MODULO S2.2 · AGOSTO 2026

Cloud, Identità ed e-Evidence

Indagare dove la prova è custodita da terzi:
audit log, account compromessi, ordini europei

`aws cloudtrail lookup-events` • `Get-MgAuditLogSignIn` • `kubectl get events`

Al termine del modulo lo studente sarà in grado di

01 · ACQUISIRE

Log e configurazioni dei principali provider cloud, documentando integrità, perimetro e finestra temporale della raccolta

02 · RICOSTRUIRE

La compromissione di un'identità e di un tenant, dal primo accesso illecito alle azioni compiute con l'account

03 · ATTIVARE

Gli strumenti giuridici per ottenere e conservare dati presso i provider, incluso il quadro e-evidence dell'Unione europea

Prerequisiti. Il modulo presuppone M5 (network e cloud forensics) e i moduli core di apertura: metodo e acquisizione (M1-M3), basi dell'AI e protocollo di validazione (M7-M8).

SCHEMA DEL MODULO

Dal log del provider all'ordine europeo di produzione

01 · FONTI

I log dei provider

- Audit log
- Retention e licenze
- Integrità della copia

02 · ATTACCHI

Identità e tenant

- Furto di token
- Consenso OAuth
- BEC in Microsoft 365

03 · AMBIENTI

Container e provider

- Kubernetes
- Snapshot e volumi
- Congelamento dei dati

04 · DIRITTO E AI

Ordini e anomalie

- Reg. (UE) 2023/1543
- Protocollo Budapest
- UEBA e base rate

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

APPROFONDIMENTO · AUDIT LOG DEI PROVIDER

Audit log del provider: la fonte primaria

Nel cloud molte azioni lasciano tracce soltanto nei registri del fornitore. **AWS CloudTrail** documenta le chiamate alle API di gestione; i log di accesso di **Microsoft Entra ID** registrano autenticazioni, indirizzi e dispositivi; l'**Unified Audit Log** di Microsoft 365 (Microsoft Purview Audit) raccoglie le attività su posta, file e amministrazione; Google Workspace offre registri analoghi.

Il punto critico è la **conservazione**: le finestre variano per servizio e spesso dipendono dalla licenza. L'acquisizione consiste nell'esportare i log con strumenti documentati, calcolare l'hash dei file ottenuti e annotare query, filtri e intervallo temporale, perché un altro consulente possa ripetere la stessa estrazione.

Va accertata e verbalizzata anche la configurazione dell'audit attiva al momento dei fatti: i log contengono solo ciò che il servizio era impostato per registrare.

ESEMPIO · LA FINESTRA CHE SI CHIUDE

Un'azienda scopre sei settimane dopo i fatti che un account amministrativo ha creato nuove chiavi di accesso nel proprio ambiente AWS.

La cronologia degli eventi di CloudTrail copre gli ultimi 90 giorni e l'analisi è ancora possibile. I log di accesso dell'identity provider, conservati per un periodo più breve, sono in parte perduti: la relazione dichiara la lacuna e indica le fonti alternative usate.

APPROFONDIMENTO · COMPROMISSIONE DELL'IDENTITÀ

Identità cloud compromesse e loro tracce

Proxy AiTM e furto di token

Una pagina di phishing si interpone fra utente e servizio, supera l'MFA e cattura il **cookie di sessione**. Nei log: accesso riuscito con MFA, poi la stessa sessione riusata da un altro indirizzo e da un altro client.

Consenso OAuth fraudolento

L'utente autorizza un'applicazione malevola con permessi su posta o file. Nessuna password viene sottratta: restano l'**evento di consenso** nell'audit e le azioni dell'applicazione, che opera con un proprio token.

Abuso delle notifiche MFA

Con la password già in mano, l'attaccante invia richieste di approvazione finché una viene accettata. I log mostrano **sequenze di richieste** negate o scadute, poi un'approvazione in un orario insolito.

ESEMPIO · In un tenant simulato, la casella di un responsabile amministrativo invia messaggi a fornitori sconosciuti. I log mostrano un accesso con MFA dalla sede alle 9:02 e, alle 9:04, accessi non interattivi della stessa sessione da un hosting estero. Per chiudere l'accesso occorre revocare sessioni e token: il solo cambio di password può non bastare.

APPROFONDIMENTO · BUSINESS EMAIL COMPROMISE

BEC in Microsoft 365: ricostruire la frode

Nella Business Email Compromise l'attaccante usa una casella legittima per deviare pagamenti o raccogliere informazioni. Le tracce stanno nella casella e nei log del tenant: **regole di posta** che inoltrano o nascondono messaggi, accessi da indirizzi o client inattesi, messaggi inviati e poi cancellati.

L'evento **MailItemsAccessed**, presente nell'audit con le licenze che lo prevedono, indica quali messaggi sono stati letti e da quale sessione. Su questa base si stabilisce che cosa l'attaccante ha visto, si ricostruisce la cronologia delle conversazioni alterate e si quantifica il danno, dato utile anche per le notifiche di violazione.

Le regole create dall'attaccante vengono spesso rimosse dopo la frode, ma creazione e cancellazione restano negli eventi di audit.

ESEMPIO · LA FATTURA DEVIATA

Un cliente simulato riceve dalla casella autentica di un fornitore la richiesta di pagare una fattura su un nuovo IBAN.

Nel tenant del fornitore l'audit mostra una regola che sposta nella cartella RSS i messaggi contenenti «bonifico», creata tre giorni prima da una sessione estera. Gli eventi di accesso alla posta indicano che l'attaccante ha letto tutto il carteggio con il cliente.

Container e Kubernetes: prove effimere

Carichi effimeri

Un container può vivere pochi minuti: quando il pod viene ricreato, il suo file system scrivibile scompare. La prova si cattura durante l'esecuzione o si cerca nei **volumi persistenti** e nei log raccolti centralmente.

Snapshot e immagini

Gli snapshot dei dischi dei nodi e dei volumi, presi con le API del provider, fissano lo stato del sistema. L'**immagine** d'origine, identificata dal digest nel registro, separa i file originali da quelli aggiunti in esecuzione.

Audit log del cluster

L'audit di Kubernetes registra le richieste all'API server: creazione di pod, comandi eseguiti con exec, lettura di segreti. Va abilitato con una policy adeguata e **inviato fuori dal cluster**, altrimenti segue la sorte dei nodi.

ESEMPIO · In un cluster simulato un pod esegue un miner di criptovaluta per due ore, poi viene eliminato e sul nodo non resta traccia. L'audit esportato all'esterno mostra la creazione del pod, l'account di servizio usato e un'immagine pubblica non autorizzata. Il registro conserva quell'immagine con il suo digest, ed è quella il reperto da analizzare.

APPROFONDIMENTO · PROVE PRESSO IL PROVIDER

Quando la prova è custodita dal provider

Molti dati rilevanti non sono nella disponibilità dell'indagato né della vittima: dati degli abbonati, indirizzi di accesso, contenuti archiviati da servizi di terzi. Si ottengono dal fornitore con titoli giuridici adeguati, e il tempo lavora contro l'indagine perché le **finestre di conservazione** possono essere brevi.

La prima mossa è il **congelamento**, cioè una richiesta di conservazione che sospende la cancellazione ordinaria in attesa dell'ordine di produzione. All'arrivo dei dati la catena di custodia diventa condivisa: si documentano chi li ha estratti presso il provider, il formato, eventuali hash o firme, la trasmissione e la verifica alla ricezione.

Nelle indagini aziendali vale la stessa logica: i contratti con i fornitori dovrebbero fissare tempi e modi di consegna dei log in caso di incidente.

ESEMPIO · IL LOG CHE NON C'È PIÙ

Per identificare l'autore di accessi abusivi a un servizio online estero servono i log di accesso conservati dal fornitore.

La richiesta parte dopo mesi e i log risultano cancellati secondo la politica di conservazione del servizio. Una richiesta di conservazione inviata nei primi giorni li avrebbe congelati: la relazione riporta l'assenza come limite dell'accertamento, senza colmarla con supposizioni.

e-Evidence: ordini diretti ai provider

Ordine europeo di produzione

L'autorità di uno Stato membro chiede al provider, tramite il destinatario designato nell'Unione, la consegna di dati elettronici: entro **10 giorni**, oppure entro **8 ore** nei casi di emergenza.

Ordine europeo di conservazione

Obbliga il provider a conservare dati già esistenti in vista di un ordine di produzione. La conservazione dura **60 giorni**, prorogabili una sola volta di 30 se servono per emettere l'ordine.

Ambito e destinatari

Dati degli abbonati e dati utili solo a identificare l'utente: qualsiasi reato. Traffico e contenuti: reati con pena massima di almeno **tre anni** o reati specifici, come quelli informatici. Destinatari designati secondo la Dir. (UE) 2023/1544.

ESEMPIO · Dal 18 agosto 2026, data di piena applicazione del Reg. (UE) 2023/1543, una procura che indaga su una frode online può chiedere direttamente a un provider di posta stabilito in un altro Stato membro i dati di accesso dell'account sospetto. Prima serviva un ordine europeo di indagine. Per il consulente cambia il formato dei dati ricevuti, da descrivere e verificare in relazione.

APPROFONDIMENTO · COOPERAZIONE INTERNAZIONALE

Budapest, ordine di indagine, rogatoria

Il **Secondo Protocollo addizionale alla Convenzione di Budapest** (2022) prevede richieste dirette ai registrar per i dati di registrazione dei nomi a dominio, richieste dirette ai provider per i dati degli abbonati e canali di cooperazione d'urgenza. Il suo valore pratico dipende dallo stato delle ratifiche, da verificare caso per caso.

Nell'Unione resta disponibile l'**ordine europeo di indagine** (Dir. 2014/41/UE, attuata in Italia con il d.lgs. 108/2017), che passa per l'autorità dell'altro Stato; verso i Paesi terzi c'è la **rogatoria**, spesso lenta. Lo strumento si sceglie in base a dove si trova il provider, al tipo di dato e all'urgenza.

Per il consulente conta sapere quale canale ha prodotto i dati: tempi, formato e garanzie di integrità cambiano da uno strumento all'altro.

ESEMPIO · IL DOMINIO DI PHISHING

Ipotesi didattica: un dominio usato per una campagna di phishing è registrato presso un registrar di un Paese extra UE con cui il Secondo Protocollo è in vigore.

La richiesta diretta dei dati di registrazione consente di collegarlo rapidamente ad altri domini dello stesso registrante. Senza quel canale la stessa informazione avrebbe richiesto una rogatoria, con tempi difficili da prevedere.

APPROFONDIMENTO · AI SUGLI ACCESSI

Anomalie di accesso da validare sui log

Impossible travel

Due accessi dello stesso utente da luoghi troppo distanti per il tempo trascorso. Indicatore utile, con molti falsi allarmi dovuti a VPN, proxy e reti mobili: la **geolocalizzazione degli indirizzi IP** è approssimativa.

UEBA

I sistemi di user and entity behavior analytics apprendono il comportamento abituale e segnalano scostamenti di orario, volume e applicazioni. Il **punteggio di rischio** è una stima del modello, da riportare con versione e soglie.

Base rate

Gli accessi malevoli sono una frazione minima del totale, e anche un modello accurato produce molte segnalazioni infondate. Come nel modulo 8, ogni allarme va verificato sui **log grezzi** prima di entrare in relazione.

ESEMPIO · In un tenant simulato di 5.000 utenti il sistema segnala in un mese 140 casi di impossible travel. La verifica sui log grezzi ne riconduce 131 a VPN e roaming, 8 a viaggi reali e uno solo a un token rubato. In relazione vanno il metodo di verifica e le prove tratte dai log; il punteggio del modello resta un indizio.

LABORATORIO · LETTURE · VERIFICA

Una frode in un tenant simulato

Laboratorio

- Tenant Microsoft 365 simulato, vittima di BEC
- Eventi **CloudTrail** sintetici da correlare
- Cronologia, dati letti e danno

`DELIVERABLE: ricostruzione e richiesta di conservazione`

Letture obbligatorie

- NIST IR 8006, *NIST Cloud Computing Forensic Science Challenges*
- Reg. (UE) 2023/1543
- Documentazione di Microsoft Purview Audit

Verifica

Ogni passaggio va ancorato a un evento di log citato.

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

> La qualità di un'indagine cloud si decide prima dell'incidente, nella configurazione dei log.

Grazie per l'attenzione

Vincenzo Calabrò

Domande, materiali del corso e contatti sul sito del docente

vincenzocalabro.it