About the Course Project

Welcome to the final project for the **Incident Response and Digital Forensics** course. In this project, you will apply the knowledge and skills learned in this course to a real-world-inspired scenario.

The tasks in this hands-on project correspond to the activities performed by an incident response team leader as part of their critical organizational responsibilities, which include creating an incident response plan and outlining the key actions for conducting a digital forensics investigation.

Imagine yourself as an incident response team leader hired by SecureSync Corp., a mid-sized technology company, while you complete this project.

The final project is divided into two parts:
Part 1: Create an incident response plan using the NIST incident response plan
Part 2: Identify the required steps for a digital forensics investigation

While performing the tasks, ensure you adhere to the instructions and create comprehensive deliverables.

You will be provided with one text based documents, where you can store your answers. You'll copy and paste your answers for each task, referred to a prompt, in the online final project for peer review.

You will then serve as a peer reviewer for another peer. You will review their project submission using the provided rubric and document feedback. You will, in turn, receive feedback on your submission from a peer reviewer.

After completing your peer review, review the example solutions provided to compare your answers to the solution examples.

You can then participate in an optional discussion with your peers and reflect on the key takeaways from your final project submissions.

To summarize:

- Read and follow the instructions carefully to complete and submit the project.
- Complete your peer review.
- Compare your submissions with the project solution examples.

Final Project: Incident Response and Forensics

Welcome to your final project where you will apply your knowledge of incident responses and forensics to a real-world scenario. This is a two-part final project.

In **Part 1**, you'll review a case study and complete related tasks where you identify tasks that are part of the NIST incident response framework for this organization.

In **Part 2**, you will create an incident response plan that outlines the steps your organization would follow for any digital forensics investigation.

Next review the **Before you begin** instructions and follow the instructions to download the files that contains the questions you'll answer as part of your final project. You will also save your answers to these questions in these documents. Later, you'll copy and paste your answers into text files for evaluation and grading.

Before you begin

Before you begin your project tasks, you need following applications available on your computer:

- A text editor application such as:
    - Microsoft Word
    - A PDF viewer
    - Google Docs
    - Notepad or other text editor

To complete your work, you will open the following text-based solution document on your computer and save your answers in that document.

Final Project Solution document

When you submit your final project answers you will copy and paste your answers from the text document into the provided text upload fields.

Download your documents

This course provides the following text based tasks for Part 1 and Part 2 final project tasks.

1. Right-click to download and save the following text document to an accessible location. You'll enter your answers to the final project questions within this text based document. You can open this document using a text editor, Google Docs, or other text file compatible word processing program.

2. Next, review the steps needed to save and submit your text-based final project answers.

Saving and submitting your text-based final project answers

Follow the instructions within each file to complete your final project assignments.

1. Locate your downloaded solution file.
2. Follow the instructions within the file to complete your final project assignments.
3. Save your file to an accessible location.
4. Follow the instructions in the course to submit your final project answers.

Let's get started with your final project.

Part 1: Create the incident response plan details using the NIST incident response framework.

Review the following case study. Afterward, open the template, and answer the questions based on the information supplied in the case study. Remember to save your answers in the document provided. You'll copy and paste your answers into text fields located within the online final project assignment.

Case study: Incident response at SecureSync Corporation

SecureSync Corporation is a mid-sized technology company that develops cloud-based solutions for businesses. With a team of over 500 employees, this organization prides itself on innovation and reliability. The company is headquartered in San Francisco with additional offices in Austin and Boston. The company's IT infrastructure supports a client base of approximately 200,000 users. Although the organization feels confident in its incident response capabilities, the company does not have a formalized incident response plan.

Technical details

The company's IT infrastructure follows a hybrid model that combines on-premises servers with cloud-based services, specifically using Azure and Amazon Web Services (AWS) for scalability and redundancy. These services host the company's cloud-based solutions, which are segmented into virtual private networks (VPNs) for enhanced security. The organization's network architecture supports a multilayered security approach, incorporating firewalls, intrusion detection systems (IDS), and data encryption protocols.

Current security tools and protocols

SecureSync Corporation uses the following security tools and protocols:

- **Firewalls:** SecureSync Corp. uses hardware and software firewalls to control incoming and outgoing network traffic based on predetermined security rules. These firewalls are critical in defending against unauthorized access.
- **Intrusion detection and prevention systems (IDPS):** The company uses real-time IDPS to monitor network traffic for suspicious activities and potential threats. These systems alert the IT team when anomalies are detected.
- **Endpoint security:** All employee devices are equipped with endpoint protection software, such as antivirus, threat detection, and response capabilities, to safeguard against malware infection and data breaches.
- **Encryption and data security:** Company data at rest and in transit is encrypted using advanced encryption standards (AES).
- **Access controls:** Role-based access control (RBAC) ensures employees can only access the resources necessary for their roles, minimizing the risk of internal threats.
- **Logging and monitoring:** Comprehensive logging configurations capture detailed records across all systems and applications. These logs play a crucial role in incident detection and retrospective analysis.

Although SecureSync Corp. understands the importance of incident response, the company does not have a formal incident response plan documented. The Chief Information Officer (CIO) recognizes the need to document the preparedness plan, which will now include:

- Updated staff training programs focused on recognizing phishing attempts,
- Prompt reporting of suspicious activity
- Regular security drills.

The organization has established key personnel roles, which include an incident response team leader, a communication liaison, and technical specialists.

The organization also invested in advanced detection software systems to enhance their defenses against cyberthreats.

Incident response in action

On a busy Monday morning, the IT security team at SecureSync Corp. detected unusual network activity. The IT security team identified multiple unauthorized access attempts on the company's email server, which stores sensitive client data and internal communications. This attempt raised concerns about a potential data breach. Initial scans revealed malware deployed to siphon sensitive data to an unknown offsite server.

During the incident investigation, the following information was discovered:

- The IT security team received alerts about anomalous behavior indicative of a cyberattack using the company's Incident Detection System (IDS).
- Log files revealed remote logins occurring at odd hours and from unusual locations.
- Automated scripts captured packet details, suggesting potential data exfiltration.

The company activated the incident response team upon confirmation of the breach and began a detailed investigation. Analysts discovered that the attack vector was a sophisticated spear-phishing email that compromised user email accounts and gave attackers backdoor access. The incident response team constructed a timeline to trace the incident's development and identify affected systems.

The team's rapid response initially focused on short-term containment to limit further damage. The team sealed off critical access points by deactivating compromised accounts and isolating affected network segments. The company performed an extensive threat hunt to identify the malware. Threat intelligence research helped the team understand the malware's typical behavior. The team used these insights to devise an eradication plan that included removing malicious code from all infected systems. After confirming malware eradication, the team shifted their efforts to recovery. The team restored systems from secure backups and conducted system-wide checks to ensure no residual damage or vulnerabilities remained undetected. The team then established continuous monitoring to detect any attempts at further breaches or compromises.

With the incident under control, SecureSync Corp. initiated a comprehensive post-mortem analysis to evaluate its incident response strategy. The analysis focused on response times, communication efficiency, security protocol effectiveness, and areas needing improvement. Team debriefings highlighted necessary enhancements in the incident response plan, particularly regarding threat intelligence sharing and expedited cross-departmental communication. New preventive measures were discussed and documented, and actions were taken to patch identified vulnerabilities.

SecureSync Corp. also planned educational workshops to reinforce cybersecurity practices among employees to mitigate potential future threats. The management also

recognized the importance of public transparency and issued a client-facing report assuring clients of improved security measures, reinforcing trust, and retaining brand credibility.

Next, complete your **Part 1** final project assignment tasks.

Complete the Final Project Part 1 Assignment Tasks

After you open the **Part 1 solution document** where you can save your answers complete the following tasks. The following tasks are numbered to match how you will supply the answers for **Submission and Evaluation**

When responding to a security incident, you need a solid team that knows their roles and moves fast. Here are four of the most important positions I'd include on my team and what I'd expect from them:

Prompt 1

List the roles and responsibilities of four key team members in the incident response team.

Role 1: Incident Response Lead (me)

I'd be responsible for coordinating the response from start to finish. That includes documenting everything, assigning tasks, checking with each role, and making sure we're aligned with NIST's phases. I'd also act as the bridge between technical staff and leadership; no nothing gets lost in translation.

Role 2: Communications Liaison

This person dives deep into the system: checking how the malware got in, how far it spread, and what kind of damage it did. They'd also help guide decisions on containment and recovery, especially when systems are critical to operations.

Role 3: Security Analyst

They'd monitor alerts, dig through logs, and help identify indicators of compromise (IOC's). Their job is to stay hands on with the tools we use daily and sport unusual patterns before they turn into something bigger.

When it comes to early detection, monitoring is everything. In this scenario, the attack came through a spear-phishing email, so I'd want to focus on tools that can catch the suspicious behavior across email, endpoint, and network activity.

Prompt 2

List the four methods, or tasks, you can use to monitor this company's internal systems for unusual activity.

Here's what I would monitor and how:

Method 1: Email Gateway & Span Filters:

I'd start by reviewing logs from or email security gateway (like Proofpoint or Microsoft Defender). I'd be looking for unusual subject lines, strange attachment types, or links spoofing addresses.

Method 2: Endpoint Detection & Response

Tools like CrowdStrike or SentinelOne would help flag the moment malware starts behaving oddly, like trying to escalate privileges or reach out to external IP's. I'd check for lateral movement too.

Method 4: SIEM Logs (Splunk or QRadar)

Our SIEM would give us a full view of login patterns, failed access attempts, or strange traffic spikes. It's also where I'd set up rules for alerting if certain IOC's pop up (like a known bad IP or file hash).

Method 5: DNS and Network Traffic Monitoring

I'd watch outbound connections closely. If I see traffic going to an unfamiliar domain or a high volume of DNS lookups to external sites, that's a red flag, especially it it's coming from a user who clicked a phishing link.

Method 6: User Behavior Analytics (UBA)

If we had UBA in place, I'd check for odd access times, impossible travel logins, or employees suddenly accessing large amounts of sensitive data they normally wouldn't touch.

Under the NIST Incident Response Framework, solid documentation is everything, not just for tracking the incident but for compliance, future audits, and legal protection. If SecureSync Corp detects malware in their environment, here are four key details I'd make sure to document:

Prompt 3

Using what you know about the NIST framework and this company, list four details to include when documenting detected incidents.

1. What was detected (with timestamps): I'd record exactly what triggered the alert, for example: a phishing email with a malicious attachment or outbound traffic to a known bad IP. Timestamps matter here because they establish a timeline of the event and help trace how far the attack spread.
2. Initial Scope and Impact: How many users or systems were affected? Did the malware hit internal servers or just a single workstation? Documenting the potential impact helps guide containment decisions and support risk assessments later.
3. Detection Method and Tool Used: Whether it was flagged by an EDR tool, SIEM alert or firewall log, I'd specify exactly what system caught it and what rule or trigger fired. This info helps when tuning future alerts and providing due diligence to external auditors.
4. Actions Taken (and When): Every action, from isolating a machine to resetting a password, should be logged with a timestamp and who did it. This creates a reliable paper trail and supports chain of command custody for any future investigation.

Once malware is detected at SecureSync Corp, the goal is to keep the situation from getting worse while preserving evidence and protecting daily operations. Here are two containment strategies I'd recommend.

Prompt 4

Use the following format:

Containment strategy name: A sentence that explains how the strategy will help the company with containment.

List at least two containment strategies and explain how these strategies will help the company with containment.

Endpoint Isolation: Disconnecting infected devices from the network stops the malware from spreading.

Block Malicious Network Traffic: Blocking communication to malicious IP's prevents data exfiltration and cuts off attacker access.

Prompt 5

List the four-steps the company would use to conduct post-incident reviews based on the NIST framework.

List the answers using the following format:

Step 1: Review and validate the incident response actions taken, including how the detection, analysis, containment, and recovery were handled.
Step 2: Identify gaps in procedures, tools, or communication that affected the incident response process.
Step 3: Document lessons learned and update the incident response plant to reflect improvements or adjustments needed.
Step 4 : Share findings with relevant stakeholders and provide updated training to the response team if necessary.

Prompt 6

Using the NIST framework, write a checklist of three tasks an organization can use to structure an approach for updating the response plan based on findings.

Checklist:

Conduct a post incident review meeting with all involved stakeholders. Debriefing as a team helps identify what worked, what didn't and where the response plan needs updates. Everyone's input ensures that blind spots are addressed.

Update documentation to reflect lessons learned. This includes refining the incident response plan, modifying detection and escalation procedures, and adjust communication protocols so future responses are more efficient and aligned.

Test and retrain based on revised procedures. After changes are made, it's important to walk through tabletop exercises or live drills using the updated plan.

This ensures the team understands the revisions and is better prepared going forward.

Prompt 7

Based on the case study and the NIST framework, list four sources of digital evidence necessary for incident investigation.

Write your answers in a list using the following format:

Source 1: System and application logs from affected endpoints and servers.
Source 2: Network traffic logs, including firewall and intrusion detection/prevention system (IDS/IPS) data.
Source 3: Email headers and message metadata associated with the phishing attempt.
Source 2: File system artifacts such as downloaded payloads or modified executables.

Prompt 8

List the three steps required to assess the collected digital evidence and verify its integrity.

Use the following format:

Step 1: Perform cryptographic hashing (SHA-256) on collected evidence to generate a baseline hash value.
Step 2: Analyze the evidence in a controlled, forensically sound environment to ensure data remains unaltered.
Step 3: recalculate and compare hash values post analysis to confirm the integrity of the evidence was preserved.

2. Validate that you completed all of your answers for prompts 1 - 8.
3. If you did not already renamed your text document to use it later, rename the Part 1 template document as ***Solution document_YourInitials***, and save the document in an accessible location for later use.
4. Begin your work for Part 2.

Part 2: Forensic investigations: Creating an Incident Response Plan

In part 2 of this final project, you will document steps and reasoning for an incident response plan that outlines the steps an organization would follow for any digital forensics investigation.

Your company will use this document as its standardized process and checklist to ensure consistency, thoroughness, and integrity in future investigations. You will divide the plan into four phases, each with specific objectives.

Prompt 9

List the three types of digital evidence that the organization should review as part of a forensic investigation to determine the breach's origin and method. Then explain the purpose for that digital evidence.

Provide your answer using the following format:

Evidence Type 1: Write a sentence that explains the purpose for this digital evidence.
Evidence Type 2: Write a sentence that explains the purpose for this digital evidence.
Evidence Type 3: Write a sentence that explains the purpose for this digital evidence.

Evidence Type 1: Network Traffic Logs

These help identify when and how the attacker access the system, including the specific IP addresses, ports, or protocols used during the breach.

Evidence Type 2: System and application logs

These provide a timeline of user activity and system behavior, which can help pinpoint privilege escalation, suspicious commands, or backdoor installations.

Evidence Type 3: File system metadata artifacts

This includes timestamps and file modification history, which helps determine what files were accessed or altered during the incident.

Prompt 10

Using what you know about digital forensics, list four key components to include in structured reports following each incident and describe each component.

Provide your answer using the following format:

First key component: Executive Summary

I'd start with a clean overview that spells out what went down, a spear phishing email triggered a malware infection, we caught it, and this report outlines how. This section is for execs or legal, jargon free, so it's short and includes the date of detection, impact on operations, and whether customer data was affected.

Second key component: Technical Analysis

This section is where I break it all down: how the phishing email got through, what the malware did once inside, how far it spread, and which systems were hit. I'd include IOC details, logs from our EDR and SIEM, and map our attacker behavior step by step.

Third key component: Timeline of events

Here's where the full play by play goes. I'd build out a detailed, timestamped sequence from the initial alter to final recovery. That includes all response actions: isolating endpoints, blocking malicious IP's, and restoring affected services. It's critical for audits and training the team later.

Fourth key component: Lessons Learned and Recommendations

Finally, I'd wrap with a reflection: What worked, what didn't, and what we're doing next. In SecureSync's case, maybe we revise phishing awareness training or reconfigure EDR rules. This part feeds directly into our continuous improvement cycle for IR.

Congratulations! You've now completed all final project assignments!

2. Validate that you completed all sections.
3. Save your answers into your **Solution document_YourInitials**, and save the document in an accessible location for later final project submission.

Finalize your assignment

Before you submit your assignment, complete these steps:

1. Verify that you provided answers to all tasks.

2. Remember to rename the solution document as described (Project solution document_YourInitials)
3. Remove the instruction sections or examples provided in the Project solution document. Your final deliverables should only contain your work. However, keep the answers that were provided for you.

Submit your answers

1. After you finalize your document, open the **Final Project Submission and Evaluation** assignment.
2. Select the **My Submission** and follow the onscreen instructions to submit your answers.

Evaluating other submissions

Giving, receiving, and incorporating feedback is a crucial professional skill. After you submit your deliverable, your next task is to use the guidance provided within the rubric to review and provide feedback on another peer's submission.

A total of forty-four (44) points are allotted for this final course project. The points are distributed across the answers to the tasks contained in the following solution documents:

Final Project

Incident Response Plan and Digital Forensics Investigation

List the roles and responsibilities of four key team members in the incident response team.

When responding to a security incident, you need a solid team that knows their roles and moves fast. Here are four of the most important positions I'd include on my team and what I'd expect from them:

Role 1: Incident Response Lead (me)

I'd be responsible for coordinating the response from start to finish. That includes documenting everything, assigning tasks, checking with each role, and making sure we're aligned with NIST's phases. I'd also act as the bridge between technical staff and leadership; no nothing gets lost in translation.

Role 2: Communications Liaison

This person dives deep into the system: checking how the malware got in, how far it spread, and what kind of damage it did. They'd also help guide decisions on containment and recovery, especially when systems are critical to operations.

Role 3: Security Analyst

They'd monitor alerts, dig through logs, and help identify indicators of compromise (IOC's). Their job is to stay hands on with the tools we use daily and sport unusual patterns before they turn into something bigger.

List the four methods, or tasks, you can use to monitor this company's internal systems for unusual activity.

When it comes to early detection, monitoring is everything. In this scenario, the attack came through a spear-phishing email, so I'd want to focus on tools that can catch the suspicious behavior across email, endpoint, and network activity.

Here's what I would monitor and how:

Method 1: Email Gateway & Span Filters:

I'd start by reviewing logs from or email security gateway (like Proofpoint or Microsoft Defender). I'd be looking for unusual subject lines, strange attachment types, or links spoofing addresses.

Method 2: Endpoint Detection & Response

Tools like CrowdStrike or SentinelOne would help flag the moment malware starts behaving oddly, like trying to escalate privileges or reach out to external IP's. I'd check for lateral movement too.

Method 4: SIEM Logs (Splunk or QRadar)

Our SIEM would give us a full view of login patterns, failed access attempts, or strange traffic spikes. It's also where I'd set up rules for alerting if certain IOC's pop up (like a known bad IP or file hash).

Method 5: DNS and Network Traffic Monitoring

I'd watch outbound connections closely. If I see traffic going to an unfamiliar domain or a high volume of DNS lookups to external sites, that's a red flag, especially it it's coming from a user who clicked a phishing link.

Method 6: User Behavior Analytics (UBA)

If we had UBA in place, I'd check for odd access times, impossible travel logins, or employees suddenly accessing large amounts of sensitive data they normally wouldn't touch.

Using what you know about the NIST framework and this company, list four details to include when documenting detected incidents.

Under the NIST Incident Response Framework, solid documentation is everything, not just for tracking the incident but for compliance, future audits, and legal protection. If SecureSync Corp detects malware in their environment, here are four key details I'd make sure to document:

What was detected (with timestamps): I'd record exactly what triggered the alert, for example: a phishing email with a malicious attachment or outbound traffic to a known bad IP. Timestamps matter here because they establish a timeline of the event and help trace how far the attack spread.

Initial Scope and Impact: How many users or systems were affected? Did the malware hit internal servers or just a single workstation? Documenting the potential impact helps guide containment decisions and support risk assessments later.

Detection Method and Tool Used: Whether it was flagged by an EDR tool, SIEM alert or firewall log, I'd specify exactly what system caught it and what rule or trigger fired. This info helps when tuning future alerts and providing due diligence to external auditors.

Actions Taken (and When): Every action, from isolating a machine to resetting a password, should be logged with a timestamp and who did it. This creates a reliable paper trail and supports chain of command custody for any future investigation.

Once malware is detected at SecureSync Corp, the goal is to keep the situation from getting worse while preserving evidence and protecting daily operations. Here are two containment strategies I'd recommend.

List at least two containment strategies and explain how these strategies will help the company with containment.

Endpoint Isolation: Disconnecting infected devices from the network stops the malware from spreading.

Block Malicious Network Traffic: Blocking communication to malicious IP's prevents data exfiltration and cuts off attacker access.

List the four-steps the company would use to conduct post-incident reviews based on the NIST framework.

Step 1: Review and validate the incident response actions taken, including how the detection, analysis, containment, and recovery were handled.
Step 2: Identify gaps in procedures, tools, or communication that affected the incident response process.
Step 3: Document lessons learned and update the incident response plant to reflect improvements or adjustments needed.
Step 4 : Share findings with relevant stakeholders and provide updated training to the response team if necessary.

Using the NIST framework, write a checklist of three tasks an organization can use to structure an approach for updating the response plan based on findings.

Checklist:

Conduct a post incident review meeting with all involved stakeholders. Debriefing as a team helps identify what worked, what didn't and where the response plan needs updates. Everyone's input ensures that blind spots are addressed.

Update documentation to reflect lessons learned. This includes refining the incident response plan, modifying detection and escalation procedures, and adjust communication protocols so future responses are more efficient and aligned.

Test and retrain based on revised procedures. After changes are made, it's important to walk through tabletop exercises or live drills using the updated plan. This ensures the team understands the revisions and is better prepared going forward.

Based on the case study and the NIST framework, list four sources of digital evidence necessary for incident investigation.

Source 1: System and application logs from affected endpoints and servers.
Source 2: Network traffic logs, including firewall and intrusion detection/prevention system (IDS/IPS) data.
Source 3: Email headers and message metadata associated with the phishing attempt.
Source 4: File system artifacts such as downloaded payloads or modified executables.

List the three steps required to assess the collected digital evidence and verify its integrity.

Step 1: Perform cryptographic hashing (SHA-256) on collected evidence to generate a baseline hash value.
Step 2: Analyze the evidence in a controlled, forensically sound environment to

ensure data remains unaltered.
Step 3: recalculate and compare hash values post analysis to confirm the integrity of the evidence was preserved.

Part 2: Forensic investigations: Creating an Incident Response Plan

Your company will use this document as its standardized process and checklist to ensure consistency, thoroughness, and integrity in future investigations. You will divide the plan into four phases, each with specific objectives.

List the three types of digital evidence that the organization should review as part of a forensic investigation to determine the breach's origin and method. Then explain the purpose for that digital evidence.

Evidence Type 1: Network Traffic Logs

These help identify when and how the attacker access the system, including the specific IP addresses, ports, or protocols used during the breach.

Evidence Type 2: System and application logs

These provide a timeline of user activity and system behavior, which can help pinpoint privilege escalation, suspicious commands, or backdoor installations.

Evidence Type 3: File system metadata artifacts

This includes timestamps and file modification history, which helps determine what files were accessed or altered during the incident.

Using what you know about digital forensics, list four key components to include in structured reports following each incident and describe each component.

First key component: Executive Summary

I'd start with a clean overview that spells out what went down, a spear phishing email triggered a malware infection, we caught it, and this report outlines how. This section is for execs or legal, jargon free, so it's short and includes the date of detection, impact on operations, and whether customer data was affected.

Second key component: Technical Analysis

This section is where I break it all down: how the phishing email got through, what the malware did once inside, how far it spread, and which systems were hit. I'd include IOC details, logs from our EDR and SIEM, and map our attacker behavior step by step.

Third key component: Timeline of events

Here's where the full play by play goes. I'd build out a detailed, timestamped sequence from the initial alter to final recovery. That includes all response actions: isolating endpoints, blocking malicious IP's, and restoring affected services. It's critical for audits and training the team later.

Fourth key component: Lessons Learned and Recommendations

Finally, I'd wrap with a reflection: What worked, what didn't, and what we're doing next. In SecureSync's case, maybe we revise phishing awareness training or reconfigure EDR rules. This part feeds directly into our continuous improvement cycle for IR.