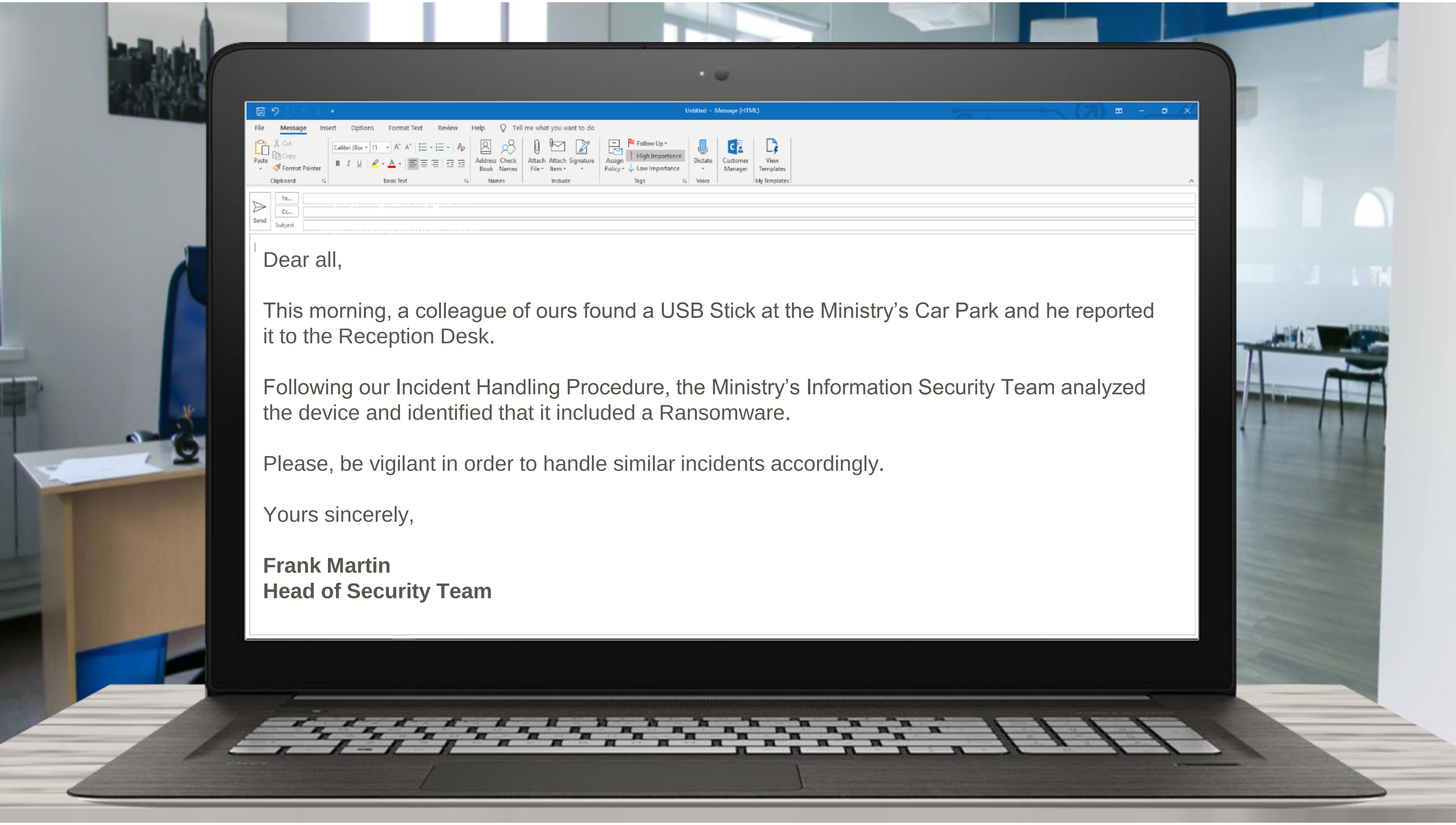
Expand Access / Strengthen Foothold

Encrypt Data

Blackmail /Ransom

# Self paced e-learning

## Example - ENISA e-learning



Dear all,

This morning, a colleague of ours found a USB Stick at the Ministry’s Car Park and he reported it to the Reception Desk.

Following our Incident Handling Procedure, the Ministry’s Information Security Team analyzed the device and identified that it included a Ransomware.

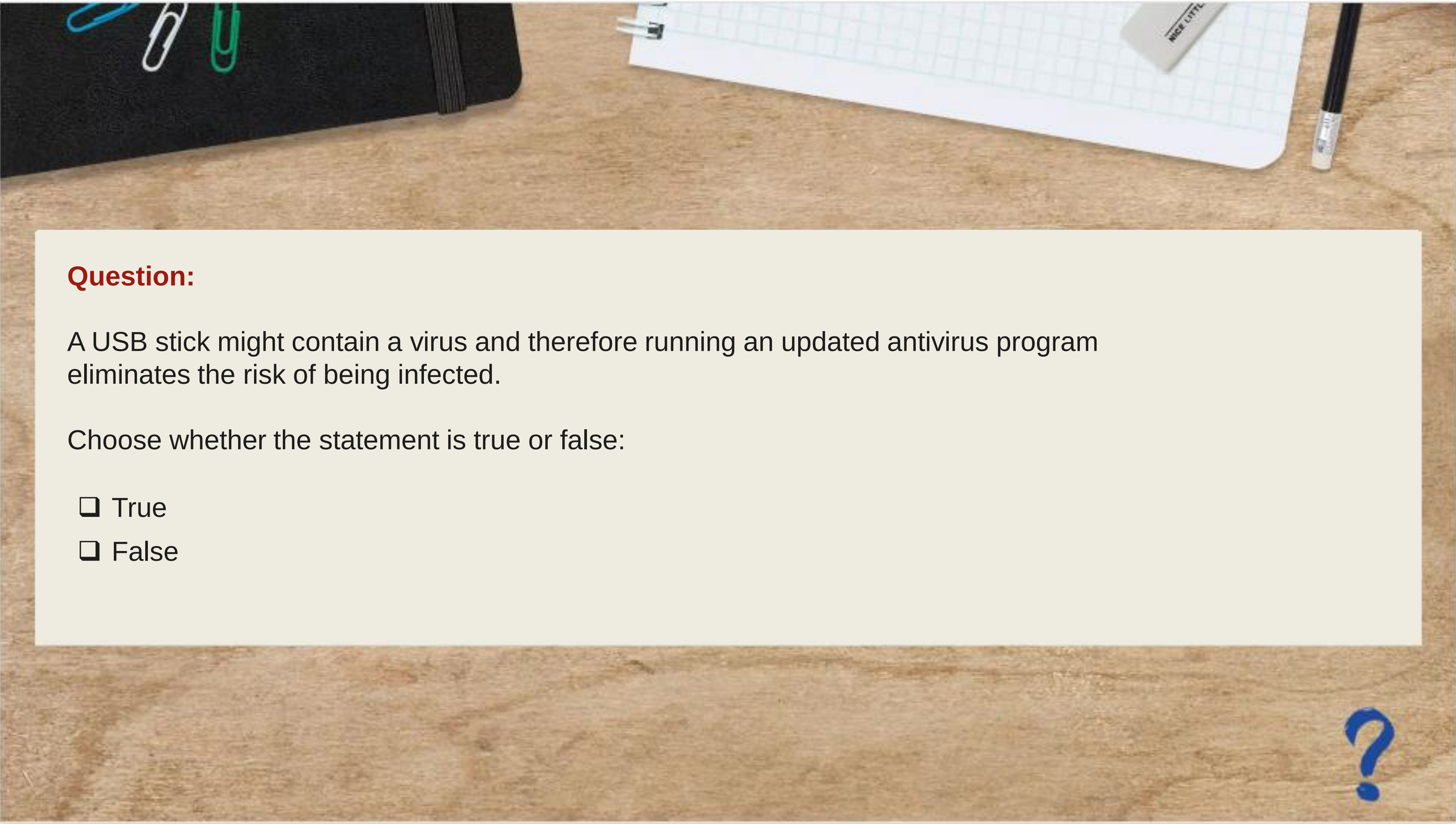
Please, be vigilant in order to handle similar incidents accordingly.

Yours sincerely,

**Frank Martin**
**Head of Security Team**

# Self paced e-learning

## Example - ENISA e-learning



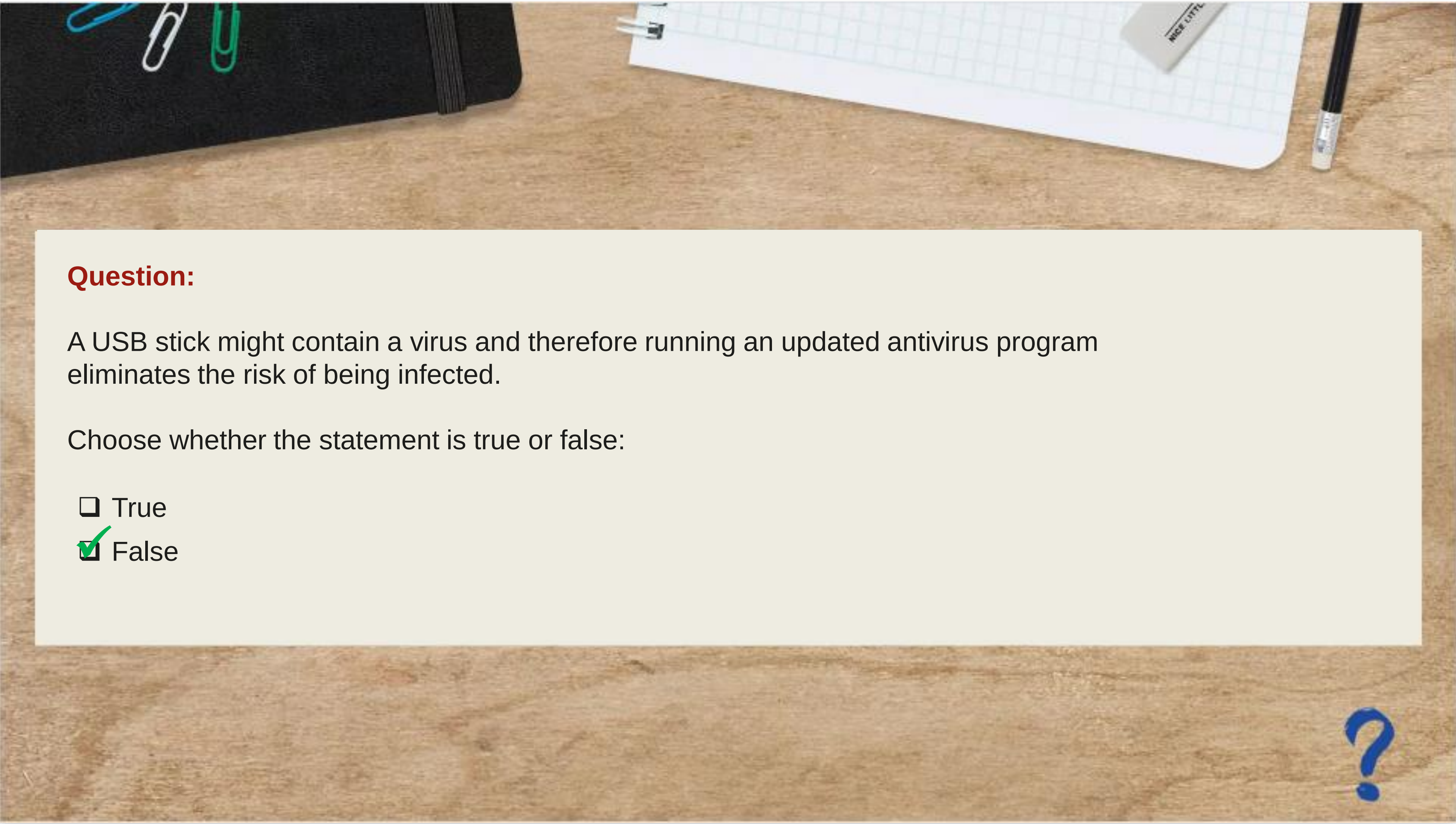
**Question:**

A USB stick might contain a virus and therefore running an updated antivirus program eliminates the risk of being infected.

Choose whether the statement is true or false:

- ☐ True
- ☐ False

# Self paced e-learning



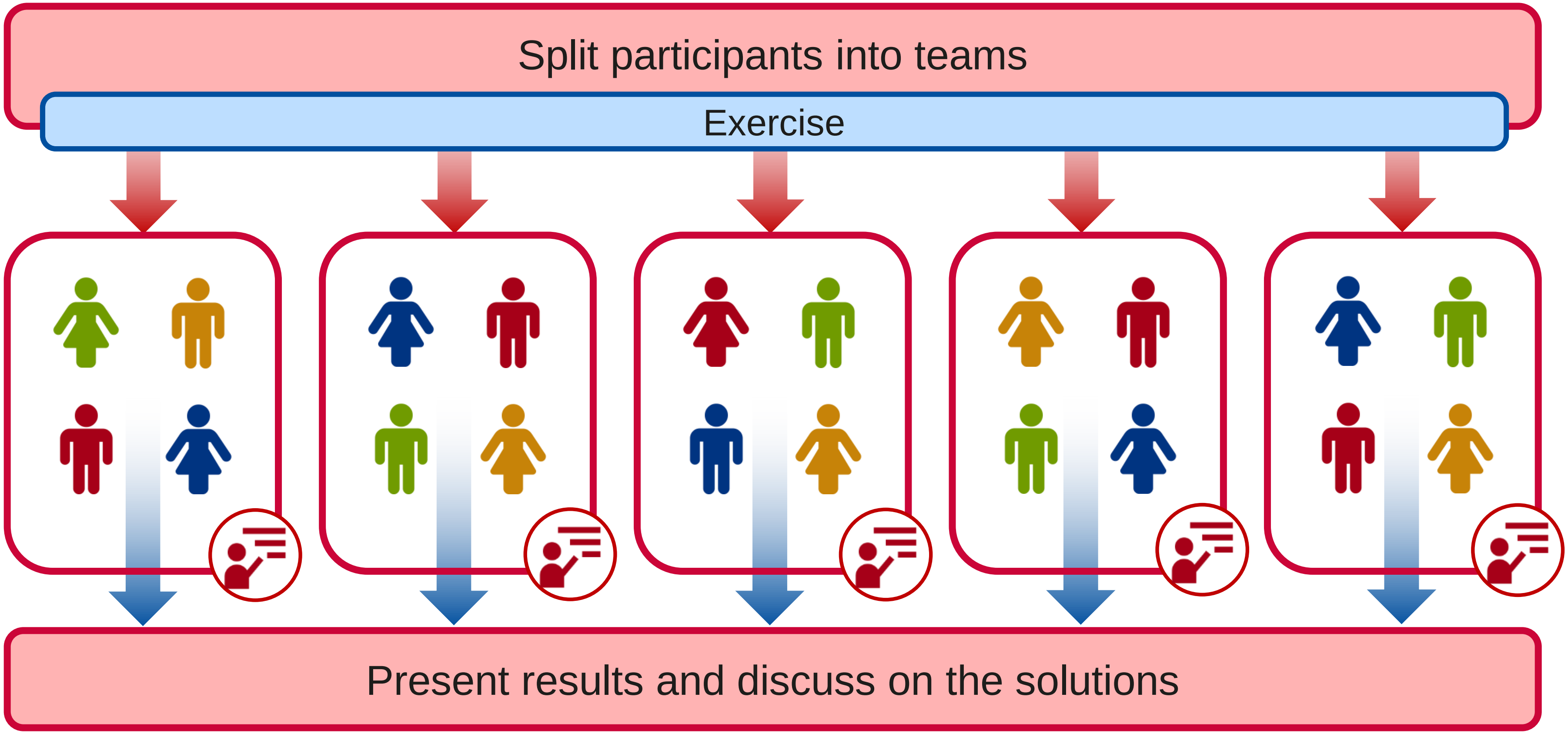
**Question:**

A USB stick might contain a virus and therefore running an updated antivirus program eliminates the risk of being infected.

Choose whether the statement is true or false:

- □ True
- ☑ False

# COOPERATIVE TABLE-TOP EXERCISES

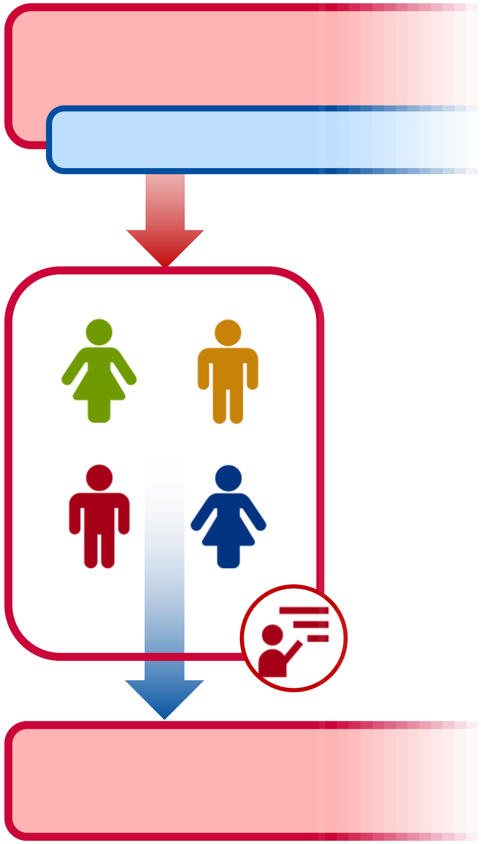


Split participants into teams

Exercise

Present results and discuss on the solutions

# COOPERATIVE TABLE-TOP EXERCISES



## Each team

- A trainer act as a facilitator
- Participants collaborate to complete the exercise
  - Discuss the exercise
  - Share screen and fill in their report/results
  - Search through the provided documents

# THANK YOU FOR YOUR ATTENTION ☺

**European Union Agency for Cybersecurity**
Vasilissis Sofias Str 1, Maroussi
Attiki, Greece

☎ +30 28 14 40 9711

✉ Fabio.DiFranco@enisa.europa.eu

🌐 www.enisa.europa.eu