

MODULO 01

Fondamenti di Incident Response

Il ciclo di vita dell'incidente come processo strutturato e ripetibile: modelli NIST e SANS, organizzazione di SOC, CSIRT e CERT, playbook e runbook.

NIST SP 800-61r3

SANS PICERL

ISO/IEC 27035

Una traccia core e tre specializzazioni



Abstract e obiettivi formativi

Abstract

Il modulo introduce la risposta agli incidenti come processo strutturato e ripetibile. Si presentano i modelli di riferimento NIST SP 800-61r3 e SANS (ciclo PICERL), l'organizzazione di SOC, CSIRT e CERT e la funzione di playbook e runbook, fino agli obblighi di notifica previsti da GDPR e NIS2.

Obiettivi formativi (Bloom)

- **Comprendere:** descrivere le fasi del ciclo di vita di un incidente
- **Applicare:** classificare un evento per severità e categoria
- **Creare:** progettare un playbook per uno scenario assegnato

Traccia core

01

02

07

Detection & Response

03

04

05

06

o

Digital Forensics

08

09

10

11

o

Sicurezza dell'AI

06

12

13

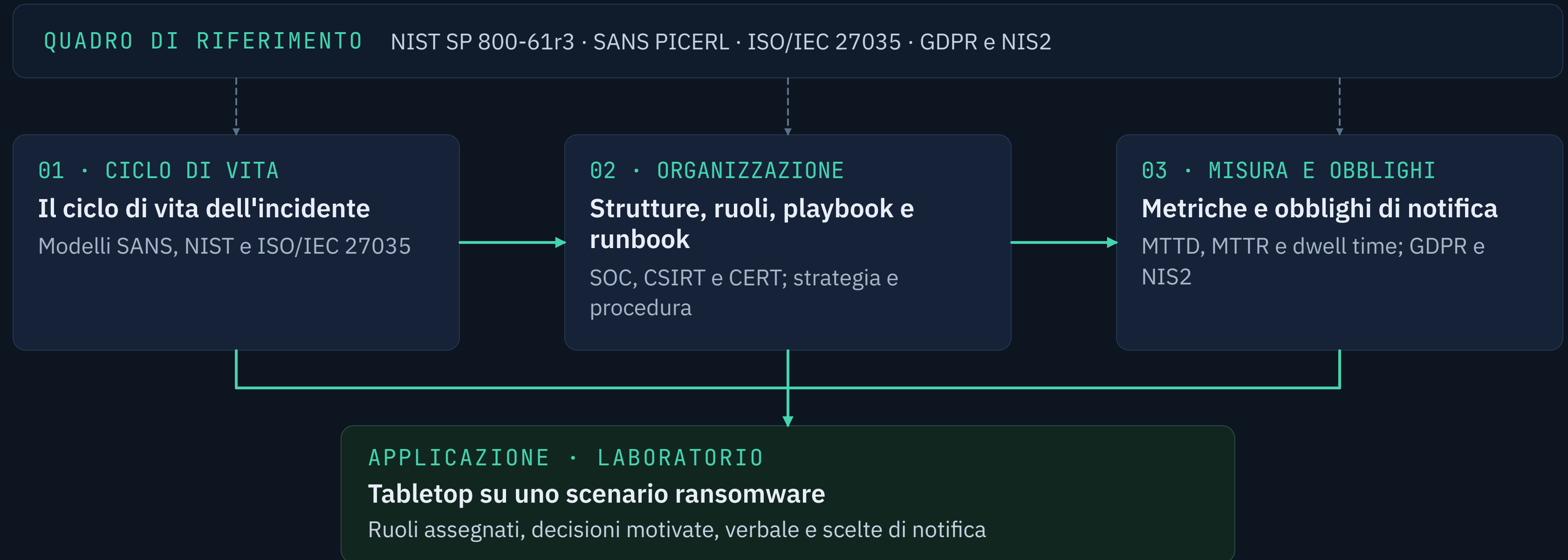
14

Traccia core

15

16

Come si organizza e si misura la risposta



Il ciclo di vita dell'incidente

P-01

Preparazione

Policy, strumenti,
formazione,
playbook

I-02

Identificazione

Detection, triage,
dichiarazione

C-03

Contenimento

Limitare il danno,
preservare le
evidenze

E-04

Eradicazione

Rimozione della
causa e degli
accessi

R-05

Ripristino

Ritorno in esercizio,
monitoraggio

L-06

Lezioni apprese

Post-incident
review,
miglioramento

Le sei fasi sono quelle del modello SANS. NIST SP 800-61r2 le raggruppava in quattro; la revisione 3 (2025) adotta un modello basato sulle sei funzioni del NIST CSF 2.0. In entrambi i modelli il contenimento precede l'eradicazione e le lezioni apprese aggiornano la preparazione.

Strutture, ruoli, playbook e runbook

Le strutture

- **SOC:** monitoraggio continuo e prima linea di detection
- **CSIRT:** squadra di risposta che coordina la gestione dell'incidente
- **CERT:** denominazione storica dei CSIRT e marchio della Carnegie Mellon University, usata spesso da strutture nazionali o settoriali
- Escalation e comunicazione di crisi definite in anticipo

Playbook e runbook

- **Playbook:** strategia di risposta per categoria di incidente, con decisioni e responsabilità
- **Runbook:** procedura operativa passo per passo, eseguibile e automatizzabile
- Entrambi versionati, verificati nelle esercitazioni tabletop e aggiornati dopo ogni incidente

Metriche di risposta e obblighi di notifica

MTTD

Tempo medio di rilevamento dell'incidente

MTTR

Tempo medio di risposta, ripristino o rimedio, secondo la definizione adottata

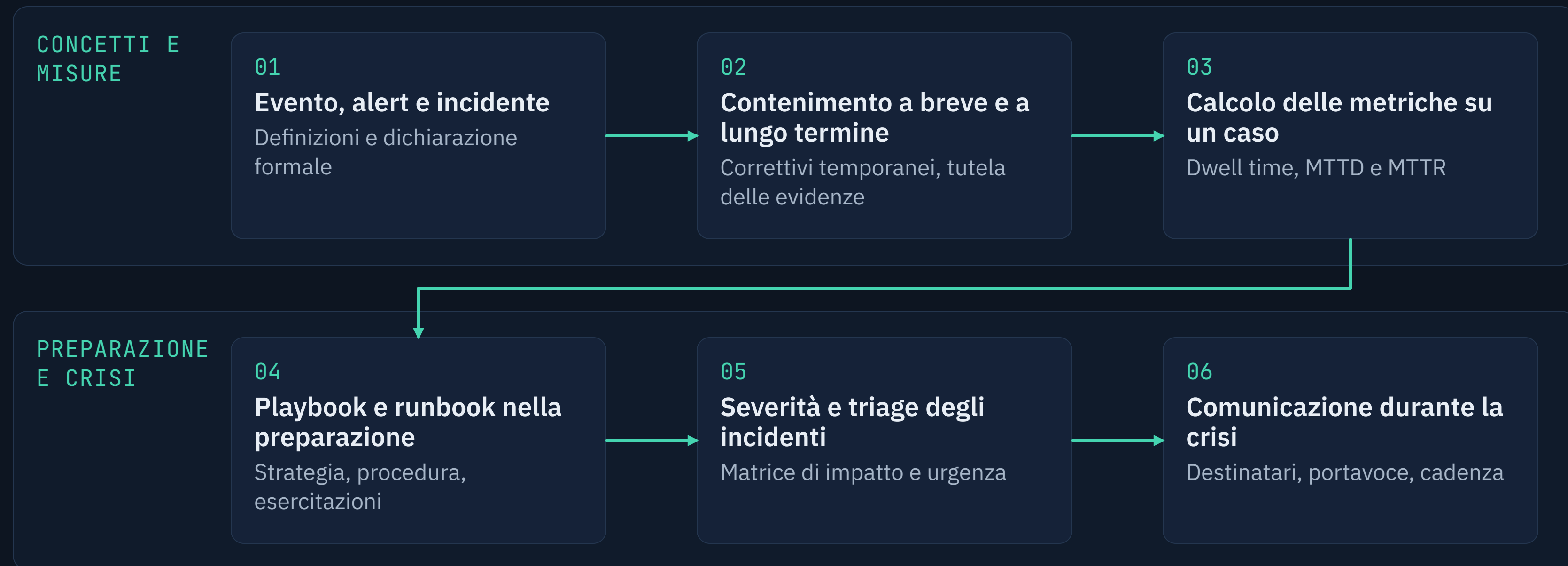
DWELL

Permanenza dell'attaccante prima della scoperta; mediana globale 2025: 14 giorni

Obblighi di notifica

- **GDPR, artt. 33–34**: notifica al Garante senza ingiustificato ritardo e, ove possibile, entro 72 ore dalla conoscenza della violazione, salvo rischio improbabile; comunicazione agli interessati se il rischio è elevato
- **NIS2** (art. 25): incidenti significativi; al CSIRT Italia pre-notifica entro 24 ore e notifica entro 72 ore dalla conoscenza, relazione finale entro un mese dalla notifica

Nozioni operative per gestire un incidente



Evento, alert e incidente

Un **evento** è qualunque occorrenza osservabile in un sistema o in una rete, come un accesso o una connessione. Un **alert** è un evento che una regola o un modello segnala come potenzialmente rilevante. Un *incidente*, nella definizione NIST, è un'occorrenza che, senza autorizzazione legittima, mette in pericolo in modo effettivo o imminente integrità, riservatezza o disponibilità di informazioni o sistemi, oppure viola o minaccia di violare leggi, policy o procedure di sicurezza. La dichiarazione di incidente è un atto formale che attiva il CSIRT, la valutazione degli obblighi di notifica e la conservazione delle evidenze; i termini di notifica decorrono però dalla conoscenza del fatto.

Scenario didattico

Diecimila accessi falliti in un'ora su un portale esposto, distribuiti su molti account con poche password comuni, sono diecimila eventi e generano un alert di password spraying. Si ha un incidente quando uno degli accessi riesce; se l'account è amministrativo, la severità aumenta.

Metodo

Severità e categoria assegnate al momento della dichiarazione determinano escalation e risorse e orientano la verifica degli obblighi di notifica, i cui presupposti sono fissati dalle norme.

Contenimento a breve e a lungo termine

Il contenimento a **breve termine** limita subito il danno con azioni rapide e reversibili: isolamento degli host, blocco degli account, segmentazione d'emergenza. Le azioni vanno scelte in modo da preservare le evidenze; un host la cui memoria serve all'indagine non va spento prima dell'acquisizione. Il contenimento a **lungo termine** mantiene in esercizio i sistemi mentre si prepara l'eradicazione e si ricostruiscono in parallelo sistemi puliti: si applicano correttivi temporanei come la rimozione di account e backdoor dell'attaccante e le patch, si ruotano le credenziali e si rafforza il monitoraggio.

Scenario didattico

In un attacco ransomware, nel breve termine si isolano i segmenti colpiti e si sospendono le condivisioni di rete, lasciando accesi gli host necessari all'acquisizione della memoria. Nel lungo termine si applicano correttivi temporanei ai sistemi che devono restare in esercizio e si ricostruisce un'infrastruttura pulita; il ritorno dei servizi da backup verificati appartiene alla fase di ripristino.

Cautele

Un contenimento precoce limita il danno ma può avvisare l'attaccante e alterare le evidenze. Un'osservazione più lunga arricchisce l'indagine al prezzo di un impatto più esteso. La scelta va motivata e registrata, perché sarà esaminata nella revisione post-incidente e, se necessario, in sede giudiziaria.

Calcolo delle metriche su un caso

Scenario didattico: un attaccante accede lunedì alle 09:00 tramite phishing e l'alert UEBA scatta mercoledì alle 15:00. Il CSIRT dichiara l'incidente alle 16:30 e completa contenimento e ripristino venerdì alle 12:00. Il **dwell time**, dall'accesso alla scoperta, è di 54 ore; dalla dichiarazione al ripristino trascorrono 43,5 ore. **MTTD e MTTR** sono medie calcolate sull'insieme degli incidenti di un periodo e non sul singolo caso, con un valore che dipende da come la definizione fissa gli istanti di inizio e di fine.

Metodo

Le metriche servono a confrontare il processo con sé stesso nel tempo e a dimensionare gli investimenti, per esempio a verificare se l'introduzione del triage assistito dall'AI riduce l'MTTD, come avviene nel project work del Modulo 16.

Limiti

Quando diventano obiettivi individuali, le metriche inducono i comportamenti opportunistici descritti dalla legge di Goodhart, come la chiusura prematura dei ticket o il declassamento di incidenti a eventi.

Playbook e runbook nella preparazione

Il **playbook** fissa la strategia di risposta a una classe di incidenti, per esempio phishing, ransomware o compromissione di account, e ne indica fasi, decisioni, responsabili, soglie di escalation e il momento in cui coinvolgere la funzione legale e la comunicazione. Il **runbook** descrive la sequenza operativa che l'analista esegue: comandi di isolamento, strumenti di acquisizione, moduli di verbalizzazione. Il playbook si rivede quando cambiano l'organizzazione o le norme, mentre il runbook segue l'evoluzione della tecnologia. Entrambi si redigono prima dell'incidente, si verificano con esercitazioni tabletop e si gestiscono sotto controllo di versione.

Scenario didattico

Il playbook ransomware di un'organizzazione assegna all'incident commander la scelta tra spegnimento e isolamento degli host, secondo i criteri del Modulo 7. Il runbook collegato elenca i comandi di isolamento per EDR, switch e ambienti cloud. Durante un'esercitazione emerge che manca la procedura per il segmento OT, e la correzione riguarda il runbook.

Ruolo dell'AI

Playbook scritti con precisione sono il presupposto dell'automazione trattata nei Moduli 5 e 6, perché un playbook ambiguo, una volta automatizzato, produce decisioni incoerenti su larga scala. Un LLM può proporre bozze e segnalare disallineamenti tra runbook e documentazione tecnica.

Severità e triage degli incidenti

La severità di un incidente combina l'**impatto** su dati, servizi, persone e obblighi normativi con l'**urgenza**, legata a un attacco in corso o a una propagazione in atto. Una matrice di impatto e urgenza, definita nel playbook, stabilisce priorità, tempi di presa in carico e catena di reperibilità. La classificazione iniziale è provvisoria: quando l'indagine chiarisce l'estensione, un phishing isolato può rivelarsi una compromissione del dominio. Il processo indica quindi chi rivaluta la severità, in quali momenti e con quale registrazione della decisione.

Scenario didattico

Alle 02:10 scatta un alert su un account di servizio con accesso al gestionale: impatto potenziale alto, nessuna attività in corso. Il caso è classificato di severità 3 e messo in coda. Alle 02:40 lo stesso account crea un utente amministrativo: l'urgenza diventa massima, la severità sale a 1 e si attiva la reperibilità.

Ruolo dell'AI

I modelli di scoring del Modulo 3 propongono una priorità, ma il riferimento resta la matrice scritta. Se il modello assegna severità 3 a un caso che la matrice classifica di severità 1, prevale la matrice e la discrepanza viene registrata come possibile errore del modello.

Comunicazione durante la crisi

Ogni incidente grave procede su due linee parallele, quella tecnica e quella della comunicazione. Gli interlocutori hanno esigenze diverse: il vertice aziendale chiede impatto e decisioni da prendere, i gruppi tecnici dettagli operativi, la funzione legale il controllo delle ammissioni e dell'uso del termine «violazione», le autorità i contenuti e i termini fissati dalle norme (Modulo 15), i dipendenti istruzioni semplici. Le prassi più diffuse prevedono un solo portavoce autorizzato per canale, aggiornamenti a cadenza fissa anche in assenza di novità e l'attenzione a non scrivere, nemmeno nelle chat interne, ipotesi non verificate o ammissioni che sarebbero pregiudizievoli se acquisite in un procedimento.

Scenario didattico

Ransomware rilevato il venerdì sera. Alle 21:00 il vertice riceve una nota di mezza pagina con i fatti accertati, l'impatto e il prossimo aggiornamento fissato alle 23:00, i dipendenti un messaggio con l'istruzione di non accendere i portatili; i dettagli tecnici restano interni finché l'estensione non è accertata. Il titolare, con il supporto del DPO, avvia la valutazione prevista dall'art. 33 GDPR.

Ruolo dell'AI

Un LLM può preparare rapidamente versioni dello stesso aggiornamento per destinatari diversi. Ogni testo diretto all'esterno o alle autorità passa dalla revisione umana e legale, perché un'informazione errata in una notifica resta agli atti dell'autorità e può esporre l'organizzazione a contestazioni.

Tabletop su uno scenario ransomware

Svolgimento

1. Assegnazione dei ruoli: responsabile della gestione, analisti, comunicazione, funzione legale
2. Iniezione progressiva degli eventi dello scenario da parte del docente
3. Applicazione del ciclo PICERL con decisioni motivate e tracciate
4. Redazione del verbale d'incidente e debriefing finale

Consegna

- Verbale d'incidente del gruppo
- Decisioni di notifica motivate (GDPR / NIS2)
- Una lezione appresa per ruolo

Lecture e autovalutazione

Lecture obbligatorie

- NIST SP 800-61r3 (2025), *Incident Response Recommendations and Considerations for Cybersecurity Risk Management*
- P. Kral, *Incident Handler's Handbook*, SANS Institute (2012)
- ENISA, *Good Practice Guide for Incident Management*

Domande di autovalutazione

1. Quali criteri distinguono un evento da un incidente?
2. Perché il contenimento precede l'eradicazione?
3. Quali metriche misurano l'efficacia di un CSIRT?
4. Quando scatta l'obbligo di notifica ex art. 33 GDPR?
5. Che differenza c'è tra playbook e runbook?

FINE DELLA LEZIONE • MODULO 01

Grazie

Fondamenti di Incident Response • Corso «Incident Response potenziata dall'AI»

Domande e materiali: ricevimento del docente. Profilo e contatti:
vincenzocalabro.it



Vincenzo Calabrò

CYBER SECURITY • DIGITAL FORENSICS



VINCENZOCALABRO.IT