DEFENDERS

Defending VET Students within Cybersecurity Innovation

MODULE 5: INCIDENT RESPONSE AND MANAGEMENT

Project No: 2025-1-PL01-KA210-VET-000363642

www.defenders-project.eu

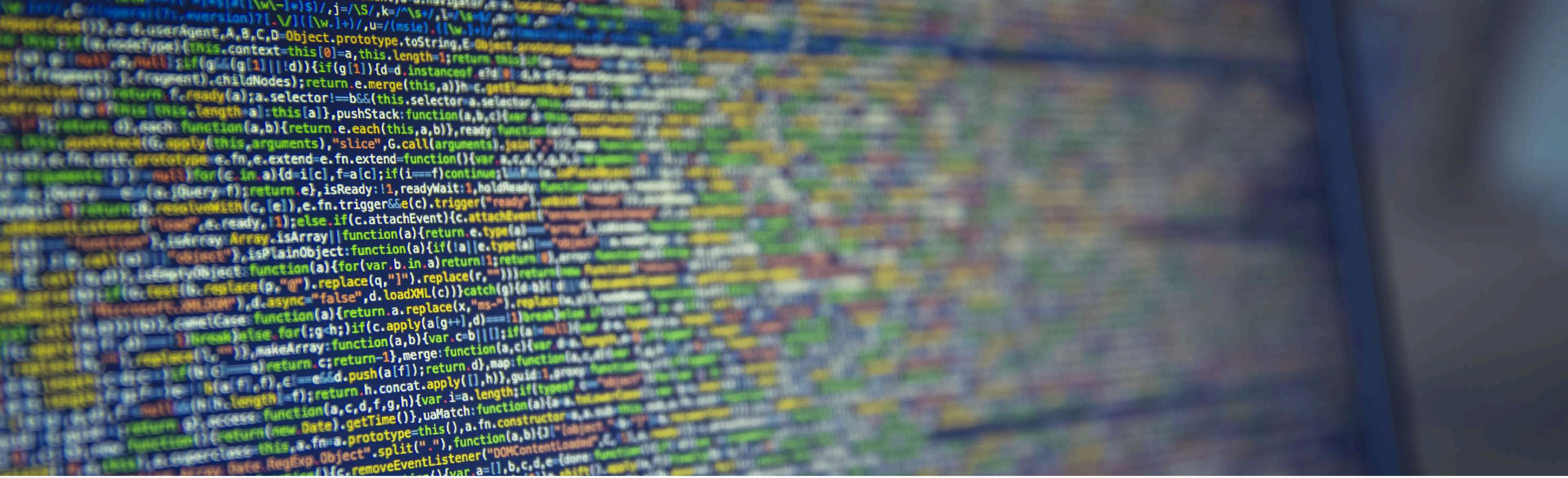
FUNDACJA ROZWOJU SPOŁECZNEGO CIVITAS

M.S.A. ΚΕΝΤΡΟ ΔΙΑ ΒΙΟΥ ΜΑΘΗΣΗΣ

NIKOLA KAREV State High School & VET Centre Strumica

Co-funded by the European Union

Funded by the EU. The views and opinions expressed are solely those of the author(s) and do not necessarily reflect the views and opinions of the European Union or the Foundation for the Development of the Education System. Neither the European Union nor the Foundation for the Development of the Education System are responsible.



MODULE ROADMAP

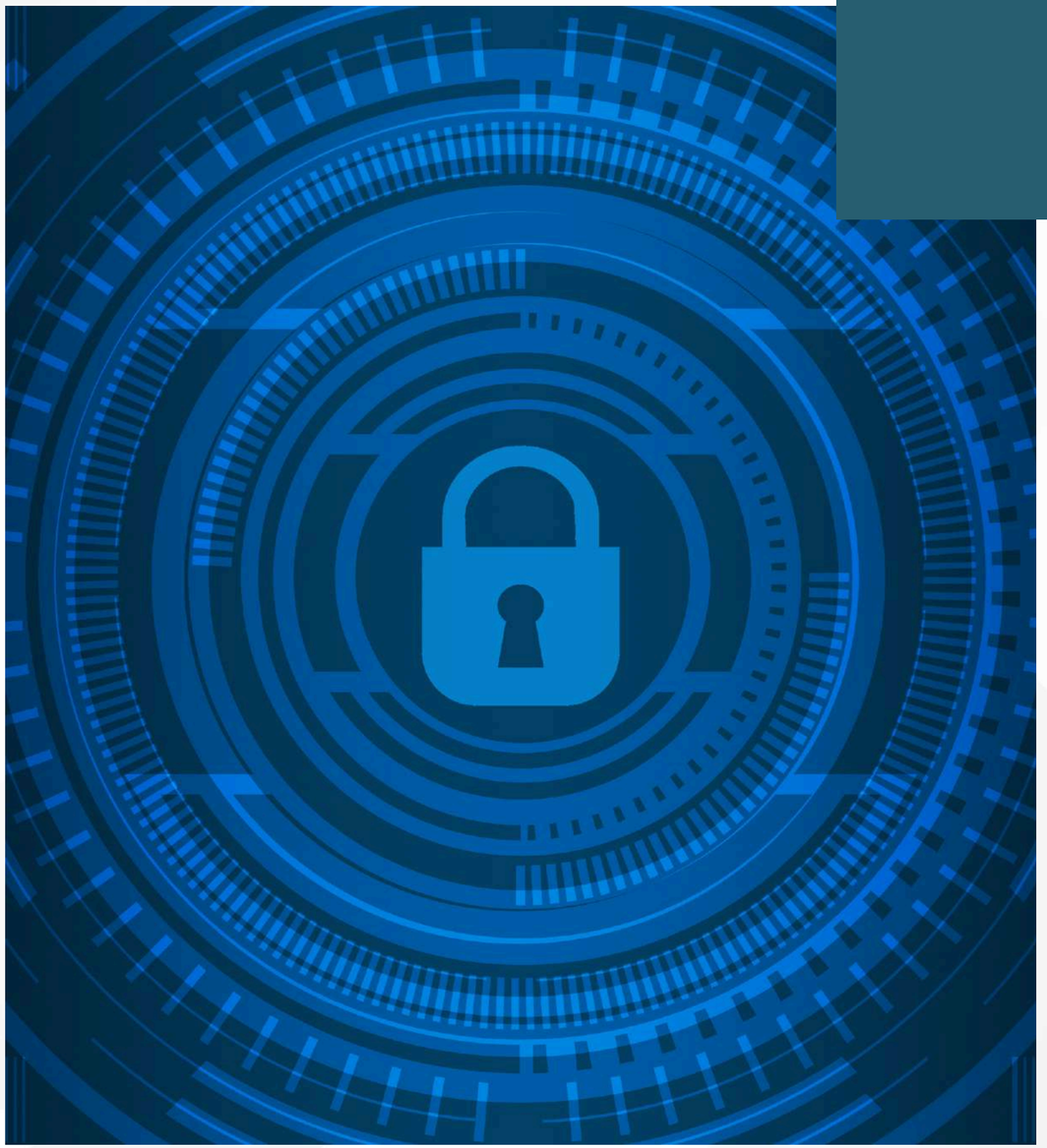
LEARNING PATH AND STRUCTURE

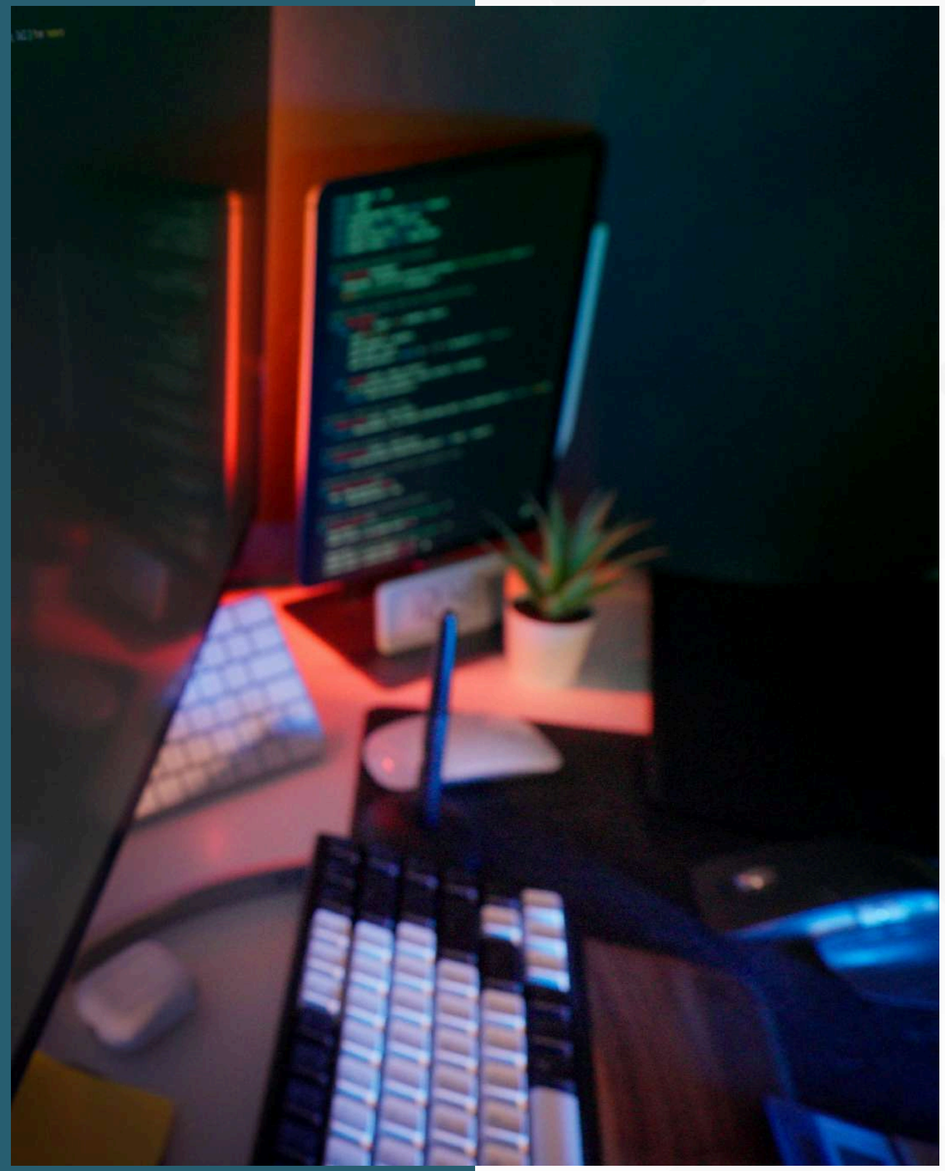
From understanding incidents to practicing escalation, containment, recovery and post-incident learning.

EXECUTIVE SUMMARY

What this module enables learners to do

- Recognise suspicious events and decide when escalation is required
- Apply a structured incident response lifecycle in VET environments
- Use triage, severity classification, playbooks and checklists
- Coordinate technical, managerial and communication actions
- Translate incidents into organisational learning and better cyber hygiene





INTRODUCTION

Why incident response matters in VET

- VET labs often imitate real workplaces and may contain real data
- Students, teachers and administrators all influence the attack surface
- The first minutes decide whether a problem stays local or becomes institutional
- Formal reporting prevents the “I fixed it quietly” trap
- The module builds practical response muscle memory

OVERVIEW

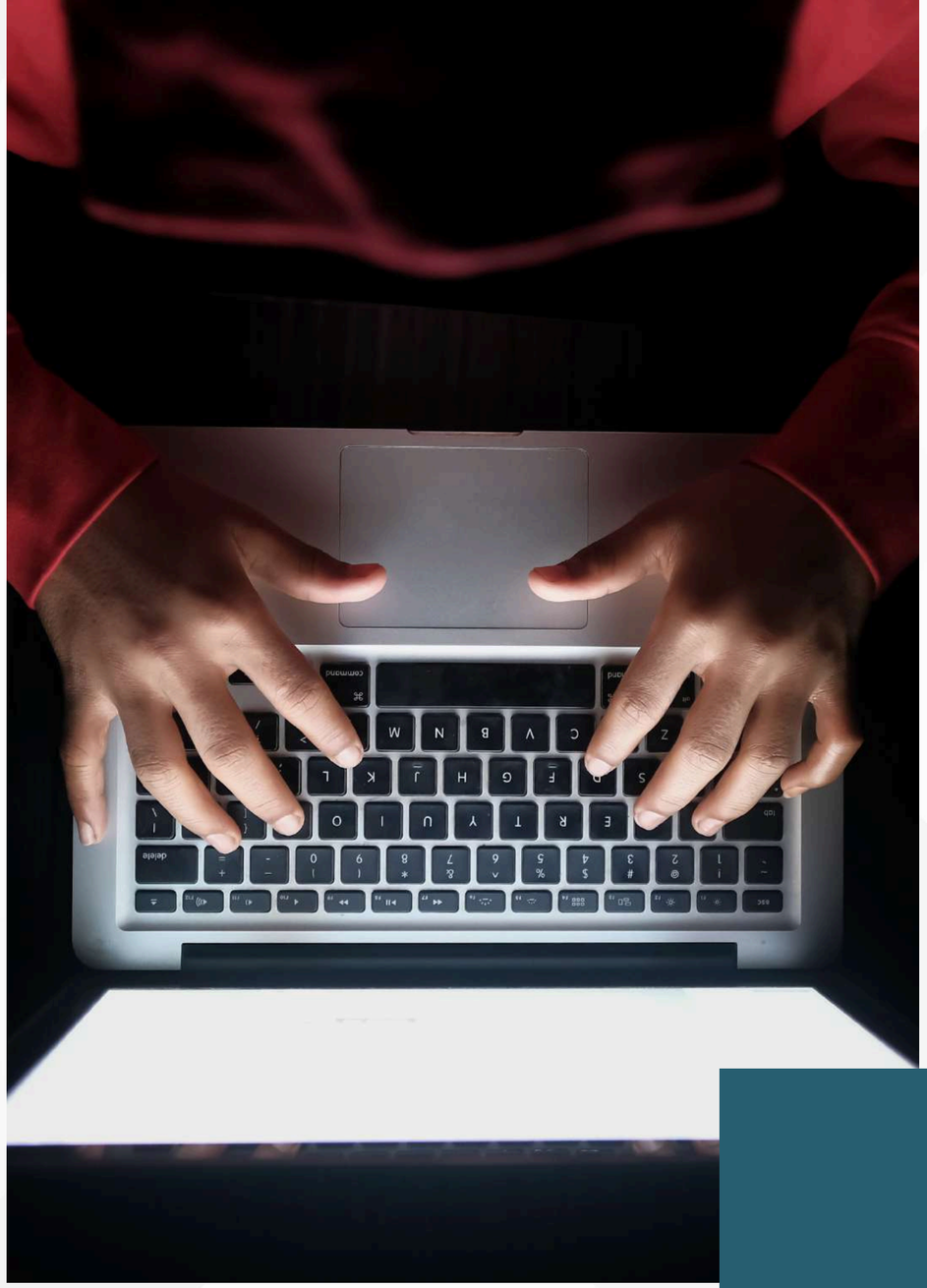
The incident response lifecycle

- NIST: preparation, detection and analysis, containment, eradication, recovery, post-incident activity
- SANS PICERL: preparation, identification, containment, eradication, recovery, lessons learned
- Modern NIST SP 800-61r3 links incidents with cyber risk management
- CSF 2.0 functions: Govern, Identify, Protect, Detect, Respond, Recover
- Response and recovery must be prepared before the crisis

IMPORTANCE OF THE TOPIC

Incidents are inevitable; chaos is optional

- A small phishing message can become credential theft, data leakage or ransomware
- Educational institutions face concentration risk through LMS, cloud and vendors
- Delayed detection increases legal, financial and reputational damage
- Good response protects learning continuity and trust
- Preparedness is cheaper than improvisation under pressure



LEARNING OBJECTIVES

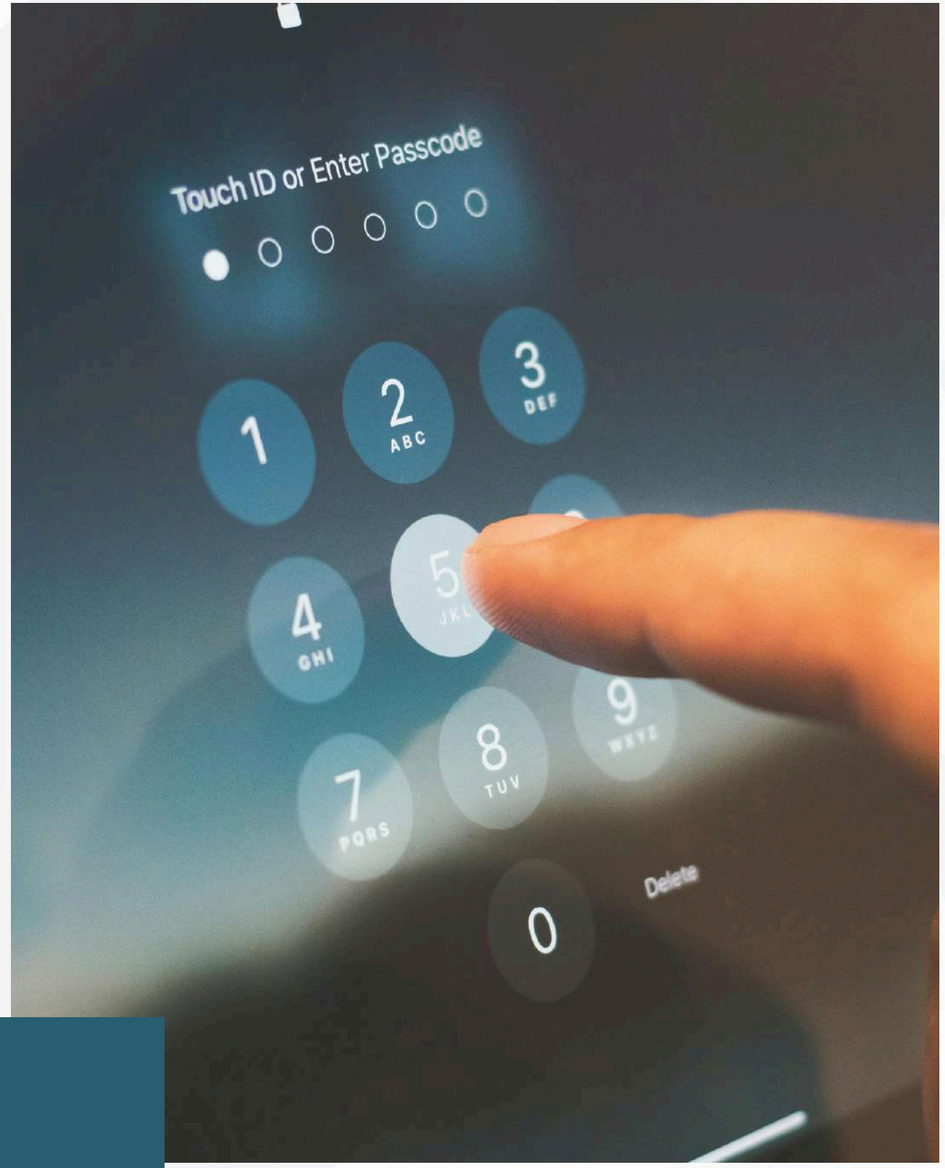
By the end of the module learners can...

- Distinguish event, alert, security incident and data breach
- Identify basic IoCs and collect useful initial evidence
- Classify severity using impact, urgency and confidence
- Use a playbook for phishing, ransomware or lost device incidents
- Support communication, recovery and post-incident review

KEY CONCEPTS AND DEFINITIONS

Shared vocabulary prevents operational confusion

- **IoC:** technical trace such as malicious IP, hash, domain or file path
- **Triage:** first prioritisation and routing of an alert or incident
- **Playbook:** repeatable response guide for a specific scenario
- **Event:** observable change in system or network behaviour
- **Alert:** signal generated by monitoring, user report or tool
- **Incident:** confirmed or suspected violation of security policy



CONTEXT AND BACKGROUND

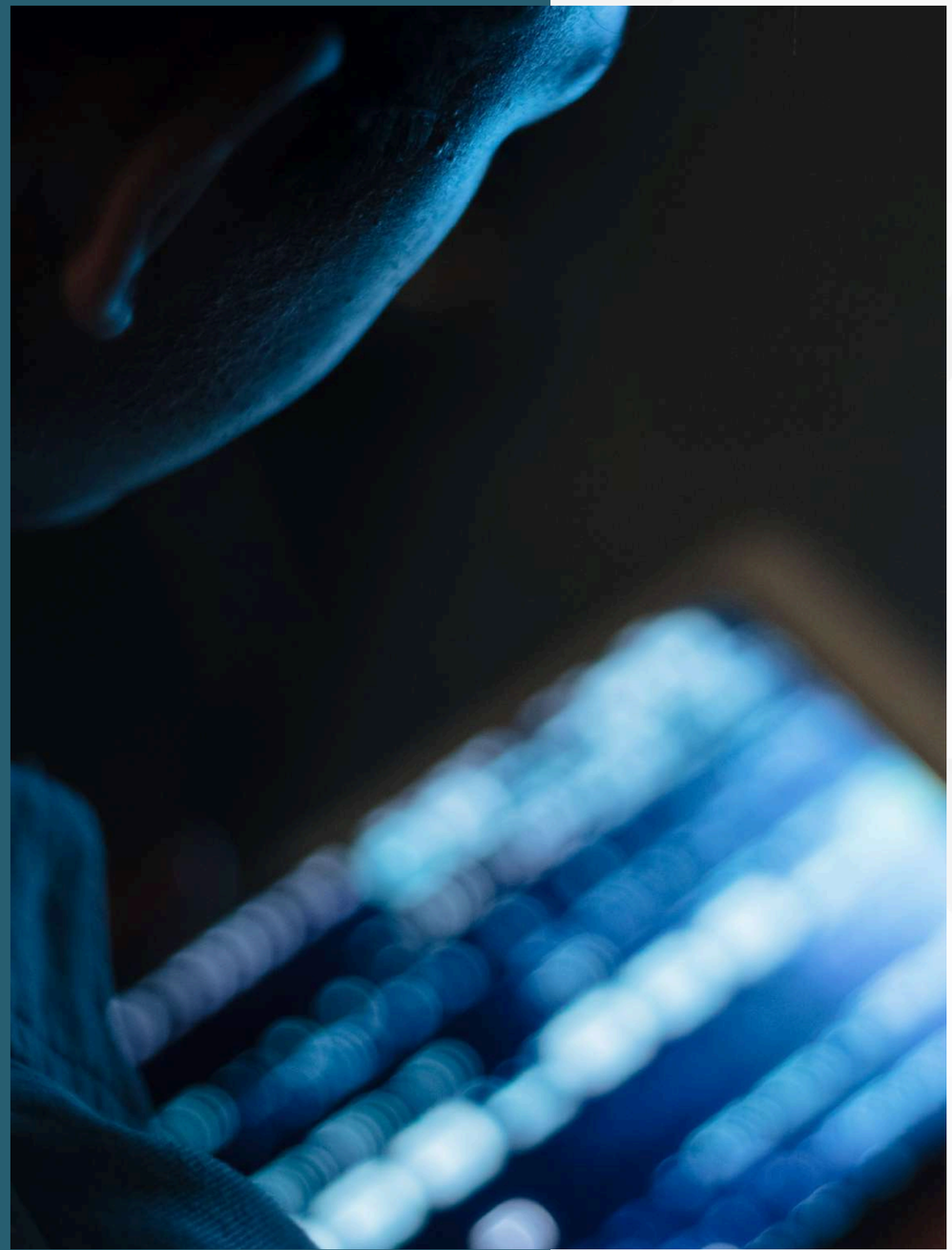
VET-specific risk landscape

- LMS platforms, e-mail, student records and lab devices are critical assets
- Simulated industrial networks may be connected to real infrastructure
- Shared computers and removable media increase exposure
- Informal reporting can be fast, but weakens documentation
- Third-party tools extend both capability and risk

MAIN THEMES

The backbone of the module

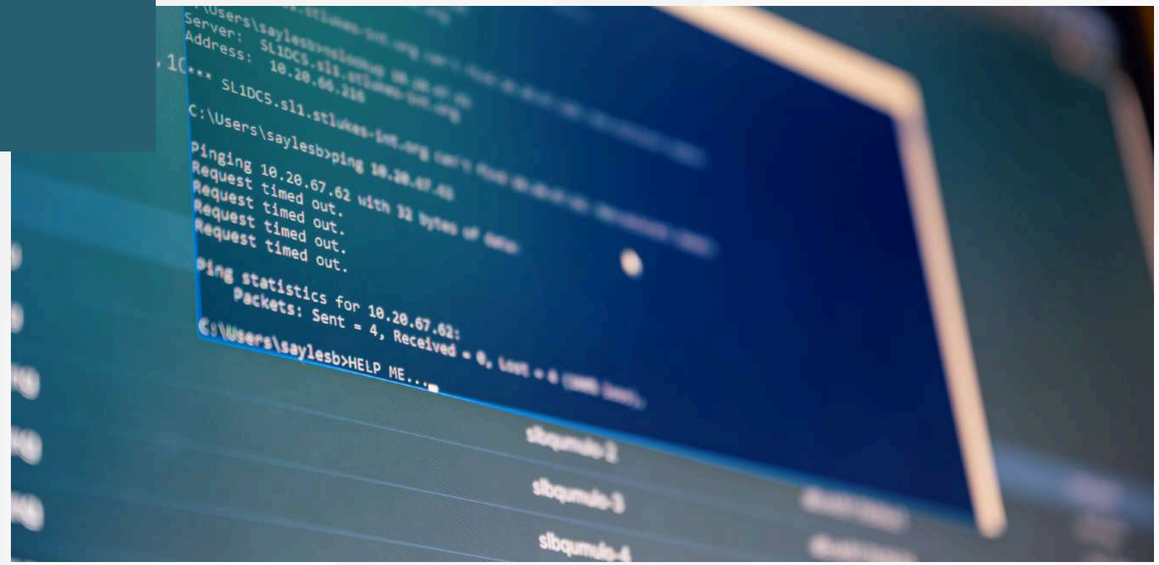
- Readiness: roles, contact lists, logging, backups and exercises
- Detection: signals, IoCs, reports, anomaly recognition
- Decision-making: severity, escalation and containment trade-offs
- Continuity: recovery priorities and safe restoration
- Learning: post-incident review, updated controls and training

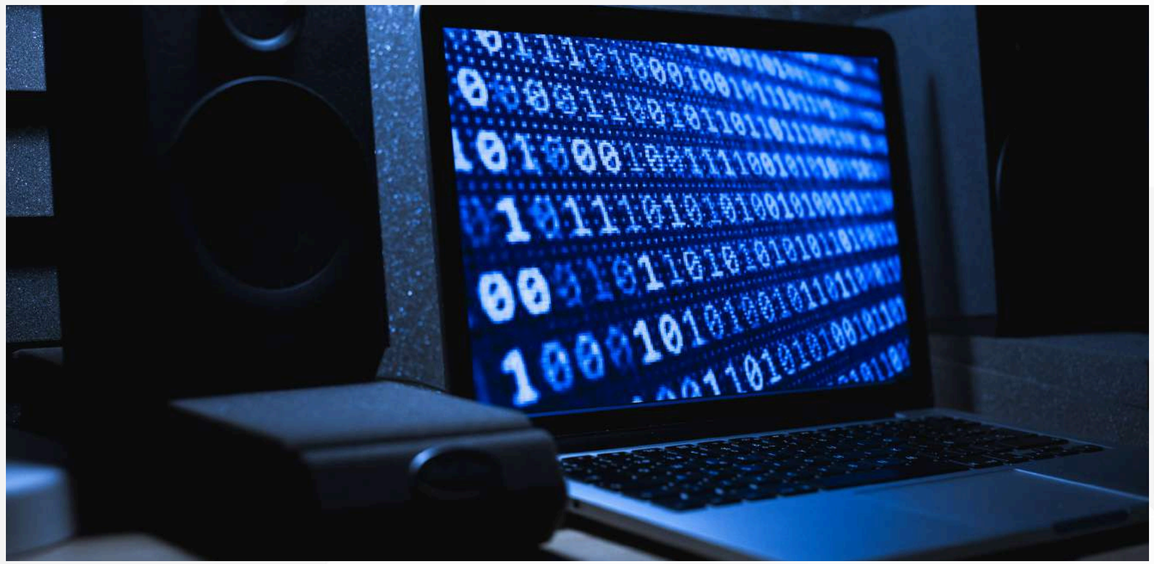


CORE PRINCIPLES

Rules that survive the pressure of an incident

- Do not destroy evidence while trying to fix the problem
- Contain first, understand progressively, recover safely
- Use least privilege and verified identities during response
- Communicate early, accurately and without speculation
- Document decisions, timestamps, systems and responsible persons
- Update the playbook after every serious exercise or incident

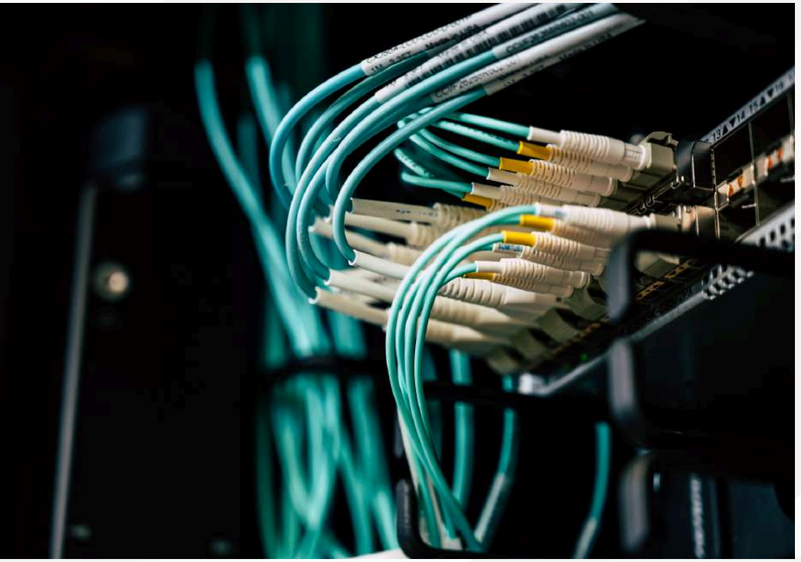


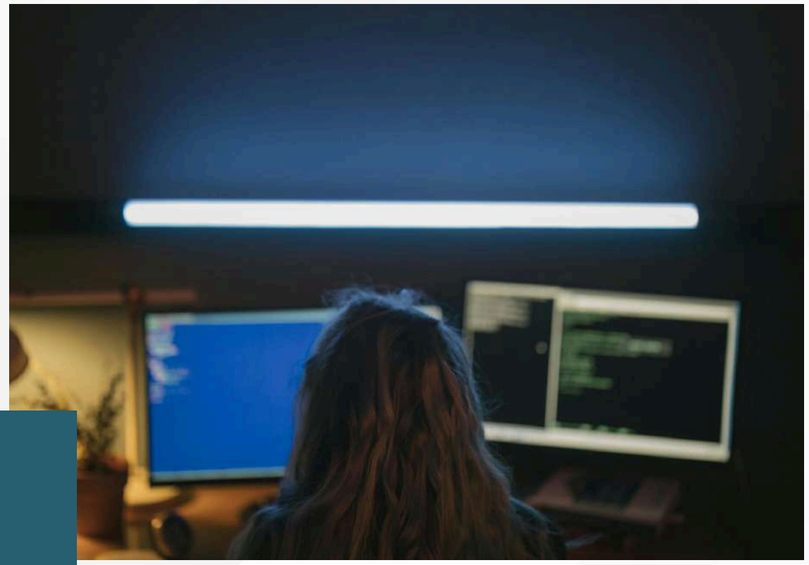


PHASE 1: PREPARATION

Build readiness before the alarm sounds

- Define CSIRT/CIRT roles: leader, technical lead, communications, legal/DPO, management
- Maintain asset inventory and critical service priorities
- Prepare out-of-band contact channels and emergency access rules
- Create playbooks for phishing, ransomware, lost device and cloud misconfiguration
- Test backups and practice tabletop exercises at least once per semester





CSIRT / CIRT TEAM MODEL

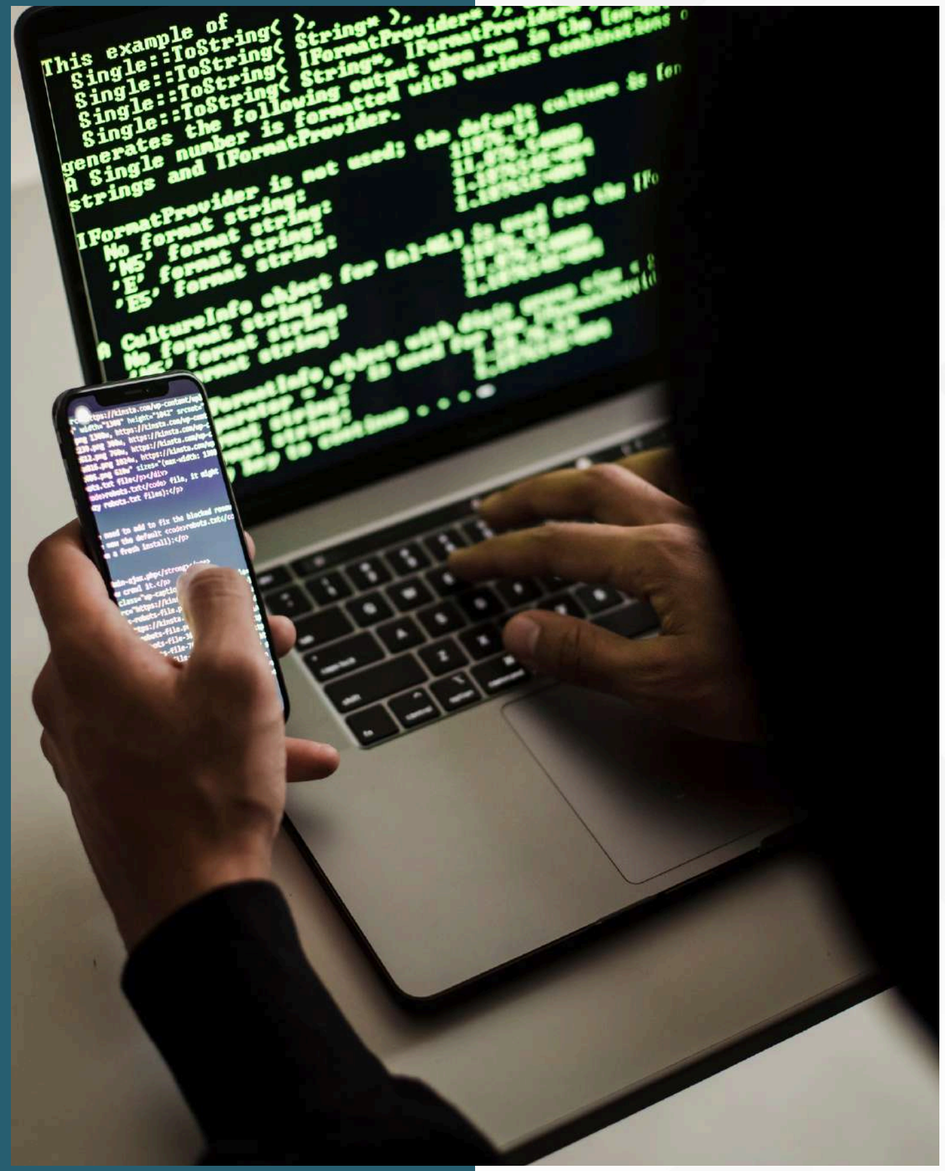
Incident response is a coordinated team sport

- **Incident commander:** keeps decisions and timeline under control
- **Technical handlers:** analyse logs, isolate systems, preserve evidence
- **Institutional leadership:** approves disruption and external communication
- **DPO/legal:** evaluates personal data and regulatory obligations
- **Teachers/admin staff/students:** report early and avoid “silent repair”
- **Vendor/MSSP:** supports systems outside institutional control

PHASE 2: DETECTION AND ANALYSIS

From weak signals to validated incident

- Collect alerts from users, SIEM/EDR, LMS logs, e-mail gateways and helpdesk
- Look for IoCs: suspicious logins, unusual IPs, hashes, domains, processes and file changes
- Determine scope: affected accounts, devices, data, services and time window
- Validate whether the attacker is still active
- Preserve evidence: logs, e-mail headers, screenshots and ticket identifiers



TRIAGE AND SEVERITY CLASSIFICATION

Prioritise without panic

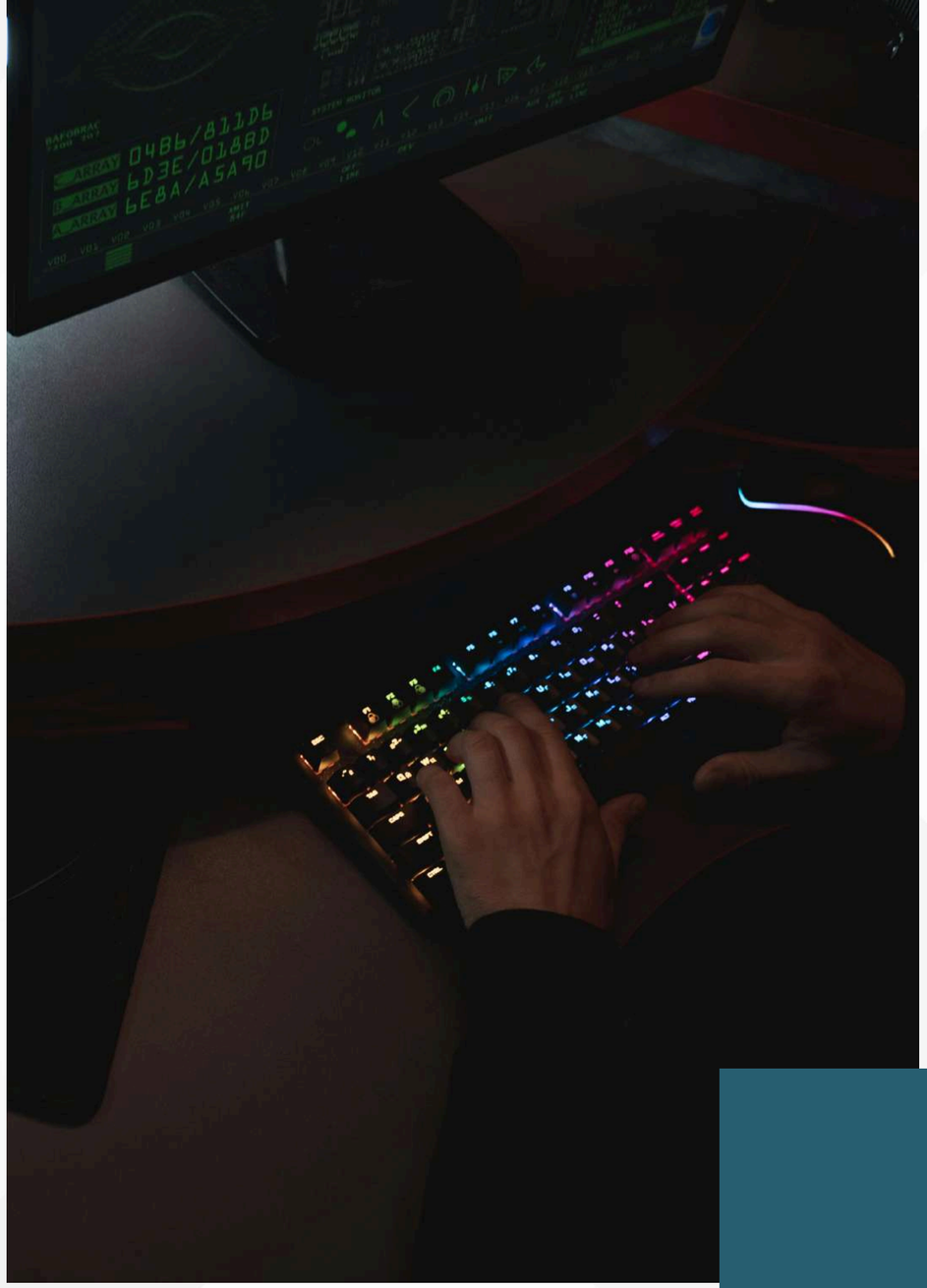
- Functional impact: which learning or administrative services are affected?
- Information impact: personal data, credentials, exam material or financial records?
- Recoverability: how hard is restoration and how reliable are backups?
- Confidence: confirmed incident, likely incident or weak signal?
- Escalate immediately when critical data, privileged accounts or ransomware are involved

Low **Medium** **High** **Critical**

PHASE 3: CONTAINMENT

Stop the bleeding while keeping evidence usable

- Short-term: isolate workstation, disable account, block domain or IP, revoke sessions
- Long-term: segment network, create clean parallel service, apply firewall rules
- Avoid mass deletion before evidence is captured
- Decide acceptable disruption: learning continuity versus risk of spread
- Coordinate with vendor if the affected service is outsourced



PHASE 4: ERADICATION

Remove the root cause, not only the symptom

- Identify initial access vector: phishing, leaked credentials, vulnerable service or misconfiguration
- Remove malware, backdoors, rogue accounts and malicious forwarding rules
- Patch exploited vulnerabilities and harden exposed services
- Reset credentials and review privileged access
- Confirm that IoCs no longer appear in logs and endpoints

PHASE 5: RECOVERY

Return to service safely and visibly

- Restore from clean, validated backups only
- Prioritise services: identity, communication, LMS, student records, finance, labs
- Monitor for re-entry, persistence or abnormal traffic
- Communicate restoration steps and known limitations
- Document residual risk and temporary controls

PHASE 6: LESSONS LEARNED

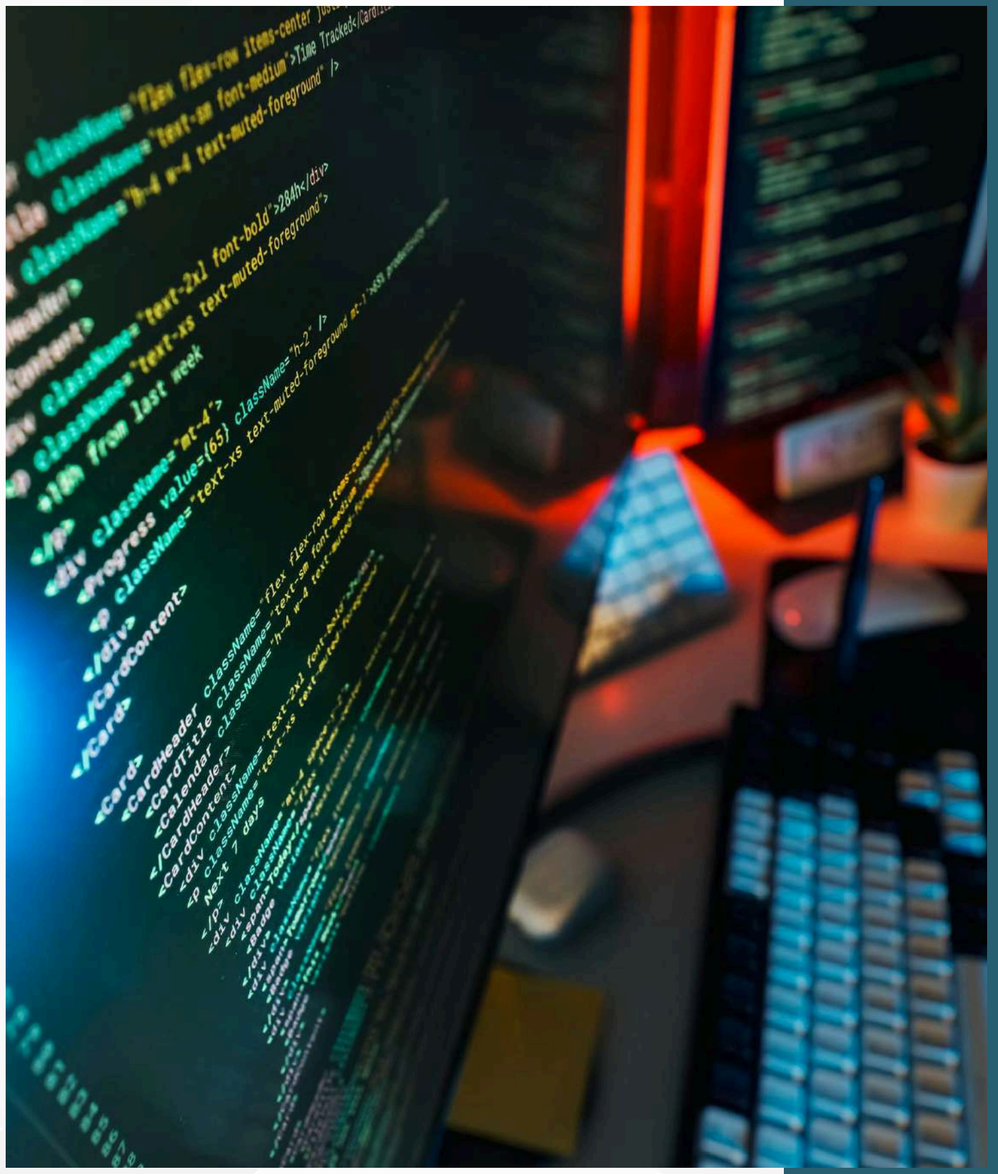
Close the loop before memory fades

- Hold post-incident review while facts are still fresh
- Reconstruct the timeline: detection, decisions, containment and recovery
- Identify gaps in tools, roles, training and communication
- Convert lessons into owners, deadlines and measurable improvements
- Share anonymised learning cases with students and staff

CHALLENGES AND RISKS

What usually breaks under pressure

- Unclear decision rights: nobody knows who can shut down a service
- Over-reliance on informal phone calls and undocumented fixes
- Poor visibility: missing logs, unsynchronised clocks or no endpoint telemetry
- Vendor opacity during cloud or LMS incidents
- Communication vacuum filled by rumours
- Backups that exist in theory but fail in restoration



OPPORTUNITIES AND BENEFITS

What good incident response creates

- Shorter downtime and less damage from attacks
- Better protection of learners, staff and partner data
- Stronger trust with employers, parents, regulators and funders
- Improved cyber hygiene across the whole institution
- Reusable learning scenarios for VET cybersecurity education
- Evidence-based investment decisions after incidents

PRACTICAL APPLICATIONS

Where learners apply the method

- **Student lab:** suspicious traffic from a simulated PLC network
- **LMS:** teacher account sends unexpected links to a class group
- **Administration:** lost laptop containing practice placement files
- **Cloud drive:** folder with assessment sheets accidentally shared publicly
- **E-mail:** finance office receives invoice redirection request
- **Workshop:** shared workstation displays ransomware note

TOOLS AND METHODS

From simple checklists to advanced platforms

- **Reporting form:** who, what, when, where, evidence attached
- **SIEM/EDR:** correlation, endpoint visibility and alert enrichment
- **Threat intelligence:** known malicious domains, IPs, hashes and TTPs
- **SOAR/playbooks:** structured automation for repetitive actions
- **Forensic readiness:** log retention, evidence chain and secure storage
- **Communication templates:** internal notice, management brief, user advisory

PLAYBOOK: PHISHING IN A VET INSTITUTION

A minimum viable response checklist

- Capture message, headers, URLs and recipient list
- Disable or reset compromised account; revoke sessions and MFA tokens if needed
- Block malicious domains, hashes and sender infrastructure
- Search for similar messages across mailboxes
- Warn affected users with clear instructions
- Review whether data or credentials were exposed

COMMUNICATION STRATEGY

Say enough, say it early, say it accurately

- Separate audiences: students, staff, leadership, partners, vendors and regulators
- Use plain language: what happened, what to do now, where to ask questions
- Avoid speculation, blame and unsupported technical claims
- Coordinate technical and legal messages before release
- Maintain a single source of truth and update it regularly

CASE EXAMPLE 1: LMS / CANVAS-TYPE BREACH

Third-party concentration risk

- Scenario: provider compromise affects many institutions at once
- Risk: stolen messages, credentials, student data or defaced login pages
- Immediate actions: vendor contact, SSO review, forced password reset where justified
- Containment: monitor abnormal logins and disable risky integrations
- Communication: explain uncertainty and give practical user steps
- Learning: map dependency on critical education platforms

CASE EXAMPLE 2: UNIVERSITY DATA BREACH

Credential misuse and delayed detection

- Scenario: legitimate account used to access large volumes of institutional data
- Risk: personal identifiers, health data, payroll or candidate records exposed
- Detection gap: activity looked normal until volume and pattern were analysed
- Response: account disablement, log analysis, data scoping, legal escalation
- Learning: privileged monitoring and anomaly detection are essential

CASE EXAMPLE 3: THIRD-PARTY VENDOR RISK

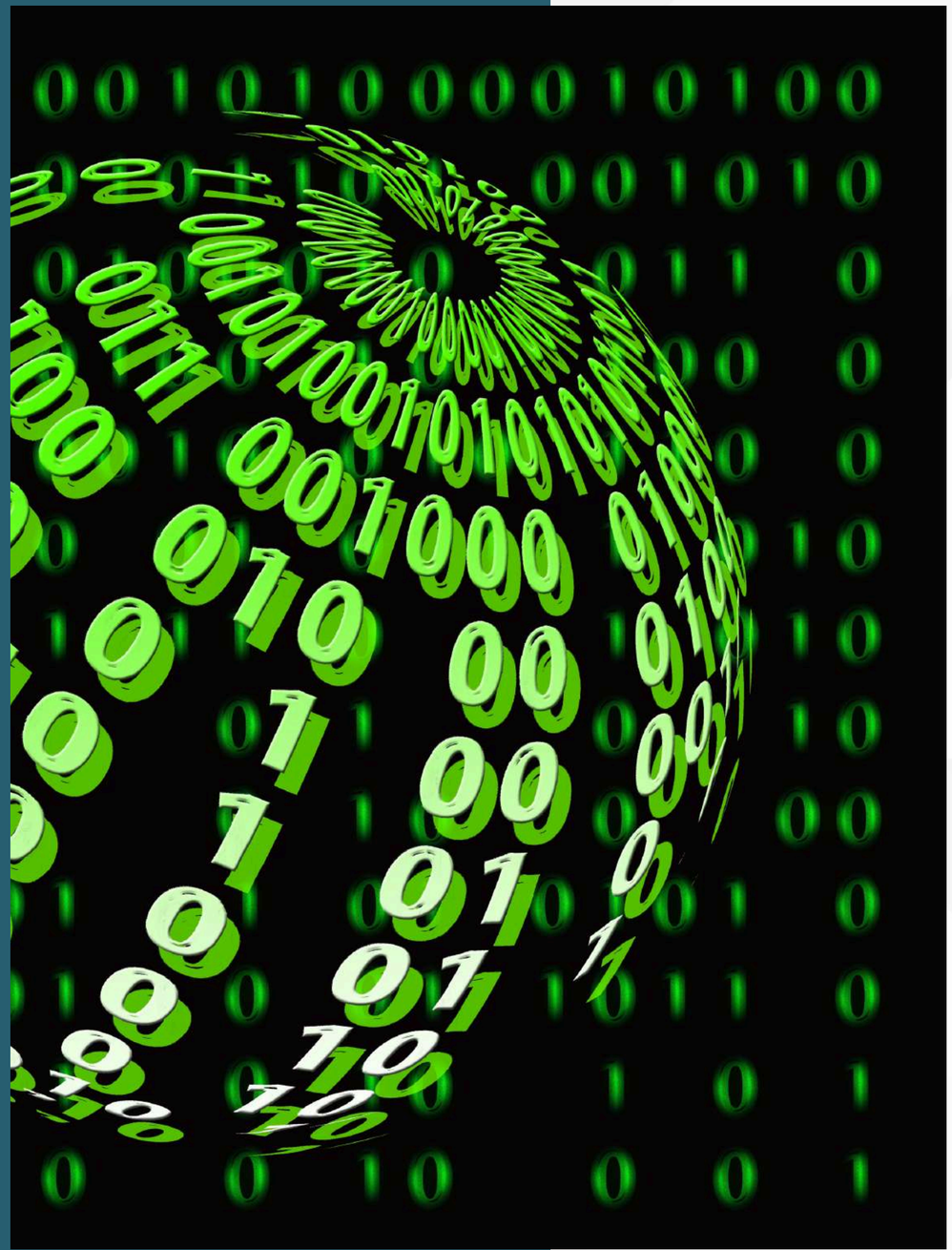
When the incident starts outside your walls

- Scenario: cloud attendance tool or practice-placement platform is breached
- Institution remains responsible for decisions affecting its community
- Check contract: notification time, evidence access and support obligations
- Prepare contingency: alternative attendance or assessment workflow
- Record decisions and keep users informed without overpromising

INTERACTIVE ACTIVITY: TABLETOP EXERCISE

“The practice coordinator account is compromised”

- Group roles: teacher, IT handler, DPO/legal, director, communications, vendor
- Round 1: decide actions in the first 15 minutes
- Round 2: decide actions in the first 4 hours
- Round 3: prepare a short message for students and staff
- Debrief: what was missing from the playbook?



REFLECTION POINTS

Questions for individual or group discussion

- Which system in your institution would cause the most disruption if unavailable?
- Who can approve isolation of an LMS, identity system or lab network?
- What evidence would you preserve before cleaning an infected device?
- How would you communicate when facts are incomplete?
- Which one cyber hygiene habit would reduce the most risk this week?

KEY TAKEAWAYS

The module in six sentences

- Incident response is part of risk management, not a side task for IT
- Preparation determines the quality of every later phase
- Triage converts noise into priorities
- Containment must balance speed, evidence and continuity
- Recovery is safe only when backups and integrity are tested
- Lessons learned turn pain into resilience

SUMMARY

What has been covered

- DEFENDERS structure and VET learning context
- NIST and SANS lifecycle models
- CSIRT/CIRT roles and escalation logic
- IoCs, triage and severity classification
- Containment, eradication, recovery and post-incident review
- Playbooks, checklists, communication and case-based learning

ASSESSMENT / REVIEW

Short knowledge check

1. Name the six SANS PICERL phases.
2. Give three examples of IoCs in a school or VET network.
3. What information belongs in the first incident report?
4. When should a compromised account be disabled?
5. Why can restoring from backup still be risky?
6. What should be updated after the post-incident review?

CONCLUSION

From awareness to disciplined action

- A resilient institution does not wait for perfect information
- Every learner and staff member can be a reliable early-warning sensor
- Playbooks reduce improvisation and support accountability
- Good cyber hygiene lowers both probability and impact
- The best incident response lesson is the one embedded before the next incident

DEFENDERS

Defending VET Students within Cybersecurity Innovation

MODULE 5: INCIDENT RESPONSE AND MANAGEMENT

Project No: 2025-1-PL01-KA210-VET-000363642

www.defenders-project.eu

FUNDACJA ROZWOJU SPOŁECZNEGO CIVITAS

M.S.A. ΚΕΝΤΡΟ ΔΙΑ ΒΙΟΥ ΜΑΘΗΣΗΣ

NIKOLA KAREV State High School & VET Centre Strumica

Co-funded by the European Union

Funded by the EU. The views and opinions expressed are solely those of the author(s) and do not necessarily reflect the views and opinions of the European Union or the Foundation for the Development of the Education System. Neither the European Union nor the Foundation for the Development of the Education System are responsible.