LESSON

CYBERSECURITY DEFENDER

AUTHOR

SERGIO ELVIRA PEREZ

CODEARTS SOLUTIONS

CYBERSECURITY DEFENDER

Cybersecurity Defender places learners inside a simulated security operations centre. Teams investigate safe, pre-prepared incidents, interpret logs and network evidence, prioritise responses and document mitigation decisions without interacting with real external targets.

Subject and level

Advanced VET learners in systems administration, networking or cybersecurity who have introductory knowledge of logs, network traffic and secure configuration.

Connection to curriculum

The activity reinforces incident analysis, network monitoring, vulnerability awareness, system hardening and technical reporting. It also supports ethical practice, evidence-based decision-making and coordinated response procedures.

Didactic and pedagogic considerations

Role rotation and timed incidents create authentic decision pressure while a closed laboratory keeps the activity safe. The teacher can assess not only whether a threat is identified, but how teams communicate evidence, prioritise risk and justify containment actions.

Time estimate

3 hours

CYBERSECURITY DEFENDER

Group size

15-25 students

Overall introduction to exercise

Students form small cyber-response units with analyst, system, incident and reporting responsibilities. They work only with intentionally vulnerable virtual machines and prepared traffic captures, progressing through alerts of increasing complexity.

The exercise treats cybersecurity as a coordinated professional process rather than a collection of tools. Technical analysis, clear escalation and accurate reporting are all necessary to complete the mission successfully.

CYBERSECURITY DEFENDER

Exercise as presented to the students

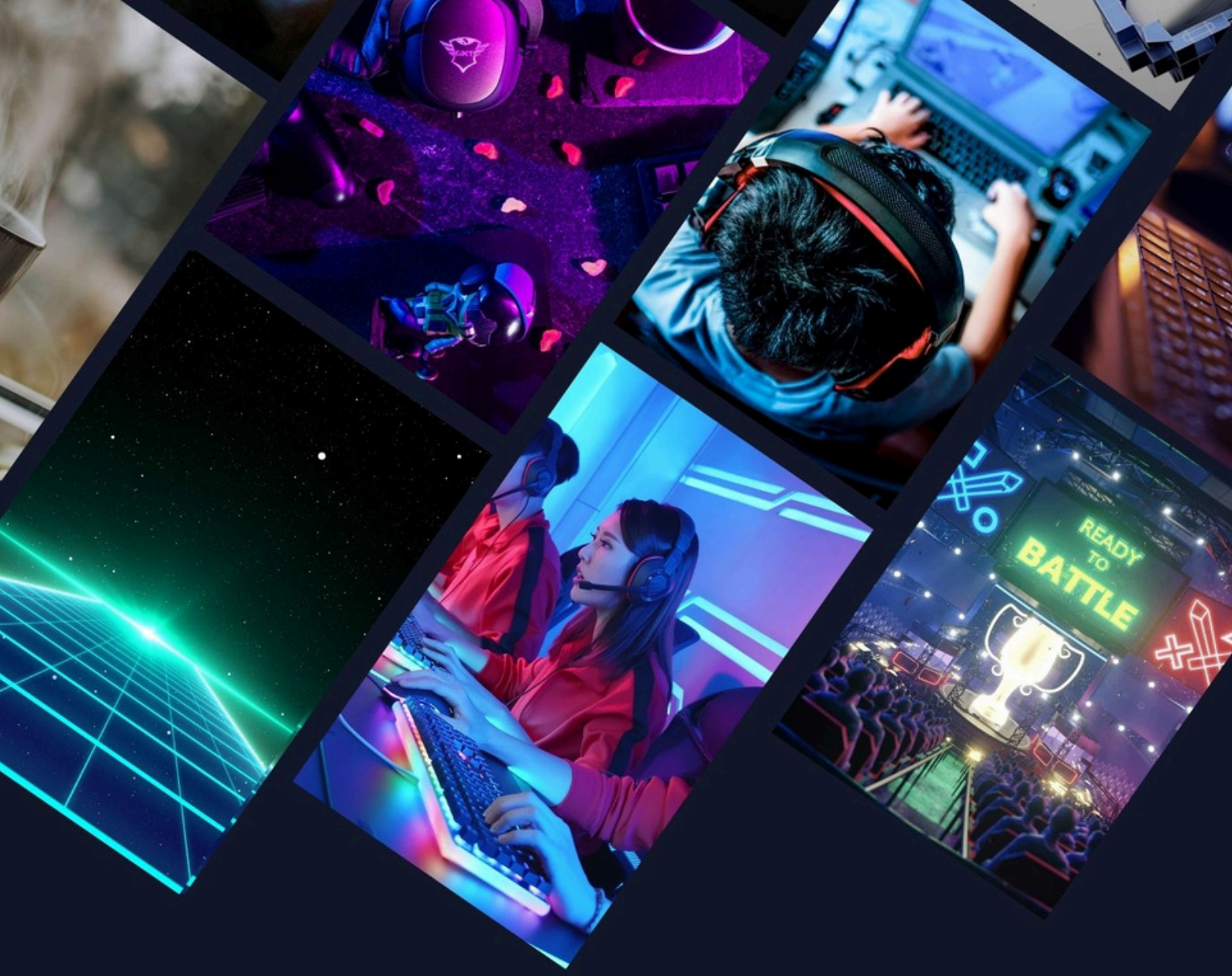
The classroom was organised as a small security operations centre. Teams of four received a closed virtual laboratory containing two intentionally vulnerable machines, prepared log files and a packet capture. Roles were assigned for analyst, incident responder, system administrator and report writer, with the reminder that all work must remain inside the training environment.

The first alert involved repeated failed logins followed by a successful connection from an unusual source. Students inspected authentication logs and a Wireshark capture, identified the sequence of events and recorded evidence before taking any action. The teacher checked that conclusions were supported by data rather than guesses.

A second incident introduced a suspicious process and an insecure service configuration. Teams had to decide what to contain first, propose a safe mitigation and explain the possible business impact of shutting down a service. A timed incident card then added a phishing report so groups had to prioritise rather than pursue every clue at once.

Throughout the simulation, all actions were written in an incident timeline. If a team made a disruptive decision, such as stopping the wrong service, the scenario reflected the consequence and they had to recover. This created a realistic reason to communicate before acting and to distinguish investigation from remediation.

Each cyber unit finished by presenting a short incident report containing evidence, impact, containment and prevention recommendations. The teacher compared technical accuracy with clarity of communication. Students experienced how cybersecurity combines analysis, calm decision-making, teamwork and ethical responsibility, not simply the use of security tools.



EASIE
Esports as Accelerator for Social Inclusive Education

E-SPORT AS ACCELERATOR FOR SOCIAL INCLUSIVE EDUCATION

WWW.EASIE.GG

Co-funded by
the European Union

FUNDED BY THE EUROPEAN UNION. VIEWS AND OPINIONS EXPRESSED ARE HOWEVER THOSE OF THE AUTHOR(S) ONLY AND DO NOT NECESSARILY REFLECT THOSE OF THE EUROPEAN UNION OR THE EUROPEAN EDUCATION AND CULTURE EXECUTIVE AGENCY (EACEA). NEITHER THE EUROPEAN UNION NOR EACEA CAN BE HELD RESPONSIBLE FOR THEM.