TASK 2

A realistic Cybersecurity incident scenario: (**Phishing Attack**)

**Context:**

About 500 people work for XYZ Corp, a medium-sized company that provides software development services to a wide range of clients. These workers include project managers, software engineers, human resources professionals, and administrative staff. Even with a strong IT setup that includes email servers, firewalls, and antivirus software, the company is still vulnerable to phishing attacks—a common mistake that many businesses encounter—despite having a strong IT infrastructure.   
Top of Form

**Objectives:**

Testing XYZ Corp's incident response capabilities in the case of a sophisticated phishing attack is the main goal of this scenario. The purpose of the scenario is to evaluate how well the organization can identify, stop, and lessen the effects of the attack while causing the least amount of interference with regular business operations. The scenario will also assess the efficiency of employee awareness and training initiatives in identifying and reporting phishing attempts.

**Scope:**

A phishing email campaign that targets employees of XYZ Corp. will be simulated in this scenario. Phishing emails are designed to look like they are from a reliable source, like a company executive or a client.  
Phishing emails are known to include harmful links or files that aim to compromise employee credentials or infect company computers with malware.  
During the course of the scenario, which will last between 24 and 48 hours, employees will periodically receive various phishing emails.  
  
Incoming phishing emails will be monitored and analysed by the incident response team, which will also be in charge of identifying compromised devices or accounts and putting in place the necessary countermeasures to lessen the threat.  
The scenario aims to replicate multiple response activities, including forensic analysis, password resets, and network isolation of impacted devices.

**Incident detection**

Analyst role for Monitoring and Analysis Intern:

* Using email security tools and records, monitor incoming emails for indications of phishing activity.
* Examine dubious emails to spot typical phishing tell-tales like faked sender addresses, dubious attachments, or connections to dubious websites.
* Record findings and notify senior incident response team members of any possible threats so they can be looked into further.
* Contribute to the creation of phishing detection protocols and guidelines by utilizing observed trends and patterns.

Monitoring User Account Activity:

* In order to spot any unusual login attempts or unlawful access, the Monitoring and Analysis Intern examines user account activity logs.
* Logs reveal numerous unsuccessful attempts within a brief period of time to log in from different user accounts.
* These actions are flagged by the intern as possible signs of a credential harvesting effort, and the incident response team is notified for additional analysis and action.

**Response plan execution:**

Identification of Incident: Using email security monitoring tools, the Monitoring and Analysis Intern finds a large number of suspicious emails with possibly harmful attachments. She then notifies the incident response team of the discovery.

Incident Review and Documentation: The Forensics Intern carefully records all actions performed and information gleaned during the response phase. The incident response team conducts a thorough post-event analysis to evaluate the efficacy of response protocols, pinpoint lessons learned, and offer suggestions for enhancement following the incident's containment and mitigation.

**Forensics Analysis:**

Evidence Gathering: The forensic intern starts by gathering digital evidence from the systems that are impacted. Disk images, RAM dumps, network traffic samples, and pertinent logs are all included in this.   
  
Memory Analysis: To find active processes, open network connections, and any malicious malware inserted into memory, the intern examines memory dumps from infected systems. They search for indications of malware execution or unusual activity that could point to a security breach.  
  
Network Traffic Analysis: To determine the source, network traffic captures are examined.

Log analysis: To piece together the incident's timing, logs from a variety of sources, such as firewalls, intrusion detection systems (IDS), and endpoint security solutions, are examined. The intern uses log data to correlate and determine the attacker's initial vector of attack, lateral movement inside the network, and actions.  
  
Timeline Reconstruction: The intern creates a timeline of the incidents' prelude and course based on the information acquired from the logs and evidence. This timeline sheds light on the attack's development and helps identify the attacker's order of action.  
  
  
Root Cause Analysis: The intern determines the incident's primary cause in light of the results of the forensic analysis. This may involve elements like unpatched software flaws, lax security measures, or staff members who are easily tricked by phishing emails.

**Evidence Collected and Logs Prepared for Post-Event Analysis**:   
  
Images on Disk: Replicas of images on disk from devices impacted.

Captured memory dumps from compromised computers are known as memory dumps.

Packet captures from intrusion detection systems or network devices are examples of network traffic captured.

Firewall logs: Recordings of network activity, both entering and leaving the system.

Endpoint logs are the records of system events and activities that come from endpoint security systems.

Email server logs: Records of all email exchanges, including sent and received messages.

Web servers that are acting as command-and-control servers or hosting potentially harmful content can save their logs.

Application logs: These are logs produced by pertinent programs or services that were part of the incident; examples include database access logs and authentication logs.

**Evaluation of the Response Plan's and the Actions Taken's Effectiveness**:  
  
In general, the XYZ Corp. response plan was successful in containing and minimizing the simulated phishing event. Among the important things the reaction did was:  
  
  
Quick Discovery and Notification: The problem was quickly discovered thanks to efficient email security tool monitoring, which enabled the response team to quickly start containment procedures. All pertinent parties were promptly notified of the occurrence thanks to the strict adherence to notification protocols.  
  
Role-Based Response: The incident response team's interns who were given designated responsibilities made a valuable contribution to the response effort. A coordinated and effective response was made possible by the interns' completion of all assigned tasks, which included monitoring, analysis, communication, and forensic investigation.  
  
Containment and Mitigation Strategies: To limit the situation and stop additional harm, the response team reset passwords, isolated compromised machines, and removed malware. Proactive security measures are valuable, as evidenced by the fact that employee awareness training helped stop more successful phishing attacks.   
  
Evidence collection and forensic analysis: A comprehensive forensic analysis was carried out on the impacted systems and data, which helped the team identify the incident's primary cause and collect data for post-incident study. In addition to ensuring that no important artifacts were missed, this all-encompassing strategy offered insightful information about the attacker's tactics, methods, and procedures (TTPs).

Areas for Improvement and Lessons Learned:  
  
Enhanced Phishing Awareness Training: Although employee awareness training helps stop more successful phishing attempts, there is still space for improvement in terms of educating people about the ever-changing strategies employed by attackers. Employees can be better equipped to identify and report phishing attempts by receiving ongoing training and participating in simulated phishing exercises.  
  
  
A more thorough and uniform documentation of response activities and conclusions would help with post-event analysis and knowledge exchange. This is an improvement above current incident response documentation. It can be easier to coordinate future response efforts and guarantee uniformity amongst response teams by establishing explicit protocols for recording incident response actions, including gathering and analysing evidence.  
  
Strengthened Endpoint Detection and Response (EDR): By making an investment in EDR solutions, an organization can enhance its capacity to identify security issues and take appropriate action in response. With the real-time insight that EDR systems offer into endpoint actions, proactive threat hunting and quick reaction to new threats are made possible.   
  
Regular Exercises in Incident Response: Regular exercises in incident response and tabletop simulations can assist verify the efficacy of the response plan, spot procedural weaknesses, and prepare staff to act professionally in emergency situations. To guarantee thorough readiness for cyber incidents, these drills should imitate real-world situations and involve cross-functional teams.

**Documentation of the incident response processes, actions taken, and outcomes. Presenting the findings and recommendations for enhancing incident response capabilities.**

Process for Responding to Incidents: Initial detection of the event came from email security tool monitoring, which found a large number of erroneous emails with possibly harmful attachments.

Notification and Coordination: Key stakeholders, such as IT employees, HR staff, and executive leadership, were promptly informed about the issue, along with the incident's existence. In order to efficiently coordinate response operations, communication channels were set up.

Role Assignment: To ensure a well-organized and effective reaction, interns were given particular duties within the incident response team, such as communication liaison, forensic investigation, and monitoring and analysis.

Containment and Mitigation: In order to contain the problem and stop more harm, compromised devices were disconnected from the network, impacted accounts had their passwords changed, and malware was eliminated.

Evidence Collection and Forensic study: Extensive evidence was gathered for post-incident study and forensic analysis was carried out on the impacted systems and data in order to determine the incident's primary cause.   
  
Training on Employee Awareness: To enforce safe email practices and stop more successful phishing attempts, all employees received awareness messages and reminders.

**Results:**   
  
Sensitive data was kept safe from future contamination by the effective containment and mitigation of the incident, which also reduced the impact on business operations.  
By gaining important insights into the attacker's tactics, methods, and procedures (TTPs), forensic investigation helped the organization fortify its defences and avert future occurrences of this kind.   
  
Additional successful phishing attempts were avoided thanks to employee awareness training, underscoring the significance of continuous security education and awareness campaigns.

**Findings and Recommendations for Enhancing Incident Response Capabilities:**

Ongoing Education and Knowledge: Conduct frequent phishing awareness training sessions and role-playing games to teach staff members how to identify and responsibly report phishing attempts. Highlight the changing strategies that attackers are using and offer helpful advice on reducing the danger of phishing attacks.  
  
Investing in advanced threat detection solutions, like email security enhancements and endpoint detection and response (EDR), can increase early identification of security problems and provide proactive threat hunting skills. This will lead to enhanced monitoring and detection.

Establish and record standardized incident response processes, which should include communication protocols, escalation routes, and clearly defined roles and duties. Make sure that every member of the response team has received training on these protocols, and that you regularly test their efficacy using exercises.  
  
Collaboration and Communication: Boost lines of communication and cooperation between the IT personnel, the incident response team, and other pertinent departments. To enable quick thinking and decision-making in the event of a security incident, promote an environment of openness and information exchange.  
  
Review of the Event and Lessons Learned: Carry out thorough post-event evaluations in order to pinpoint opportunities for enhancement and insights gained from every security occurrence. Prioritize investments in cybersecurity capabilities, update security policies, and improve incident response processes using these findings.