

MODULO S1.2 • AGOSTO 2026

Incident Response e Intrusioni su Host

Dal primo allarme alla ricostruzione dell'intrusione:
log, persistenza, movimento laterale e ransomware

`hayabusa csv-timeline -d ./evtx • velociraptor • vol.py windows.malfind`

Corso di Laurea Magistrale in Sicurezza Informatica

Al termine del modulo lo studente sarà in grado di

01 • RICOSTRUIRE

Un'intrusione su un host Windows combinando memoria, disco ed event log in una timeline unica e verificabile

02 • RICONOSCERE

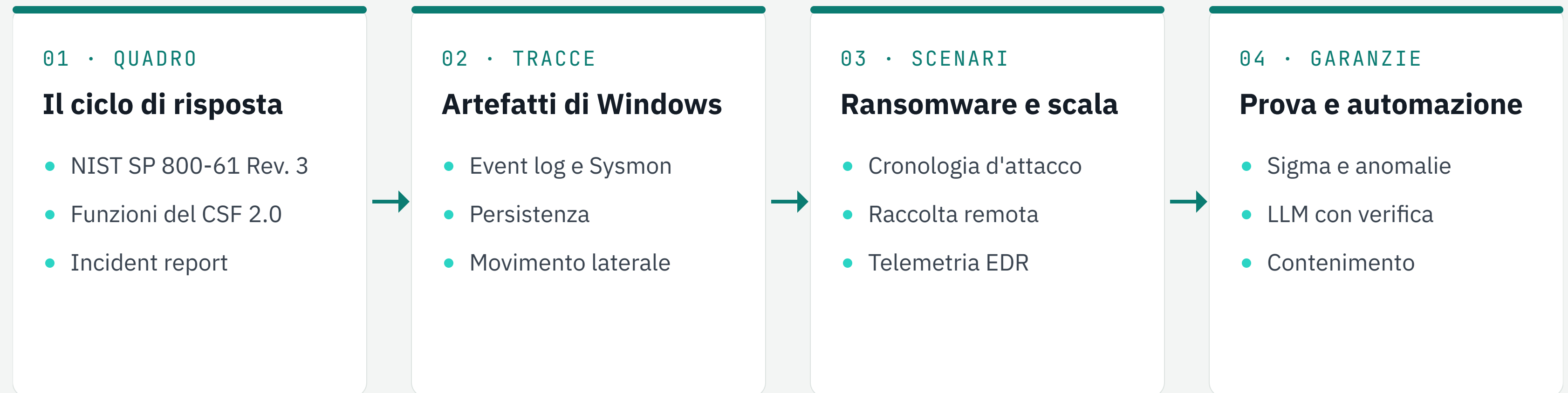
Persistenza e movimento laterale negli artefatti di Windows, datandoli e collegandoli agli account usati

03 • CONDURRE

La risposta all'incidente preservando la prova, documentando ogni azione di contenimento come operazione sul reperto

Prerequisiti. Il modulo presuppone la memory forensics di M4 e i moduli core M1-M3 e M7-M8: acquisizione, artefatti del file system, lettura critica delle metriche e protocollo di validazione su campione.

Dalla segnalazione alla ricostruzione dell'intrusione



Le quattro aree si susseguono nelle slide del modulo nello stesso ordine dello schema: ciascuna presuppone la precedente.

La forensics dentro il ciclo di risposta

La revisione 3 della guida **NIST SP 800-61**, pubblicata nell'aprile 2025, lascia il ciclo in quattro fasi delle edizioni precedenti e organizza la risposta attorno alle sei funzioni del **Cybersecurity Framework 2.0**: Govern, Identify, Protect, Detect, Respond, Recover. La risposta entra così nella gestione del rischio e comincia prima dell'allarme, con procedure e contatti già pronti.

La forensics attraversa più funzioni: conferma l'allarme in Detect, fornisce le evidenze per contenere in Respond, verifica in Recover che il ripristino non riporti in esercizio la compromissione. L'**incident report** serve a decidere in fretta; la **relazione peritale** si rivolge al giudice e richiede metodo dichiarato e catena di custodia.

Le due finalità convivono nello stesso incidente: conviene impostare la raccolta fin dall'inizio come se l'esito dovesse arrivare in aula.

ESEMPIO • DUE DOCUMENTI, UN INCIDENTE

Un'azienda subisce un accesso abusivo al gestionale. Il team interno chiude l'incidente in due giorni con un report di tre pagine: causa, sistemi coinvolti, correttivi.

Sei mesi dopo l'azienda presenta denuncia. Il consulente scopre che le evidenze citate nel report non hanno hash né orari di acquisizione: le conclusioni restano plausibili, ma vanno ricostruite su ciò che è sopravvissuto nei sistemi.

Gli event log di Windows come prova

Autenticazioni

4624 registra un accesso riuscito, **4625** un tentativo fallito. Il logon type distingue l'accesso di rete (3) dalla sessione RDP (10); account e indirizzo di origine collegano l'evento a un attore.

Processi

4688 registra la creazione di un processo. La riga di comando compare solo se la relativa policy è attiva: va verificata prima di trarre conclusioni da un'assenza.

Sysmon

Se installato, aggiunge gli eventi **1** (processi con hash), **3** (connessioni di rete) e **13** (scritture nel registro). La sua configurazione decide che cosa viene registrato e fa parte della prova.

ESEMPIO • Su un server compaiono centinaia di 4625 verso l'account amministratore, poi un 4624 di tipo 10 dallo stesso indirizzo esterno e, subito dopo, un processo PowerShell con argomenti codificati registrato da Sysmon. In relazione si verbalizzano policy di audit e dimensione massima dei log, senza le quali un'assenza non si può interpretare.

Persistenza: sopravvivere al riavvio

Dopo l'accesso iniziale l'attaccante deve garantirsi il ritorno. Su Windows le tecniche più frequenti lasciano tracce precise: chiavi di registro **Run e RunOnce**, eseguite a ogni accesso; **servizi**, la cui installazione genera l'evento 7045; **attività pianificate**, registrate dall'evento 4698 se l'audit è attivo; **sottoscrizioni WMI**, segnalate dall'evento 5861 in WMI-Activity/Operational.

La ricerca combina più fonti: il registro, anche nelle shadow copies per vedere quando una chiave è comparsa; i file XML delle attività in C:\Windows\System32\Tasks; la timeline del file system per datare l'eseguibile richiamato. Ogni meccanismo va collegato a un account e a un orario.

Autoruns elenca i punti di avvio su un sistema acceso; sulla copia forense lo stesso controllo si fa con i parser del registro.

ESEMPIO • IL TRAFFICO CHE RITORNA

Un server viene ripulito e riavviato, ma il traffico anomalo riprende dopo due giorni. Le chiavi Run risultano pulite.

Il log WMI-Activity contiene un evento 5861: una sottoscrizione lancia uno script PowerShell a ogni avvio. La shadow copy precedente data la sua comparsa al giorno dell'accesso iniziale e la collega all'account di servizio compromesso.

Seguire l'attaccante da host a host

RDP

Sulla destinazione restano un **4624 di tipo 10** e l'evento **1149** nel log RemoteConnectionManager, con utente e origine. Sul sistema di partenza: registro del client RDP e cache bitmap.

PsExec

Installa sul sistema remoto il servizio **PSEXESVC**, che genera l'evento **7045**, insieme a un accesso di rete (4624 di tipo 3). Sul sistema di partenza restano le tracce di esecuzione del programma.

WinRM e credenziali

WinRM e PowerShell remoting lasciano eventi nei log della destinazione. Il filo comune sono le **credenziali**: lo stesso account su più host, in orari compatibili, disegna il percorso.

ESEMPIO • Dalla postazione di un impiegato compromessa via phishing, l'attaccante usa le credenziali di un tecnico, sottratte dalla memoria, per raggiungere il file server con PsExec e poi il controller di dominio via RDP. La ricostruzione mette in fila 4624, 7045 e 1149 su tre macchine: stesso account, intervalli di pochi minuti.

Ransomware: l'ultimo atto di un'intrusione

Un attacco ransomware segue di solito una cronologia riconoscibile: accesso iniziale, ricognizione della rete, raccolta di credenziali, esfiltrazione dei dati, cancellazione delle copie di ripristino (ad esempio con **vssadmin delete shadows**), cifratura e nota di riscatto. Fra il primo accesso e la cifratura possono passare settimane, e ogni fase lascia tracce proprie.

Nella **doppia estorsione** l'attaccante minaccia anche di pubblicare i dati sottratti. Datare l'esfiltrazione diventa allora decisivo: stabilisce se c'è stata una violazione di dati personali e alimenta la notifica all'autorità di controllo prevista dall'**art. 33 GDPR**, entro 72 ore dalla conoscenza della violazione.

Campione e nota di riscatto si conservano come reperti: aiutano ad attribuire la famiglia e, talvolta, a trovare strumenti pubblici di decifrazione.

ESEMPIO • LA CIFRATURA DEL VENERDÌ

Uno studio professionale trova i file cifrati un sabato mattina e vuole ripristinare subito dai backup.

Prima si acquisiscono memoria e dischi dei server. La timeline mostra un accesso VPN tre settimane prima, un archivio di 40 GB inviato a un servizio di cloud storage il giovedì e la cancellazione delle shadow copies alle 23:10 del venerdì. È la data dell'esfiltrazione a indicare l'inizio della violazione.

Molti host, una sola catena di custodia

Raccolta mirata

Con decine di host l'immagine completa di ciascuno non rientra nei tempi della risposta. **KAPE** e **Velociraptor** raccolgono in parallelo un insieme definito di artefatti: registro, event log, prefetch, MFT.

Telemetria EDR

Le piattaforme EDR registrano processi, connessioni e modifiche ai file, spesso per settimane. È una fonte conservata da terzi in formati proprietari: va esportata presto, documentando query e filtri.

Integrità da remoto

Una raccolta remota è un'acquisizione a tutti gli effetti: per ogni host si conservano l'archivio con il suo hash, il log del collector con comandi e orari, il riferimento orario dei sistemi.

ESEMPIO • Un'intrusione coinvolge 60 postazioni. Con Velociraptor il team raccoglie in un'ora event log, registro e prefetch da tutte, conservando per ciascun host archivio, hash SHA-256 e log delle operazioni. Solo i quattro host con indicatori positivi vengono poi acquisiti integralmente, e la relazione motiva il criterio di scelta.

AI nella risposta, con verifica sulla fonte

Le **regole Sigma** descrivono in un formato aperto le tracce di tecniche note negli event log; **Hayabusa** le applica a migliaia di file EVTX e produce una timeline già etichettata. L'**anomaly detection** sulle autenticazioni segnala accessi in orari, da sorgenti o verso sistemi insoliti per un account.

Un LLM può riassumere una timeline di migliaia di righe e proporre ipotesi sul percorso dell'attaccante, ma ogni affermazione va ricondotta all'evento di origine prima di entrare in un documento. Valgono le cautele di M8: con eventi rari il **base rate** rende falsi allarmi la maggior parte delle segnalazioni, e la validazione su campione resta necessaria.

In relazione si dichiarano versioni delle regole, strumenti e modelli usati, e la quota di segnalazioni verificate a mano.

ESEMPIO • IL RIASSUNTO DA VERIFICARE

Su 2,3 milioni di eventi Hayabusa segnala 1.840 corrispondenze di severità alta. Un LLM eseguito in locale le riassume in una pagina e indica un account di servizio come punto di ingresso.

La verifica sugli eventi originali conferma il percorso, ma due host citati nel riassunto non compaiono nei log: il modello li aveva dedotti per analogia. La relazione li esclude.

Contenere l'attacco senza distruggere la prova

Isolare invece di spegnere

Spegnere un sistema compromesso cancella memoria, connessioni e processi attivi. Isolarlo dalla rete, tramite EDR o a livello di switch, ferma l'attaccante e conserva lo stato volatile per l'acquisizione.

Acquisire prima di ripristinare

Il reimaging restituisce il server all'esercizio e ne elimina ogni traccia. Prima si acquisiscono memoria e disco, o almeno uno **snapshot** della macchina virtuale con il suo hash; poi si ripristina.

Verbalizzare la risposta

Account disabilitati, regole di firewall, processi terminati, file rimossi: ogni azione del team modifica il reperto. Va annotata con orario, autore e motivo, come qualunque operazione su una fonte di prova.

ESEMPIO • Il responsabile IT di un ospedale chiede di riavviare subito il server dei referti compromesso. Il team concorda una sequenza: isolamento di rete, acquisizione della RAM, snapshot della macchina virtuale, ripristino dal backup verificato. Il registro delle azioni entra nel fascicolo e spiega perché alcuni file mancano rispetto all'acquisizione.

Un'intrusione da ricostruire su tre fonti

Laboratorio

- Memoria, disco ed event log di uno scenario pubblico
- Timeline unificata con Plaso e Hayabusa
- Mappatura su **MITRE ATT&CK**

DELIVERABLE: `incident report`

Letture obbligatorie

- NIST SP 800-61 Rev. 3 (2025)
- Luttgens, Pepe, Mandia, *Incident Response & Computer Forensics*, 3a ed.
- MITRE ATT&CK for Enterprise

Verifica

Ogni passaggio poggia su eventi citati, con host e orario.

Prossimo modulo: M11 Profili giuridici ed etici (traccia core), oppure il modulo base della seconda specializzazione scelta.

Una risposta ben condotta ripristina i sistemi e lascia una documentazione che altri possono verificare.



Grazie per l'attenzione

Vincenzo Calabrò

Domande, materiali del corso e contatti
sul sito del docente



vincenzocalabro.it