Incident response

Exercise 1

Scenario Overview

Hypothetically, a senior consultant's Microsoft 365 mailbox was hijacked and used to send fraudulent invoices and urgent wire-transfer requests from their coworkers. Logs show a foreign IP login, creation of malicious inbox rules, downloads of attachments, and multiple staff falling for a phishing link and lastly MFA was not yet enforced across all accounts. This incident could lead to financial losses for the company, damage its reputation, result in legal ramifications, and, at worst, risk leaking or tampering with clients' data.

1. Detection stack and alert correlation

First, our email filter (e.g. Microsoft Defender for Office 365) noticed strange new inbox rules and a rush of outgoing fake invoices. Next, our sign-in logs showed the same account logging in from another country—a red flag called an "impossible travel." At the same time, the antivirus on the employee's computer saw the browser send the password to a phishing site and download shady files. Finally, our central monitoring system (the SIEM) connected all those dots within a short period of half an hour (for example) and opened one urgent ticket for the security team. The SIEM (e.g., Splunk, IBM QRadar) aggregated logs from our email filters (Microsoft Defender), EDR, and sign-in systems. It correlated mailbox rule changes, foreign IP logins, and phishing link activity into one high-priority alert. So SIEM acts as the 'brain' of detection, unifying endpoint and network data for faster threat recognition.

Because all the tools talked to each other, we got one clear warning - "stolen password, hidden inbox rule, scam emails sent" - instead of four separate, confusing alerts. That quick, unified view let us shut the account, delete the rule, and block the attacker before they could move on to other mailboxes or the finance system.

2. Observed behaviors: MITRE ATT&CK mapping

It unfolded in three simple moves: first, an employee clicked a fake link and handed over their password - classic phishing (ATT&CK T1566). Next, the adversary did credential reuse: used that same password from a different country (a different IP) to log into the cloud mailbox, abusing a real account so the break-in looked legitimate (T1078.004). Finally, once inside, they set up secret forwarding and hiding rules so their scam emails stayed out of sight, a "hide-your-tracks" trick labeled inbox-rule manipulation (T1564.008). Together, those steps show how the attacker got in, stayed in, and covered their tracks later. Here are some more along with these.

Phishing – T1566.002 (Spearphishing Link)
The attacker sent a fake email with a malicious link that tricked multiple employees into entering credentials. This technique fits T1566.002, where links are crafted to appear trustworthy but redirect users to credential-harvesting pages.

Valid Accounts – T1078.004 (Cloud Accounts)
The attacker used stolen credentials to log in to Microsoft 365 from an unusual foreign IP address. Since no malware was dropped and access came via legitimate means, this aligns with T1078.004, where cloud-based user accounts are abused without triggering traditional endpoint defenses.

Email Collection – T1114.002 (Remote Email Collection)
Once the attacker gained access, they downloaded sensitive email attachments and viewed prior communications. This maps to T1114.002, which refers to accessing email content remotely from compromised accounts. This stage reflects the adversary's data collection intent before moving to financial fraud.

Inbox Rule Manipulation (T1564.008) matches perfectly since the attacker hid evidence and controlled information flow by secretly forwarding and hiding emails.

Command and Control – T1071.003 (Application Layer Protocol: Mail Protocols)
Although no remote shell was observed, if the inbox forwarding was configured to send messages to an external server or attacker-controlled email, this could qualify as T1071.003, which involves using standard mail protocols for command-and-control communication or data exfiltration.

3. Incident response actions

First, we stop everything right away happening: we disable the hijacked mailbox and any other account showing odd logins, force-reset their passwords, and revoke all active sessions and refresh tokens so the attacker is kicked out immediately. Next, we delete the rogue inbox rules through PowerShell (Get-InboxRule | Remove-InboxRule) or even the Gmail Audit API to undo their hidden forwarding. At the same time we add the attacker's IP range, the phishing domain, and any related URLs or hashes to our email gateway, web proxy, and firewall blocklists so no one else inside the company can reach them or download the same payloads. And then we also quarantine all computers that typed passwords into that fake page. While that's happening, the endpoint protection tools run deep scans to be sure no malicious files / secret app permissions like OAuth grants were left behind. We also reviewed traffic logs using tools like Security Onion and Wireshark to identify any abnormal connections initiated by the attacker, as shown in our monitoring section. IDS tools such as Snort or Suricata helped confirm that no data exfiltration occurred over suspicious domains during or after the phishing incident. This gave us confidence that the attacker's access was limited to email fraud and did not extend into broader lateral movement or data theft. We now double-check that every user and especially admins , now need MFA to log in.

Once the mess is contained, we put things back the way they should be: restore any missing or altered emails from backup, verify that no bogus invoices slipped through our finance systems and roll them back if they did, and watch the sign-in logs for a month to catch any repeat password spray or token replay attempts. Finally, we enable MFA for every user, build an

automated response rule that triggers a single, clear alert whenever an unusual sign-in and an inbox-rule change happen together, and update our phishing awareness training with screenshots from this incident so employees can recognize the same trick in the future, and also be able to generally prevent themselves of being deceived. By reminding everyone not to click unknown links sent to their work addresses, we greatly reduce the chance of another phishing outbreak.

So the 4 distinct steps in titles are: Containment, eradication, recovery and training lessons for staff.

4. Communications plan internally vs externally

We have top management first: The CISO (the one who runs the response) starts by briefing the executives and board: what happened, how it affects the business, and how long the fix will take—so leadership at the end is fully informed. PR and legal then notify the possible affected clients, explaining the fake-invoice scam, the steps we're taking to protect them, and assuring them their data is still safe. If any personal data might be at risk, the Data-Privacy Officer files the required report to regulators (such as GDPR authorities) within 72 hours. And finally, Internal Communications and the SOC send every employee a "stop, reset, report" bulletin: reset your password, turn on MFA, and report anything odd, with an easy FAQ that explains the new MFA rule, come at any mysterious case into contact. This approach aligns with the Crisis Management Communication practices, which stress the importance of internal transparency, external accountability, and calm leadership messaging. The CISO, legal, and PR teams work together to ensure messaging is timely, compliant (e.g.. GDPR), and protects the firm's reputation while maintaining client trust.

5. Post – incident metrics

After an incident, track three core metrics to see whether your defenses are actually getting stronger. **Mean Time to Detect (MTTD)** shows how quickly your sensors surface initial-access tactics like ATT&CK's T1566.002 (Spear-phishing Link); the shorter the gap between a user's click and your first alert, the less room an attacker has to pivot. **Mean Time to Contain (MTTC)** measures the span from that alert to full containment—password resets, session revocations, and malicious inbox-rule cleanup—and therefore reflects how efficiently your playbooks blunt techniques tied to defense-evasion and collection (e.g., T1114 Email Collection). Finally, your **Technique Coverage Ratio (TCR)**—the percentage of relevant ATT&CK techniques for which you've validated detections—highlights blind spots across all tactics, steering detection-engineering efforts toward the gaps that matter most. Together, faster MTTD and MTTC shrink attacker dwell time while a rising TCR proves you're systematically closing coverage gaps, giving you hard evidence that incident-response and detection programs are improving in ways that map directly to how adversaries operate.

6. Best detection method for obfuscated-URL phishing

Instead of just checking links against a bad list or flagging anything that looks unusual, we watch what actually happens when someone clicks. We open each link in a safe, isolated space, follow every hop in the redirect chain, and see which users land on which pages. That behavioral view lets us spot real threats even when attackers hide them behind short URLs, pack them into sneaky HTML files, or use brand new websites that haven't been blacklisted yet. This way we give a good chance of recording shady domains, IPs, and evidence that will contribute to the blocklists and protect everyone else too. Behavioral detection and AI-driven correlation help catch techniques like T1566 (Phishing) and T1564.008 (Inbox Rule Manipulation), especially when they evolve too fast for signatures.

So, the best detection method for phishing campaigns using obfuscated URLs is behavioral detection. Signature-based methods rely on known "bad" URLs, so they easily miss new or disguised links. Similarly, anomaly-based detection often overlooks carefully disguised phishing emails, since attackers deliberately make their messages look normal enough to avoid suspicion. Behavioral detection, on the other hand, actively follows and analyses what happens when a user clicks a link watching for suspicious actions like unexpected redirects or downloads - making it the most effective approach for spotting even well hidden phishing attempts.

Exercise 2

Scenario Overview

Our company, based in Europe, provides cloud services (SaaS, PaaS, and IaaS) to multiple tenants, including sensitive sectors such as healthcare and finance. Recently, one of our healthcare clients experienced a ransomware attack that encrypted critical patient records. To effectively handle similar incidents and safeguard all client data, we must maintain a detailed Incident Response Plan (IRP) compliant with EU regulations including GDPR, ISO 27035, NIS2 Directive, and aligned with best practices from frameworks like NIST 800-61.

1. Purpose & scope

The purpose of our IRP is to ensure rapid and coordinated detection, containment, and recovery from cyber incidents—particularly ransomware—that may compromise data confidentiality, integrity, or service availability for clients. The scope includes both tenant environments and our central infrastructure, supported by monitoring tools such as SIEM, EDR, and IDS, aligning with NIS2 and frameworks like NIST 800-61. Special emphasis is placed on protecting high-risk sectors like healthcare and finance, where compliance with GDPR, HIPAA, and PCI-DSS is essential.

Risk Classification

To handle incidents clearly and efficiently, we categorize them according to their severity:

Severity What must the	**Confidentiality Data Exposure**	**Integrity Data -Code Change (e.g. T1565)**	**Availability Service Disruption (e.g. T1499/T1485)**	**Compliance,Safety Regulatory & Life**

SOC do first?	(e.g. T1041/T1567)			Impact (e.g. T1491)
1 - Low	Only nonsensitive meta-data glimpsed (e.g., hostnames).	Trivial config tweak : easily rolled back.	Brief hiccup, single tenant, minutes.	No legal/ patient-safety trigger.
2 - Medium	Small set of sensitive records at risk.	Unauthorized change to non-critical info; routine restore.	Noticeable outage (≤ 1 h) or affects one tenant.	Possible but unconfirmed reporting obligation.
3- High	Large batch of regulated data (e.g., payment or health) exposed.	Critical business or clinical data altered; audit required.	Multi-tenant or extended (> 1 h) outage.	Confirmed breach or patient-safety concern.
4 - Critical	Mass exfiltration or public leak.	Destructive or fraudulent tampering that threatens core operations.	Platform-wide or life-critical downtime.	Mandatory disclosure, heavy fines, or threat to life.

2. Incident response team roles

Our Incident Response Team has clearly defined roles to streamline our response:

1. **Incident Commander** leads and coordinates the response.
2. **Security Operations Centre** (SOC) **Analysts** detect and investigate alerts.
3. **Digital Forensics Specialists** conduct detailed technical analysis.
4. **Cloud Operations Engineers** manage our cloud environments, isolating compromised resources.
5. **Client Liaison** communicates directly with impacted tenants.
6. **Data Protection Officer** (DPO) manages regulatory compliance, such as GDPR reporting.
7. **Legal and Public Relations teams** handle external communication transparently and effectively.
8. **External Security Experts** provide additional expertise as needed.

These roles ensure accountable incident handling. Having responsibilities defined reduces confusion during high-stress scenarios and supports coordinated action, as emphasized in our course slides on team structure.

3. Ransomware Response Procedure (Phase-by-Phase)

1. Detection

This is the first sign that something's wrong. In a ransomware attack, this might be a user reporting that they can't open files, strange file extensions (e.g. .locked), or an alert from antivirus or EDR tools. The Initial Access tactic from MITRE ATT&CK is relevant here: attackers might have used phishing (T1566) or exploit public-facing apps (T1190) to get in. The Execution tactic also applies, such as Command and Scripting Interpreter (T1059) to run malicious code after gaining entry.

2. Analysis

Here, the response team investigates to understand the scope and method of the attack. They check logs, scan systems, and identify which machines were affected and how the malware spread. MITRE's Discovery (T1087, T1046) and Lateral Movement (T1021, T1080) tactics are key, as attackers often explore the network and move between systems before launching the ransomware. Understanding these behaviors helps responders trace the attack path.

3. Containment

The goal now is to stop the attack from spreading further. This may involve disconnecting infected systems from the network, disabling compromised accounts, or blocking IPs. The Defense Evasion (T1070) tactic is relevant here - attackers may try to hide their presence (clearing the logs for example) to avoid detection during containment. Knowing these tactics helps our team act fast and limit further damage.

4. Eradication

In this phase, the team removes the ransomware and any backdoors left behind. They might reinstall systems, patch vulnerabilities, and reset passwords. MITRE's Persistence (T1053, T1547) and Privilege Escalation (T1068) tactics are important because attackers often install tools that let them return later or gain higher access. These must be identified and removed completely.

5. Recovery

Now the focus is on restoring systems and getting operations back to normal. This includes restoring backups, testing systems, and monitoring for any signs of reinfection. While MITRE doesn't have a specific "recovery" tactic, the impact of tactics like Impact (T1486 – Data Encrypted for Impact) is still relevant. This phase also includes validating that the ransomware's effects have been fully removed and that no attacker access remains.

4. Incident Response Playbook: Credential Harvesting

Step	Phase	Description	Tools/Methods examples	Relevant MITRE ATT&CK Tactic / Technique
1	**Preparation**	Train staff to recognize phishing and implement strong password policies and MFA. Monitor high-value targets.	Awareness training, vulnerability scans, MFA, IAM systems	*Reconnaissance, Initial Access*
2	**Detection**	Alert from SIEM or EDR about suspicious login attempts, phishing links, or unauthorized keylogger activity.	SIEM (Splunk, QRadar), EDR (CrowdStrike, Defender), IDS (Snort)	*Credential Access (T1556), Initial Access (T1566)*
3	**Analysis**	Confirm credential harvesting via log correlation, traffic inspection, endpoint forensics. Identify affected users/systems.	Wireshark, ELK Stack, endpoint logs, MITRE ATT&CK navigator	*Discovery (T1087 – Account Discovery)*
4	**Containment**	Disable affected accounts, block malicious IPs/domains, isolate infected devices.	AD account lockout, firewall rules, proxy filtering	*Command and Control (T1071)*
5	**Eradication**	Remove malware, scripts, or keyloggers used for harvesting. Patch exploited vulnerabilities.	EDR quarantine, antivirus scan, patch management	*Persistence (T1547), Defense Evasion (T1070)*
6	**Recovery**	Reset credentials, restore clean systems from backup, re-enable users, closely monitor for reinfection.	IAM tools, backup systems, audit logs	*Impact (T1499 – Service Disruption)*

7	**Post-Incident**	Conduct lessons learned, update playbooks, brief leadership. Train users based on the attack vector used.	Internal reports, IR debrief, tabletop exercise	*Continuous Improvement*

A. How would we test out IRP's effectiveness?

! T**abletop Exercises**
Walk through the credential-harvesting scenario with our incident response team. Each member explains what they would do at every step. We use a simulated attack path (for example phishing + keylogger installation) and see how the team responds.

! **Red Team / Blue Team Simulation**
We simulate credential theft using phishing or malware in a safe test environment. We leave the red team execute the attack while the blue team applies the playbook.

! **Metrics and Evaluation**
Measure performance using:

- **MTTD** (Mean Time to Detect)
- **MTTC** (Mean Time to Contain)
- **MTTR** (Mean Time to Recover)
  we would compare results with previous tests or industry benchmarks.

! **Update Based on Results**
After testing, we update the IRP to cover missed steps, unclear actions, or any confusion faced by the team.

A good recommendation: a combination of tabletop simulations and operational exercises to test IRP readiness and ensure role familiarity.

To understand which attack techniques my organization can detect or respond to, I can use the MITRE ATT&CK Navigator—a free web-based tool that lets me interact with the ATT&CK matrix visually: https://mitre-attack.github.io/attack-navigator/

1. I create a new layer for my environment:
   I can make a new layer where I list all the techniques my security tools (like SIEM, EDR, IDS) currently detect. For each technique, I can for example, use a color code: green for strong detection, yellow for partial, and red for not detected.
   Also, add comments to mention which tools detect each technique (e.g, "EDR – CrowdStrike", "SIEM Splunk rule").

2. Overlay Threat Intelligence optionally
   I can add a second layer showing techniques used by threat groups targeting the industry (e.g., FIN7, APT29 for finance/healthcare). This helps prioritize which techniques matter most.
3. Identify Detection Gaps: I can look for techniques that are: Red or uncolored (meaning undetected), common in real-world attacks or linked to Initial Access, credential access, or Impact (high-risk stages).

And lastly I'll end up with a heatmap-style view of the detection capability across all tactics (like Initial Access, Execution, Persistence, etc..)

- What actions would you take to close any detection gaps you find?

Actions:

- Tune existing tools: Improve detection rules in SIEM and EDR where logs exist but no alerts fire.
- Deploy new tools: If gaps are technical (e.g, no script logging), introduce the necessary tooling.
- Red team testing: Simulate attacks in undetected techniques to validate and refine the playbook.
- Prioritize high-risk ATT&CK tactics: Focus efforts on critical paths like Initial Access, Credential Access, and Impact.
- Maintain visibility: Regularly update your ATT&CK Navigator map as your tooling, environment, and threat landscape evolve.