MODULO 16

Project work finale

Simulazione di un'intrusione in più fasi in un'azienda fittizia: risposta e indagine forense, con e senza supporto dell'AI, e confronto delle metriche MTTD e MTTR.

TABLETOP + LAB

40% DEL VOTO

RELAZIONE FORENSE

Corso magistrale · Cyber Security · Digital Forensics & Incident Response

SCHEDA DEL MODULO

Abstract e obiettivi formativi

Abstract

Il modulo conclusivo integra l'intero percorso in una simulazione completa d'incidente: i gruppi conducono detection, risposta e indagine forense su un'intrusione multi-stadio con log realistici; metà dei gruppi opera con strumenti AI e metà senza, per confrontare MTTD e MTTR, con valore indicativo.

Obiettivi formativi (Bloom)

- **Creare**: integrare metodologia IR, strumenti AI e vincoli giuridici in un caso realistico
- **Valutare**: misurare e discutere MTTD/MTTR con e senza supporto AI
- **Creare**: produrre una relazione forense completa e difendibile e condurre la revisione delle lezioni apprese

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

SCHEMA · TEORIA

Organizzazione del project work

SVOLGIMENTO · TRE FASI

Svolgimento della simulazione

FASE 1 · TABLETOP

Gruppi misti, con un filone d'indagine per specializzazione. Ricezione dello scenario, assegnazione dei ruoli di incident commander, comunicazione, legale e scriba, pianificazione della risposta nel rispetto della policy AI

FASE 2 · LABORATORIO

Indagine su log SIEM, dump di memoria e traffico predisposti. Metà dei gruppi con strumenti AI (copilota su modello locale, triage basato su modelli), metà senza; Timesketch con i suoi analyzer per tutti. Mappatura ATT&CK e contenimenti motivati

FASE 3 · RESTITUZIONE

Confronto delle metriche tra gruppi, presentazione delle relazioni, lezioni apprese e revisione tra pari

Le metriche raccolte nella fase 2 (MTTD, MTTR, tecniche individuate, errori) alimentano nella fase 3 il confronto tra gruppi con e senza AI, che costituisce la parte sperimentale del corso.

SVOLGIMENTO · CONSEGNE

Consegne del gruppo

Relazione forense

Cronologia dell'attacco su ATT&CK, evidenze con catena di custodia, raccomandazioni, una sezione metodologica che dichiara l'eventuale uso dell'AI e un allegato per filone

Executive summary

Una pagina per il vertice: cosa è successo, impatto, cosa è stato fatto, cosa resta da fare. Linguaggio non tecnico

Registro delle decisioni

Ogni decisione con timestamp, motivazione e punto di approvazione umana; le notifiche GDPR/NIS2 valutate e motivate

Le consegne corrispondono ai destinatari tipici della documentazione di un incidente, cioè il perito, il vertice aziendale e l'autorità, e la capacità di scrivere per ciascuno fa parte della valutazione.

VALUTAZIONE · CRITERI E PESI

Rubrica di valutazione del project work

Criterio	Peso	Cosa osserva
Correttezza tecnica dell'indagine	30%	Kill chain ricostruita, evidenze corrette; punteggio per filone
Rigore metodologico e catena di custodia	25%	Processo del Modulo 7 rispettato
Uso critico e documentato dell'AI	20%	Dichiarato, verificato, con errori riconosciuti
Qualità di relazione ed executive summary	15%	Chiarezza, completezza, destinatario giusto
Lavoro di gruppo e gestione dei ruoli	10%	Ruoli esercitati, decisioni tracciate

Per ciascun criterio sono previsti quattro livelli (insufficiente, sufficiente, buono, eccellente), con descrittori espliciti consegnati agli studenti prima della simulazione. Il project work vale il 40% del voto finale; il resto è dato da prova scritta (30%), laboratori (20%) e partecipazione ai casi di studio (10%). La prova scritta ha una parte comune e una sulla specializzazione.

FASE 3 · LEZIONI APPRESE

Lezioni apprese e discussione finale

Sui risultati

- Rapidità dei gruppi con AI e casi in cui sono stati fuorviati
- Evidenze che hanno determinato la ricostruzione della kill chain
- Proporzionalità e reversibilità delle azioni di contenimento

Sul processo

- Tenuta della relazione in un contraddittorio tecnico
- Policy AI come vincolo utile o come ostacolo, con le ragioni
- Lacune del processo e modifiche da apportare alla preparazione

SCHEMA · APPROFONDIMENTI

Indicazioni pratiche per i gruppi

APPROFONDIMENTO 1

Struttura dello scenario della simulazione

La gestione di un incidente richiede insieme, sotto pressione e con informazioni incomplete, le competenze esercitate separatamente nella traccia core e nelle specializzazioni. Lo scenario del project work è un'intrusione con ransomware ed esfiltrazione di dati in un'azienda fittizia, costruito come esercitazione a **inject**: il quadro emerge progressivamente dalle evidenze, come alert, dump di memoria, log di rete e timeline, e da eventi introdotti durante lo svolgimento, tra cui una richiesta della funzione legale e una domanda della stampa. Ogni gruppo opera con i ruoli del Modulo 1; i gruppi della condizione con AI decidono anche quando usarla e quando evitarla, e la scelta è oggetto di valutazione.

Metodo

Ogni inject richiede la competenza di uno o due moduli, e riconoscerla orienta la risposta: il dump di memoria rimanda al Modulo 9, la richiesta di valutare la notifica ai sensi dell'art. 33 GDPR al Modulo 15, il messaggio attribuito al vertice aziendale, che chiede di riattivare i sistemi, al Modulo 12, l'istruzione nascosta in un ticket, eseguita dall'assistente AI interno, ai Moduli 13 e 14.

Errori frequenti

Concentrarsi sull'analisi tecnica trascurando il processo: registro delle decisioni assente, catena di custodia improvvisata, comunicazione rinviata. Nella rubrica il rigore metodologico (25%) ha un peso vicino a quello della correttezza tecnica (30%), perché chi esamina un rapporto dall'esterno ne verifica anche il processo.

APPROFONDIMENTO 2

Struttura del rapporto di incidente

Il rapporto resta agli atti dopo l'incidente e lo leggeranno vertice aziendale, funzione legale, assicurazione e, in alcuni casi, l'autorità giudiziaria. Si apre con un **executive summary** di una pagina in linguaggio non tecnico, che riporta fatti, impatto, stato e decisioni richieste, seguito da una timeline ricostruita con la fonte di ogni evento e da un'analisi tecnica con evidenze citate e riproducibili, cioè hash e riferimenti agli allegati. Completano la struttura le azioni intraprese, collegate al registro delle decisioni, e raccomandazioni ordinate per priorità e costo. Ogni affermazione deve poter essere ricondotta a un'evidenza, secondo lo standard della relazione tecnica forense del Modulo 7.

Ruolo dell'AI

L'uso dell'AI è ammesso e va dichiarato: strumenti, passaggi in cui sono stati impiegati, modelli e versioni, controlli umani effettuati. La completezza dell'appendice metodologica è valutata positivamente, e un IoC prodotto dal modello e non verificato (Modulo 6) è un errore grave.

Metodo

L'executive summary si verifica facendolo leggere a una persona estranea al gruppo: al termine della lettura deve saper dire che cosa è accaduto, quanto è grave e che cosa va deciso. Se servono spiegazioni sui termini, il testo va riscritto.

APPROFONDIMENTO 3

Discussione orale del project work

La discussione finale è impostata come un **controesame tecnico**, sul modello delle domande in udienza del Modulo 8, e verifica la capacità di sostenere ciò che è scritto nel rapporto. Le domande tipiche riguardano la scelta di contenere un host e non un altro, l'evidenza su cui poggia una conclusione e la sua tenuta se contestata, il modo in cui è stato verificato l'output di un LLM, la decisione che il gruppo prenderebbe oggi con le informazioni acquisite in seguito. Una risposta solida espone la catena tra evidenza, ragionamento e decisione, insieme ai limiti e a ciò che non si poteva sapere al momento.

Metodo

Il rapporto va riletto dal punto di vista di un consulente di controparte: ogni affermazione priva di un'evidenza o di un riferimento va corretta prima della discussione. Il registro delle decisioni tenuto durante lo scenario documenta, con data e ora, le ragioni di ogni scelta. Ogni studente risponde a una domanda sul filone della propria specializzazione e a una su un filone di un'altra.

Errori frequenti

Difendere a oltranza una conclusione debole senza riconoscerne e analizzarne i limiti. Un altro errore è attribuire all'AI una conclusione del gruppo, la cui responsabilità resta di chi firma il rapporto.

APPROFONDIMENTO 4

Ruoli e coordinamento del gruppo

Il project work valuta anche il funzionamento del gruppo. Ai ruoli del Modulo 1, da assegnare e rispettare, si aggiunge quello di **scriba**. L'**incident commander** decide e protegge il gruppo dalle interruzioni, coordinando l'analisi senza svolgerla, mentre gli analisti seguono filoni paralleli, uno per specializzazione, e chi cura la comunicazione prepara gli aggiornamenti. Lo scriba registra decisioni e orari e tiene il registro su cui si basano il rapporto (approfondimento 2) e la discussione (approfondimento 3). Il coordinamento si basa su brevi punti di sincronizzazione a cadenza fissa, in cui ogni filone riassume che cosa ha trovato, che cosa sta facendo e che cosa gli serve.

Scenario didattico

Nel gruppo A tutti lavorano sul dump di memoria, nessuno registra le decisioni e l'incident commander analizza invece di coordinare. I risultati si duplicano, la timeline resta incompleta e, quando arriva la richiesta della stampa, nessun aggiornamento è pronto. Il gruppo B, con le stesse competenze tecniche, produce un rapporto coerente grazie a ruoli chiari, sincronizzazioni regolari e uno scriba attivo.

Errori frequenti

L'incident commander che si dedica all'analisi lascia scoperto il coordinamento quando la visione d'insieme è più necessaria, per esempio quando arrivano insieme un nuovo indicatore e una richiesta esterna.

APPROFONDIMENTO 5

Uso dichiarato e verificato dell'AI

Nel project work l'AI è ammessa se il suo uso è dichiarato e verificato. La **dichiarazione** è un'appendice metodologica che indica quali strumenti sono stati usati, in quali passaggi, con quali modelli e versioni e con quali controlli umani. La **verifica** richiede che ogni output dell'AI entrato nel rapporto sia stato riscontrato sul dato originale, per esempio cercando nei log l'IoC indicato da un riassunto, confrontando la timeline ricostruita con le fonti, validando con l'analisi dinamica il comportamento di un comando spiegato da un LLM. La valutazione considera l'uso consapevole: impiegare l'AI dove accelera il lavoro, come sintesi, bozze e query, e tenerla fuori dai verdetti e dalle decisioni di contenimento.

Scenario didattico

Un gruppo usa l'LLM per la bozza dell'executive summary e per spiegare uno script offuscato, verifica entrambi i risultati e lo dichiara nell'appendice. Un altro gruppo inserisce l'output del modello come analisi definitiva, compresi IoC inesistenti, e sul criterio dell'uso dell'AI ottiene una valutazione inferiore.

Cautele

I dati dello scenario sono trattati come evidenze d'indagine e valgono le regole del Modulo 6, il cui rispetto rientra nella valutazione: nessun dato riservato verso servizi esterni non autorizzati, modello locale per i contenuti sensibili.

APPROFONDIMENTO 6

Revisione post-incidente e miglioramento

Un incidente si conclude con le **lezioni apprese**, che la SP 800-61 Rev. 2 del NIST indicava come la parte della risposta omessa più spesso. La revisione post-incidente condotta senza ricerca del colpevole (blameless) individua le cause sistemiche e produce azioni con responsabile e scadenza. Esamina come è avvenuto l'accesso iniziale e come si chiude, quale controllo è mancato, quale detection va aggiunta secondo il ciclo descritto nel Modulo 3 e quali pratiche hanno funzionato e vanno consolidate. La revisione alimenta anche il miglioramento dei sistemi AI difensivi, perché ogni caso entra nel golden set (Modulo 14) e gli errori di un copilota diventano test di regressione.

Metodo

La consegna del project work comprende una breve revisione: tre cause sistemiche, tre azioni con responsabile e scadenza, una nuova regola di detection derivata dall'episodio.

Ruolo dell'AI

Gli strumenti AI accelerano la stesura della timeline e la ricerca di casi simili nello storico; le cause sistemiche si individuano nel confronto tra i ruoli coinvolti. Gli errori dei sistemi AI emersi durante l'incidente vanno registrati come casi di test.

CHIUSURA DEL CORSO

Sintesi del corso

METODO

Il ciclo di risposta e il processo forense, applicabili con qualunque insieme di strumenti

VERIFICA

L'output dell'AI si verifica con misure esplicite (groundedness, recall) e con l'audit trail

RESPONSABILITÀ

Per ogni azione automatizzata sono definiti un responsabile e un punto di approvazione umana, con traccia nel registro delle decisioni (Moduli 5 e 15)

Dopo il corso

La prova scritta si svolge nella sessione d'esame e il ricevimento è disponibile per la revisione delle relazioni. Sono previste proposte di tesi su AI forensics, detection engineering e governance dei sistemi AI.

FINE DELLA LEZIONE · MODULO 16

Grazie

Project work finale · 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