

Incident Response & Breach Management

Dr Diarmuid Ó Briain

23 Nov 2026

DEPARTMENT OF ELECTRONIC ENGINEERING & COMMUNICATIONS
SOUTH EAST TECHNOLOGICAL UNIVERSITY

setu.ie
INSPIRING FUTURES

Version: 1.0

Licence

This work is licenced under a Creative Commons Attribution-ShareAlike 4.0 International Licence.
Full Licence: http://creativecommons.org/licenses/by-sa/4.0

Learning objectives

- At the end of this topic you will be able to:
  - Evaluate complementary IDS/IPS and SIEM detection infrastructure.
  - Formulate incident response frameworks and establish an operational CSIRT and war room.
  - Execute incident triage, implement containment strategies, and preserve digital evidence forensically.
  - Manage secure environment restoration, post-incident notifications, legal obligations, and continuous improvement reviews.

Detection Infrastructure

Monitoring - Intrusion Detection System (IDS)

- Sensors which generate security events
- Console to monitor events and alerts and control the sensors
- Central Engine that records events logged by the sensors in a database and uses a system of rules to generate alerts from security events received.

- **Host**-based IDS (HIDS)
- **Network**-based IDS (NIDS).

- Detection types
  - **Knowledge** (**Signature**) Based Detection
  - **Behaviour** (**Statistical anomaly**) Based Detection.

Intrusion Prevention System (IPS)

- A network security tool that continuously monitors incoming and outgoing traffic for malicious activity and automatically takes action to stop it in real time.
- Placed directly inline, typically right behind a firewall, it inspects data packets at wire speed, comparing them against databases of known threat signatures, protocol anomalies, and behavioural rules.
- When an IPS detects an exploit it immediately intervenes without human involvement by dropping the malicious packets, resetting the connection, or blocking traffic.

Security Information and Event Management (SIEM)

- Security solution that helps organisations detect, analyse, and respond to potential security threats and vulnerabilities before they have a chance to disrupt business operations
- SIEM systems collect and analyse data from a variety of sources, including security logs, system logs, and network traffic, to identify patterns and anomalies that may indicate a security incident.



SEIM Systems

- **Improve security visibility**
  - Collect data from a variety of sources, which gives security teams a more comprehensive view of their IT environment and the security threats that it faces
- **Detect security threats**
  - Used to detect a wide range of security threats, including malware, intrusions, and insider threats
- **Respond to security incidents**
  - Help security teams to respond to security incidents more quickly and effectively.

SEIM System benefits

- Improve security visibility
- Reduced risk of data breaches
- Improved compliance

SEIM System benefits

Feature	SIEM	IDS/IPS
Purpose	Collect and analyse security data from a variety of sources to identify threats and security incidents	Detect and actively prevent/block suspicious activity on a network or system
Use cases	Monitoring OT networks and systems for security threats and incidents	Detecting and responding to/blocking network intrusions in real time
Deployment	Typically deployed on a centralised server	Typically deployed inline (for IPS) or out-of-band (for IDS) on individual devices or network segments
Data sources	Event logs, network traffic, security alerts, etc.	Live network traffic (and host system logs for HIDS/HIPS)
Capabilities	Can identify threats and incidents by correlating data from multiple sources, generate alerts, and provide insights into security risks	Can detect suspicious activity (unusual traffic patterns or known attack signatures) and automatically drop malicious packets or block offending IPs

IDS/IPS and SIEM

- **Complimentary systems**
  - IDS/IPS system detects a suspicious IP address trying to access a critical server
  - IDS/IPS system generates an alert and blocks the traffic
  - Alert is sent to the SIEM system
  - SIEM correlates the alert with firewall logs and server logs
  - SIEM identifies a potential security incident and alerts to the security team
  - Security team investigates the alert and determines a malicious attack
  - Security team takes action to mitigate the attack.

Exercise

Ollscoil Teicneolaíochta an Oirdheiscirt
South East Technological University



Responding to a breach



Ollscoil Teicneolaíochta an Oirdheiscirt
South East Technological University

Hologram Keys Limited

Exercise Part 1

Scenario Develops

Hologram Keys Limited

- Design and produce wireless keys and access cards for various types of high-end vehicles including electric cars, helicopters, and private aircraft
- Use a co-located Cloud Service Management to house and maintain many systems as well as store data, including their intellectual property and customer information, which is highly sensitive based on the net worth of their average customer
- HK Ltd. design IP is unparalleled, they are industry leader and access to their IP could open vulnerabilities such as spoofed access keys to the transportation of the world's elite



The graveyard shift at Hologram Keys Limited

The Graveyard shift at Hologram Keys Limited

- **Hologram** has been a target for black hat hackers that sell stolen data on the dark web.
- Tonight there is minimal staff on the graveyard shift and monitoring is largely automated.
- The analysts are reviewing logs, creating backups, and performing other routine tasks.
- Mary, an analyst, notices an alert. She thinks to herself, '***This does not look right***.' She quickly checks some logs and verifies the result. It could be harmless, but it definitely needs to be checked out. It could be the tip of a very dangerous iceberg.

The phone rings



The phone rings from Hologram Keys Limited

- At home your phone rings and you sit up listening to Mary, the analyst from the SOC, on the other end of the line.
- After a few security questions to verify identity she says: "***Sorry to bother you in the middle of the night, but we've had what appears to be a major incursion, there are some logs coming from the SIEM, that shows a user that has moved laterally across systems in an abnormal way. We can not seem to see a clear path of the user's movement. There is an issue with the logs, almost like someone tried to scrub them, but we've connected the dots on at least two networks and it doesn't look good. We will need help to get to the bottom of this. What should we do? !!***"

Definitions

- **A security event**: is a record of an action taken against an information system that alters the system's state. An organisation can have millions of events that occur throughout a date.
- **A security incident**: is an event or series of correlated events that indicate that a potential violation of some control or policy has occurred. This is a smaller subset of security events.
- **A security breach**: is defined as unauthorised access that violates the confidentiality, integrity, or availability of an information asset in the form of unintentional access, destruction, or manipulation of an information asset.

Attack vector sources

- 76% breaches were financially motivated
- 73% of all cyber attacks were carried out by outsiders
- 28% of all cyber attacks were carried out by insiders

Detection and Analysis

68% of breaches took several months or longer before they were discovered

- The NIST Framework breaking it down into two groups;
  - **Precursors**:
    - Signify that an incident may occur in the future for example, when you receive alerts that several web servers are being scanned by a vulnerability scanner.
  - **Indicators**:
    - Provides evidence of a current or previous incident.
    - A typical example is when an antivirus solution triggers alerts when a host has been infected with malware.

Question 1

- **What is a security breach defined as?**

☐ Record of an action taken against an information system that alters the system's state. An organisation can have millions of events that can occur throughout a day

☐ Event or series of correlated events that indicate that a potential violation of some control or policy has occurred. Security This is a smaller subset of security events

☐ Unauthorised access that violates the confidentiality, integrity, or availability of an information asset in the form of unintentional access, destruction, or manipulation of an information asset

☐ None of the above



Question 1

- **What is a security breach defined as?**

☒ Record of an action taken against an information system that alters the system's state. An organisation can have millions of events that can occur throughout a day

☒ Event or series of correlated events that indicate that a potential violation of some control or policy has occurred. Security This is a smaller subset of security events

☑ Unauthorised access that violates the confidentiality, integrity, or availability of an information asset in the form of unintentional access, destruction, or manipulation of an information asset

☒ None of the above

Question 2

- **SIEM tools can be used for**

☐ Network Performance and Monitoring

☐ Network Traffic Analysis

☐ Network Troubleshooting

☐ None of the above



Question 2

- **SIEM tools can be used for**
  - ☑ Network Performance and Monitoring
  - ☑ Network Traffic Analysis
  - ☑ Network Troubleshooting
  - ☒ None of the above

SIEM tools are for centralised security monitoring, threat detection and incident response

Breach Response Plan

- The Breach Response Plan, Consider a model based on;
  - NIST Special Publication 800-61 Information Response Guide
  - ISO 27002 standard of good practice for Information Security
  - ITIL service operation, Incident Management (IM) practice for restoring services as quickly as possible after an incident
  - COBIT, Control Objectives for Information and Related Technologies

Question 3

- **The company could have chosen any of these to guide their risk management planning**
  - ☐ NIST SP 800-30
  - ☐ ISO 27003
  - ☐ ISO 31000
  - ☐ COSO ERM
  - ☐ ISO 45001
  - ☐ None of the above



Question 3

- **The company could have chosen any of these to guide their risk management planning**
  - ☑ NIST SP 800-30 - Guide for Conducting Risk Assessments
  - ☒ ISO 27003 - Guidelines that helps implement ISO 27001
  - ☑ ISO 31000 – Risk Management Guidelines
  - ☑ COSO ERM – Enterprise Risk Management
  - ☒ ISO 45001 - Occupational Health and Safety Management Systems
  - ☒ None of the above



Ollscoil Teicneolaíochta an Oirdheiscirt
South East Technological University

Hologram Keys Limited

Exercise Part 2

Calling in the CSIRT

You respond



You respond

- *"**Let's call in the team**."*
- You think:
  - How big is this?
  - What all did they get access to?
  - Could this just be a mistake?
  - There's a CSIRP, in place.

You respond

- *"Mary contact everyone in the Incident Response team. Everyone local should report to HQ physically.*
- *Has there been a sweep of the SOC for unauthorised physical presence?*
- *Any keylogging devices or errant USB drives plugged in? We need a complete report of that in the next hour.*
- *We also need the War Room set up ASAP. Please help us get the second floor conference room reserved and get the secure video and audio conference set up. Make sure it is encrypted. If someone is on the network, we can't have them listening in."*

Your Response

- Actions:
  - Call in the CSIRT.
  - Follow the CSIRP.
  - Sweep the SOC for unauthorised physical presence.
  - Establish the War Room.
  - Make sure it is encrypted to prevent eavesdropping.

Question 4

- **You are a security analyst working for a large organisation. You receive an alert from your Intrusion Detection System (IDS) that indicates that there may be a breach in progress. What is the FIRST thing you should do?**

☐ Contact your manager and let them know about the alert

☐ Immediately call in the CSIRT

☐ Investigate the alert further to determine if there is a real breach

☐ Do nothing, as the IDS may be generating false positives



2

Question 4

- **You are a security analyst working for a large organisation. You receive an alert from your Intrusion Detection System (IDS) that indicates that there may be a breach in progress. What is the FIRST thing you should do?**

☒ Contact your manager and let them know about the alert

☒ Immediately call in the CSIRT

☑ Investigate the alert further to determine if there is a real breach

☒ Do nothing, as the IDS may be generating false positives

Question 5

- **A precursor is the notion that there is evidence of a current or previous incident, such as an antivirus solution triggering alerts when a host has been infected with malware**

☐ True

☐ False



2

Question 5

- **A precursor is the notion that there is evidence of a current or previous incident, such as an antivirus solution triggering alerts when a host has been infected with malware**

☒ True

☑ False

A precursor identifies that an incident may occur in the future

Question 6

- **The CSIRT consists of the following**

☐ Process/Control Engineer

☐ Network Administrator

☐ System Administrator

☐ Plant Manager

☐ 3rd Party Vendor Support

☐ Chief Information Systems Officer

☐ Team Leader/Manager

☐ Lawyer

☐ Public Relations Manager

☐ Human Resources Manager

☐ Security Specialist



2

Question 6

- **The CSIRT consists of the following**

☑ Process/Control Engineer

☑ Network Administrator

☑ System Administrator

☒ Plant Manager

☑ 3rd Party Vendor Support

☒ Chief Information Systems Officer

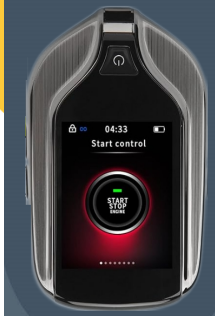
☑ Team Leader/Manager

☑ Lawyer

☑ Public Relations Manager

☑ Human Resources Manager

☑ Security Specialist



SETU Ollscoil Teicneolaíochta an Oirdheiscirt South East Technological University

Hologram Keys Limited

Exercise Part 3

The gathering of the CSIRT

CSIRT team gathers at HQ



CSIRT team gathers at HQ

- Arriving in the office you make a phone call. "***Is everyone on the way? Are you using the mobile numbers in the CSIRP?***"
- The team begins to arrive at HQ within the hour and the office is ablaze with swift footsteps and intense conversation.
- You ask Mary if there is any information on the scope so far, but there is no news, and you know it is going to take teamwork to assess this situation, let alone contain and remediate.

Detection and Analysis

- First Responders have gathered together under your direction as outlined in the CSIRP. You convene a video call and try to get a handle on who knows what so far. You're calm, but you know that time is critical, so you are speaking quickly and deliberately. You are looking for the incident lead from the SOC.
- "***Alright team, we need information, a lot of it, from a lot of places. We need to be sure we have the SOC lead on. You there? Good. After this call please head in so we can coordinate from the War Room. Also, where is that Continuous Security Monitoring (CSM) physical security report? Already sent? Great, let us review that together when you get here. We also need to get in touch with the Senior Security Engineer. Oh no, they're out of the country on vacation?***"

Incident Management Priorities

- Address life safety issues.
- Assess the incident.
- Notify and escalate.
- Triage.
- Contain the incident (Stop it from spreading).
- Analyse the nature and source of the incident.
- Track and document the incident.
- Restore to normal operations.

Question 7

- **Which of the following is NOT a factor that should be considered when evaluating and analysing a reported incident?**

- ☐ The potential impact of the incident on the organisation
- ☐ The specific type of incident
- ☐ The time zone in which the incident occurred
- ☐ Whether the incident has the potential to spread across other networks
- ☐ None of the above



Question 7

- **Which of the following is NOT a factor that should be considered when evaluating and analysing a reported incident?**

- ☒ The potential impact of the incident on the organisation
- ☒ The specific type of incident
- ☑ The time zone in which the incident occurred
- ☒ Whether the incident has the potential to spread across other networks
- ☒ None of the above

Question 8

- **When evaluating and analysing a reported incident, the most important item to determine:**

- ☐ Whether the reported incident is real or a false positive
- ☐ What systems and equipment are or may be affected by the incident
- ☐ What organisations will be affected and who should be part of the response
- ☐ The specific type of incident
- ☐ The time zone in which the incident occurred
- ☐ The time of day when the incident occurred



Question 8

- **When evaluating and analysing a reported incident, the most important item to determine:**

- ☑ Whether the reported incident is real or a false positive
- ☒ What systems and equipment are or may be affected by the incident
- ☒ What organisations will be affected and who should be part of the response
- ☒ The specific type of incident
- ☒ The time zone in which the incident occurred
- ☒ The time of day when the incident occurred



Hologram Keys Limited

Exercise Part 4

Getting to grips with the incident



War Room

- It looks like several different accounts had similar behavioural patterns on the network.
  - Could there have been a coordinated attack?
  - Or might one bad actor have been trying to confuse the investigation by using multiple accounts?
- Again, logs have been tampered with along the way, and the path that these accounts took is not entirely clear.

War Room

- Call from the NOC on secure line. In the War Room, the SOC lead takes the call.
- He announces to the room, "***This has just escalated. The NOC has confirmed the attack vector, this is a confirmed breach. We do not yet know if the attackers are still active on the systems and we are going to have to start shutting down access and locking down the networks***."
- With every new piece of information, the severity level is moving up.
- You follow on. "***There are going to be some serious business impacts from these steps. We need to stay coordinated. I want to keep the secure line open, but I need to see that encryption status report right away***."

Question 9

- **The response actions for an incident should:**
  - ☐ Be directly associated with the incident type; one approach will not fit all situations, and new attack vectors should be considered on a regular basis
  - ☐ Be implemented immediately, regardless of the severity of the incident
  - ☐ Include a comprehensive response covering containment of the problem, restoration of operations to a functional state, and prevention of a recurrence
  - ☐ Be implemented without considering the potential impact on the organisation
  - ☐ Take into consideration any forensics requirements
  - ☐ None of the above


2

Question 9

- **The response actions for an incident should:**
  - ☑ Be directly associated with the incident type; one approach will not fit all situations, and new attack vectors should be considered on a regular basis
  - ☒ Be implemented immediately, regardless of the severity of the incident
  - ☑ Include a comprehensive response covering containment of the problem, restoration of operations to a functional state, and prevention of a recurrence
  - ☒ Be implemented without considering the potential impact on the organisation
  - ☑ Take into consideration any forensics requirements
  - ☒ None of the above



SETU Ollscoil Teicneolaíochta an Oirdheiscirt
South East Technological University

Hologram Keys Limited

Exercise Part 5

The PR director arrives to up the ante

War Room



War Room

- With the continued impact of this breach expanding, and with the risk level extremely high, you begin to direct the shut down of systems that might have been compromised.
- The stakes are raised and tensions increase. People are starting to get scared. The implications of ex-filtrated data could endanger lives. Things are moving quickly and hard decisions are being made. The selected shutdowns have stopped the automation-assisted production lines and processing systems in the factory.
- Ultimately, keys are not being made. Production has ground to a halt without notice to facilities, sales, or even management.

War Room

- The head of Public Relations, Tanya, comes in the war room. She is demanding answers. She says, "***I don't understand. We know we have had a breach, but we do not even know when it happened? How can that be? I need to get in front of this. We have regulated timelines to report out. I know you already know that, but we need to have a narrative that makes sense or the media will run with it. Can you help me get a solid answer on this list of questions?***"

Question 10

- **Which of the following is NOT a step in the investigative process?**

☐ Presentation

☐ Detection

☐ Identification

☐ Preservation

☐ Collection

☐ Analysis



2

Question 10

- **Which of the following is NOT a step in the investigative process?**

☒ Presentation

☑ Detection

☒ Identification

☒ Preservation

☒ Collection

☒ Analysis

Question 11

- **It is acceptable to perform forensic work on original copies of evidence**
  - ☐ True
  - ☐ False



Question 11

- **It is acceptable to perform forensic work on original copies of evidence**
  - ☒ True
  - ☑ False

Chain of Evidence!!!

Question 12

- **Which of the following are best practices for communicating with internal and external stakeholders during a breach response?**
  - ☐ Establish a clear and consistent message
  - ☐ Communicate promptly and transparently
  - ☐ Designate a single spokesperson for all communications
  - ☐ Use technical jargon that may not be understood by all stakeholders
  - ☐ Provide regular updates, even if there is no new information.



Question 12

- **Which of the following are best practices for communicating with internal and external stakeholders during a breach response?**
  - ☑ Establish a clear and consistent message
  - ☑ Communicate promptly and transparently
  - ☑ Designate a single spokesperson for all communications
  - ☒ Use technical jargon that may not be understood by all stakeholders
  - ☑ Provide regular updates, even if there is no new information.



Hologram Keys Limited

Exercise Part 6

The Plant Director raises the stakes even higher



War room

- The team is trying to divide and conquer, and some have started working on the answers to the PR-related questions.
- You do not think that is the best use of time, but you can't micromanage each step, so you keep your head down and continue managing the containment.

War room

- The Plant Manager, Richard, comes into the War Room. He says, "***What do you mean I won't be able to run the factory systems for the next four hours? That will cost an incredible amount of money. Are we supposed to just have 35 line workers stand around and wait? You have to be able to get those systems back up immediately***."
- You know there is no way to do that right now without opening yourselves up to continuous vulnerabilities, so you try to explain that to the Plant Manager. He does not like what he is hearing, and is pushing you for alternatives.
- Blame is being traded. One team member accuses another, "***What do you mean you reran the logs from the SIEM? I just queued that job too. We can't be wasting time doing the same work. You need to communicate.***" The accused replies assertively, "***That is not helpful. You know that the SIEM logs are in my domain of expertise and it makes sense that I would doing it. We should all be doing whatever we do best at this point***."

Recovery Strategies

- Maximum Tolerable Downtime (MTD)
  - **Non essential**: 30 days
  - **Normal**: 7 days
  - **Important**: 72 hours
  - **Urgent**: 24 hours
  - **Critical**: Minutes to hours
- Recovery Time Objective (RTO)
- **Non essential**: 24 – 72 hrs
- **Normal**: 12 – 24 hrs
- **Important**: 4 – 12 hrs
- **Urgent**: < 4 hours
- **Critical**: Seconds to 1 hr

Question 13

- **Non-Forensic e-Discovery is designed to be procedural but also account for scalability, since cases can range from one custodian to thousands very quickly.**

☐ True

☐ False



2

Question 13

- **Non-Forensic e-Discovery is designed to be procedural but also account for scalability, since cases can range from one custodian to thousands very quickly.**

☑ True

☒ False

- **non-forensic e-discovery** refers to the process of collecting, processing, and reviewing Electronically Stored Information (ESI) for purposes other than litigation or law enforcement.
- This means that it can be used for a wide range of cases, from those with a single custodian to those with thousands of custodians.
- The **procedural nature** of Non-Forensic e-Discovery helps to ensure that all cases are handled in a consistent and defensible manner. This is important because the results of e-Discovery can have a significant impact on the outcome of a legal case.
- The **scalability** of Non-Forensic e-Discovery is important because the volume of ESI is growing exponentially. This means that e-Discovery tools and processes must be able to handle large volumes of data in a timely and efficient manner.

Question 14

- **What is NOT the right course of action in containing a breach?**

☐ Close off the initial attack vector

☐ Turn off the affected hosts

☐ Isolate the affected hosts from the network

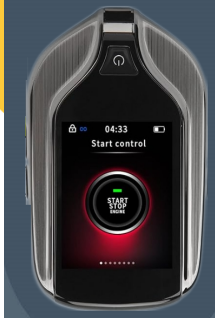
☐ Implement firewall, DNS, and web filtering blocks



2

Question 14

- **What is NOT the right course of action in containing a breach?**
  - ☒ Close off the initial attack vector
  - ☑ Turn off the affected hosts
  - ☒ Isolate the affected hosts from the network
  - ☒ Implement firewall, DNS, and web filtering blocks



Ollscoil Teicneolaíochta an Oirdheiscirt
South East Technological University

Hologram Keys Limited

Exercise Part 7

Getting to grips with the evolving chaos



War Room

- You announce, "***Okay, enough is enough. We have a CSIRP for a reason. We need to get back to the plan. You quickly see nodding heads and see some of the tension dissipate***".
- You continue, "***This is a stressful enough situation without adding team squabbling to the mix. I know everyone is tired and frustrated, but we've got to remain on track and on the plan. Roles are assigned based on the plan. We made those decisions when we developed the plan for a reason. We have no time to waste.***
- ***Let us go around the table and identify the responsibilities from the plan. You will be contacting the appropriate stakeholders. You will be managing containment and chain of custody. You will relay with PR and communications to ensure we have met regulations and are giving the right information at the right time. You, could you please make more tea? Thank you.***"

Question 15

- **What are some things to consider before recovering systems affected by a breach? (select all that apply).**

- ☐ Business Services
- ☐ Order of Operation
- ☐ Complexity
- ☐ Immediate restoration



Question 15

- **What are some things to consider before recovering systems affected by a breach? (select all that apply).**

- ☑ Business Services
- ☑ Order of Operation
- ☑ Complexity
- ☒ Immediate restoration

Question 16

- **Active defence is the concept of implementing additional security controls for monitoring purposes, especially on systems and resources that were affected by the breach.**

- ☐ True
- ☐ False



Question 16

- **Active defence is the concept of implementing additional security controls for monitoring purposes, especially on systems and resources that were affected by the breach.**

- ☒ True
- ☑ False

- Active defence is a broader concept that encompasses a variety of strategies for disrupting and thwarting cyberattacks. It also encompasses:
  - Implementing additional security controls
  - Gathering threat intelligence
  - Sharing threat intelligence
  - Disrupting attacks
  - Defending against attacks
  - Remediating attacks

Question 17

- **When communicating to external parties, which groups of people should be notified of the breach? (select all that apply).**

  - ☐ The media
  - ☐ Regulators
  - ☐ Customers
  - ☐ Government and law enforcement



Question 17

- **When communicating to external parties, which groups of people should be notified of the breach? (select all that apply).**

  - ☑ The media
  - ☑ Regulators
  - ☑ Customers
  - ☑ Government and law enforcement

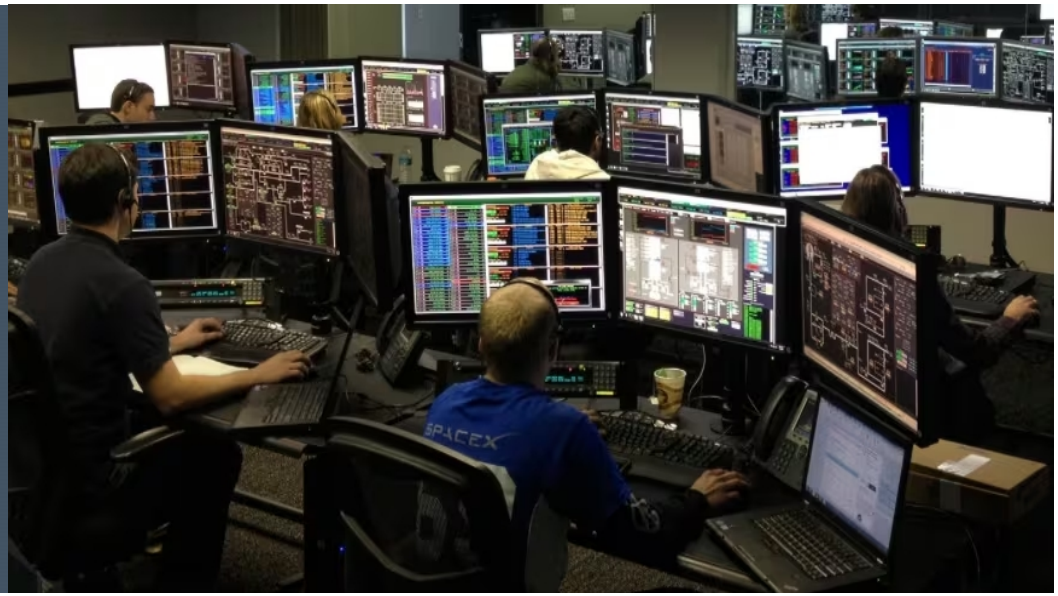


Ollscoil Teicneolaíochta an Oirdheiscirt
South East Technological University

Hologram Keys Limited

Exercise Part 8

Recovery and Notification



War Room

- Progress slowly begins to be made. Everyone is reminded of their roles and things are becoming clearer.
- The investigation is wrapping up and the next steps for communications are clear. You've now progressed into the Recovery and Notification phase.
- Systems need to come back up and you need to get production up and running ASAP.
- You have the data you need. You just need to be sure you protect it. The plan is working. The team has remembered what they put into it and why. The right information is coming in from the right people and they are making the best use of their time.

War Room

- The shutdown has locked out the bad actors for now and the data is captured to build a case. The team has a plan for the post mortem and will be able to complete an after-action review in an orderly fashion. Systems are being restored and production has resumed.
- All appropriate parties are in tight communication with their respective response liaison and everyone is on point and on message with those requesting information.
- The Forensics Team will continue their investigation and work to develop and document strategic recommendations for future enhancements.

Question 18

- **Gap assessments conducted after remediating a breach are a good way to review and identify holes in your security posture. What concept does this apply to? (Select all that apply):**

☐ People, Process, and Technology

☐ Risk Assessments

☐ Business Continuity Management

☐ Security Awareness and Training



2

Question 18

- **Gap assessments conducted after remediating a breach are a good way to review and identify holes in your security posture. What concept does this apply to?**

☑ People, Process, and Technology

☑ Risk Assessments

☒ Business Continuity Management

☒ Security Awareness and Training

Question 19

- **What can be done to minimise the impact to an organisation's reputation after a breach?**

- ☐ Do not inform the media, customers, or public about the breach
- ☐ Ensure your legal and PR teams have a strategy to prevent your brand tarnishing
- ☐ Be transparent and honest, and avoid delaying any updates to relevant parties
- ☐ Rebrand the organisation entirely so it appears like a new company



2

Question 19

- **What can be done to minimise the impact to an organisation's reputation after a breach?**

- ☒ Do not inform the media, customers, or public about the breach
- ☑ Ensure your legal and PR teams have a strategy to prevent your brand tarnishing
- ☑ Be transparent and honest, and avoid delaying any updates to relevant parties
- ☒ Rebrand the organisation entirely so it appears like a new company

Question 20

- **What is the purpose of cyber insurance?**

- ☐ Help organisations reduce or mitigate risk exposures by offsetting the costs of recovering from a security breach or incident
- ☐ To help purchase security tools
- ☐ Provide security services in the event of a security breach or incident
- ☐ To stop hackers



2

Question 20

- **What is the purpose of cyber insurance?**

- ☑ Help organisations reduce or mitigate risk exposures by offsetting the costs of recovering from a security breach or incident
- ☒ To help purchase security tools
- ☒ Provide security services in the event of a security breach or incident
- ☒ To stop hackers



Learning Outcomes

Learning outcomes

You should now be able to:

- Evaluate complementary IDS/IPS and SIEM detection infrastructure. ✓
- Formulate incident response frameworks and establish an operational CSIRT and war room. ✓
- Execute incident triage, implement containment strategies, and preserve digital evidence forensically. ✓
- Manage secure environment restoration, post-incident notifications, legal obligations, and continuous improvement reviews. ✓

EUR ING Dr Diarmuid Ó Briain
Innealtóir Cairte agus Léachtóir Sinsearach

D +353 59 917 5000 | E diarmuid.obriain@setu.ie | **setu.ie**
Campas Bhóthar Chill Chainnigh, Ceatharlach, R93 V960, Éire

EOLAS-I Research Centre

Thank you