SECURITY SUMMIT

Security Summit

Verona 28 ottobre 2026

Clusit

ASTREA

AI · CONTESTO · SUPERVISIONE UMANA

Le 2:41 di notte

Dall'alert alla decisione

Quando l'analista collega segnali distanti nel tempo e trasforma un sospetto in una nuova detection.

Matteo Colella | Senior Security Advisor –*Security Lab*

Emanuele Briganti | Presale Manager EMEA *ReeVo S.p.A.*



UN SEGNALE. TRE GIORNI DI STORIA.

Matteo Colella



Membro del Comitato Scientifico e
della commissione Premio Tesi del Clusit

Senior Security Advisor –*Security Lab*

Emanuele Briganti



Appassionato di CyberSecurity dagli anni 90

Presale Manager EMEA *ReeVo S.p.A.*

LO SCENARIO · I NUMERI DEL 2025

Si muovono in minuti. Li scopriamo in giorni.

RAPPORTO CLUSIT 2026 · ITALIA

507

incidenti gravi (+42%): il 9,6% del totale mondiale

CROWDSTRIKE · GTR 2026

29 min

per passare dal primo sistema violato al successivo (record: 27 s)

MANDIANT · M-TRENDS 2026

14 giorni

dalla compromissione al rilevamento (mediana; 11 nel 2024)

Per il Rapporto Clusit 2026 l'AI è un moltiplicatore del rischio: non inventa nuove minacce, ma rende più efficaci quelle esistenti.

Fonti: Rapporto Clusit 2026 (incidenti gravi di dominio pubblico, anno 2025); CrowdStrike 2026 Global Threat Report; Mandiant M-Trends 2026.

Gli incidenti crescono, l'attaccante si muove in minuti e può restare invisibile per giorni.

Gli attacchi vanno a velocità macchina.

PALO ALTO NETWORKS · 2026

4×

più veloci con l'AI avversaria, dall'accesso all'azione

NUOVA VULNERABILITÀ

~15 min

per scovarla e sfruttarla

ESFILTRAZIONE

<2 h

per completare un'esfiltrazione di dati

Quando l'analista apre l'alert, l'attacco è già due passi avanti: il tempo del difensore umano, da solo, non regge il ritmo di un avversario automatizzato.

Ordini di grandezza: Palo Alto Networks — «Fight AI with AI» (Cortex), 2026.

Il tempo del difensore umano, da solo, non regge: quando l'analista apre l'alert, l'attacco è già due passi avanti.

Attacchi che si scrivono, si clonano, si adattano.

01

PHISHING

Su misura

Email personalizzate, multilingue, senza errori di stile. Generate a migliaia.

02

DEEPFAKE

Voce e volto

Il CEO ricreato in una call per autorizzare un bonifico.

03

EXPLOIT

Automatici

Nuove vulnerabilità scoperte e sfruttate in minuti, non giorni.

04

MALWARE

Polimorfico

Muta a ogni esecuzione: le firme statiche non bastano più.

L'AI non rende l'attacco più furbo: lo rende più veloce, più credibile e più economico da ripetere.

LA RISPOSTA

All'AI si risponde con l'AI.

Detection, triage e correlazione a velocità macchina: un SOC agentico che pianifica, ragiona ed esegue, invece di accodare alert.

RILEVA

Rileva in minuti

Sensori e telemetria in tempo reale comprimono il tempo di rilevamento

CORRELA

Correla il contesto

Identità, asset e threat intel in un'unica catena, non alert isolati

PROPONE

Propone la risposta

Azioni di contenimento già pronte, misurabili e ripetibili

Alla velocità dell'attacco si risponde con la velocità della macchina. La decisione, come vedremo, resta umana.

IL PERNO · HUMAN ON TOP

L'analista è on top, non in the loop.

L'AI gestisce il ciclo veloce da sola: un umano a ogni passaggio la riporterebbe alla velocità umana. L'analista sta sopra: supervisiona, decide e firma le scelte che contano.

L'AI NEL LOOP

Rileva, arricchisce, correla, propone

Per ogni alert, 24 ore su 24. È il ciclo in cui l'umano non entra

L'ANALISTA ON TOP

Legge il quadro, valuta, decide, approva

Le azioni che pesano relazioni e denaro. Lo vedremo nell'esempio

PERCHÉ NON IN THE LOOP

Chiedere conferma a ogni passo rallenterebbe troppo

L'attaccante è già due passi avanti

Velocità della macchina + giudizio umano sulle decisioni finali: una risposta rapida e affidabile.

Gli attaccanti non si infiltrano più: si loggano.

01

PERIMETRO

Niente infiltrazione

Non c'è un muro da bucare: l'accesso avviene da una porta legittima, il login.

✗ il perimetro non vede

02

CREDENZIALI

Basta un'identità

Una credenziale o un token di sessione rubato apre la porta, spesso aggirando l'MFA.

✗ l'MFA non basta

03

DENTRO

Si agisce da utente

Da dentro l'attaccante è un utente legittimo: ogni azione, da sola, è normale.

✗ nessun alert scatta

Non servono muri più alti: la partita si gioca sul riconoscere l'uso illecito di un'identità legittima — prima che diventi un danno.

Alle 2:41 arriva un alert Entra ID.

02:41

Utente della contabilità

Registrato un nuovo dispositivo da una rete insolita. Un portatile legittimo o persistenza?

TELEMETRIA · ENTRA ID

SEVERITÀ INIZIALE: BASSA

Utente: amministrazione@azienda.it

Evento: Register device

Contesto: IP hosting / ore 02:41

MFA già soddisfatta in precedenza.

L’alert è basso. La domanda dell’analista: chi sta davvero registrando questo dispositivo?

Il SOC non cerca solo anomalie. Cerca significato.

MACCHINA

Osserva e ordina milioni di eventi

Rileva · Arricchisce · Propone

ANALISTA

Formula un’ipotesi e verifica ciò che manca

Interpreta · Decide · Assume responsabilità

RISULTATO

Una conoscenza che diventa riutilizzabile

Indagine → detection → risposta

Il vantaggio nasce quando il ragionamento umano diventa capacità sistematica.

L'AI accelera l’intera catena, non solo l’email.

01

ESCA

Più credibile

Testi coerenti con ruolo, settore e conversazione.

02

ACCESSO

Più scalabile

Landing page, codici e polling generati in automatico.

03

DOPO IL LOGIN

Più mirato

Ricerca di fatture, contatti e conversazioni sensibili.

L’effetto per il SOC: tanti gesti tecnicamente leciti, orchestrati con ritmo e obiettivo malevolo.

Non è un caso limite.

HUNTRESS · GEN–APR 2026

+1.380%

Device Code Phishing vs lug–dic 2025

HUNTRESS · UNA SOLA ONDATA

344

organizzazioni raggiunte

MICROSOFT · SET 2026

>12.000

caselle compromesse collegate a EvilTokens

44 temi di esca. AI nella scrittura, nell’infrastruttura e nell’analisi delle mailbox.

Fonti: Microsoft Threat Intelligence (22/09/2026); Huntress (06/2026).

L'attaccante non entra: si autentica.

01

PAGINA VERA

microsoft.com/devicelogin

02

MFA VERA

Autorizzata dalla vittima

03

SESSIONE DELL'ATTACCANTE

Token ottenuto tramite flusso lecito

Il successo della MFA dice che la vittima si è autenticata. Non dice che abbia autorizzato la sessione giusta.

PRIMA IL MECCANISMO

Il Device Code Flow è legittimo.

1

DISPOSITIVO

Richiede un codice

→

2

PERSONA

Apre Microsoft e approva

→

3

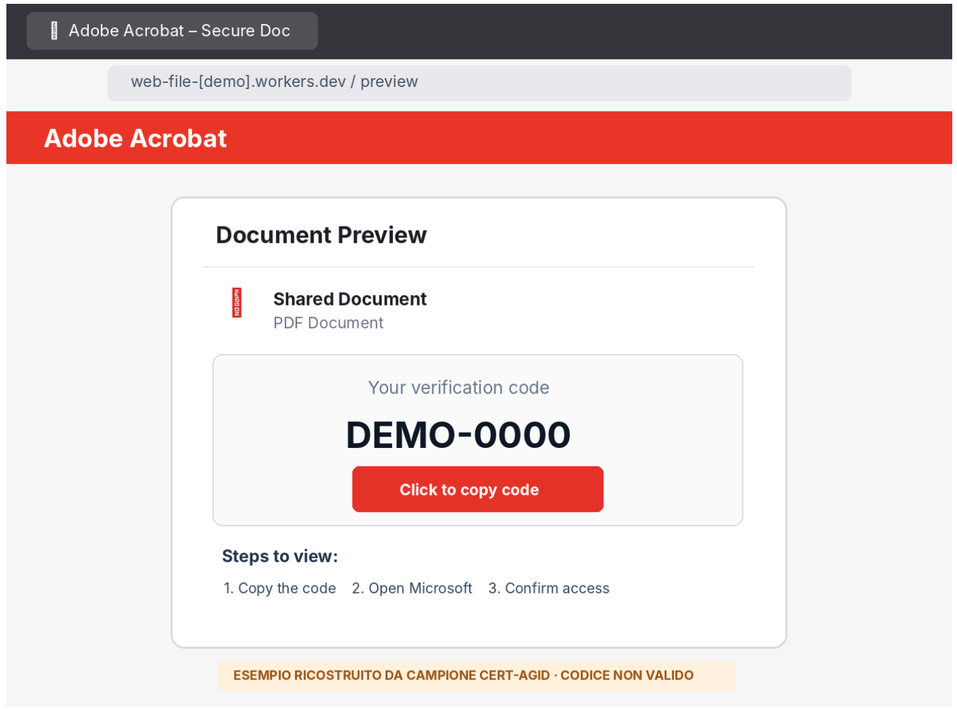
DISPOSITIVO

Riceve i token OAuth

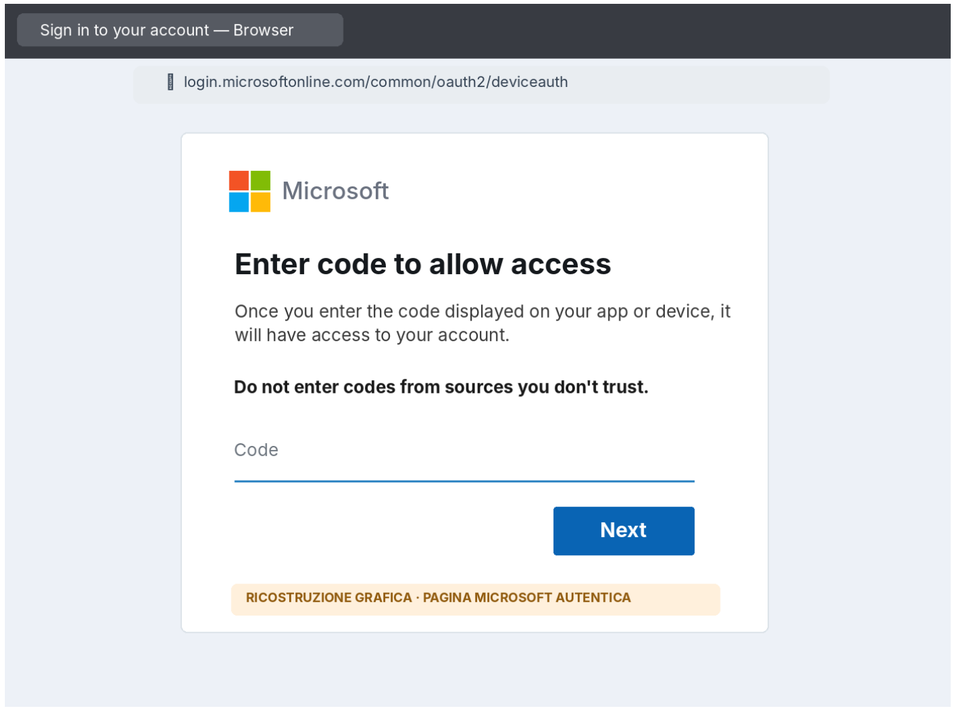
Pensato per smart TV, dispositivi condivisi e ambienti privi di tastiera o browser comodo.

Il codice è su una pagina-esca. Il login è davvero Microsoft.

① PAGINA-ESCA · SITO DELL'ATTACCANTE



② AUTENTICAZIONE · MICROSOFT LEGITTIMO



La vittima inserisce il codice sul portale vero. La sessione autorizzata è quella avviata dall'attaccante.

Ricostruzioni grafiche da screenshot documentati · CERT-AGID, 08/04/2026; Microsoft Threat Intelligence, 22/09/2026

PHISHING-AS-A-SERVICE

Un servizio criminale, non un kit artigianale.

01

ESCA PERSONALIZZATA

AI + contesto business

02

LANDING DINAMICA

Hosting serverless

03

TOKEN & MAILBOX

Raccolta e analisi automatica

04

OBIETTIVO BEC

Thread finanziari e contatti

Il business model è SaaS; la superficie da difendere è il comportamento dell’identità.

Perché i controlli tradizionali vedono tutto “pulito”?

EMAIL

Mittente già compromesso

Non sempre c’è spoofing.

BROWSER

Login Microsoft autentico

La pagina è legittima.

IDENTITÀ

MFA completata

L’accesso può risultare riuscito.

ENDPOINT

Nessun eseguibile malevolo

L’EDR può non rilevare nulla.

Il segnale non è nell’oggetto isolato. È nella sequenza degli eventi sulla stessa identità.

Una storia in tre giorni.

Un utente della contabilità.

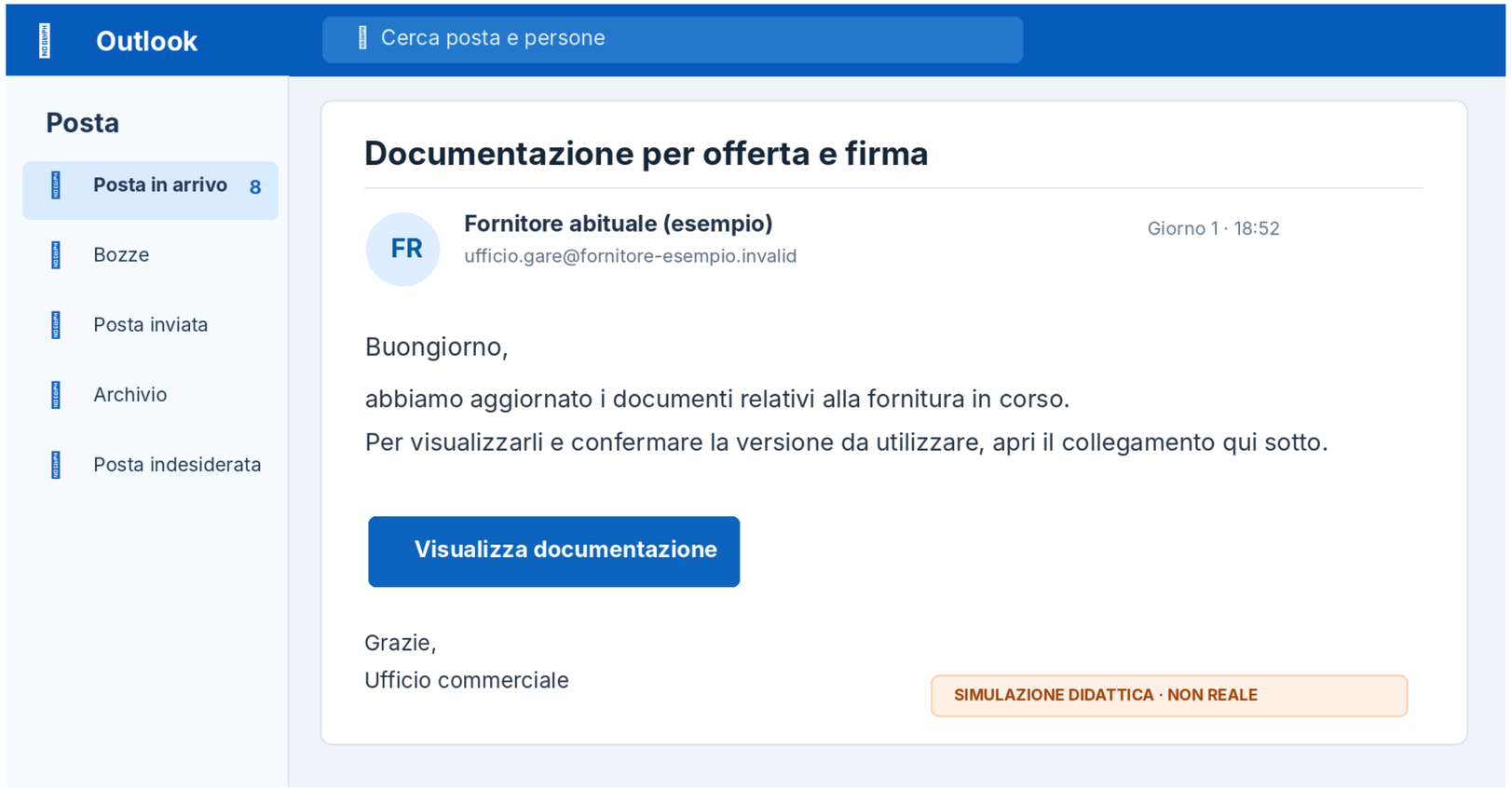
Un fornitore abituale.

Cinque passaggi. Un alert decisivo.

Il segnale decisivo arriva al giorno 3. L’ingresso nell’account è avvenuto prima.

SCENARIO NARRATIVO, NON INCIDENTE ATTRIBUITO A UN CLIENTE

Giorno 1 · 18:52 — Un’email perfettamente plausibile.



PERCHÉ FUNZIONA

MITTENTE
Fornitore e conversazione familiari

CONTESTO
Documenti, ordini e scadenze reali

RICHIESTA
Nessuna password da inserire nell’email

Messaggio ricostruito per il caso simulato. Le esche RFP, fatture e documenti condivisi sono documentate da Microsoft e CERT-AGID.

NESSUN ALERT

Giorno 1 · 18:56 — Accesso riuscito.

LATO VITTIMA

«È arrivato un documento dal fornitore.»

Apre il link, copia il codice, va su Microsoft, completa la MFA.

LATO ATTACCANTE

Una sessione OAuth viene autorizzata.

La vittima continua a lavorare. Il token è utilizzabile dall’altra parte.

Nel SIEM resta la telemetria di autenticazione. Non nasce necessariamente un alert.

Giorno 2 · 09:18 — La mailbox viene consultata.

09:18

Consultazione anomala di email

Casella della contabilità

Conversazioni finanziarie da un IP / ASN poco abituale.

Un’attività sospetta, non ancora una prova.

Microsoft 365 · Unified Audit Log — SCENARIO SIMULATO

Accesso alla mailbox · Exchange Online — REVIEW

Orario locale	Giorno 2 · 09:18
Identità	amministrazione@azienda.example
Workload	Exchange Online
Operazione	MailItemsAccessed
Volume osservato	**Accessi ripetuti a conversazioni finanziarie**
Contesto sorgente	**IP / ASN non abituale per l’utente**
Interpretazione	Ricognizione possibile · non prova di compromissione

RICOSTRUZIONE · DATI FITTIZI

Vista M365 audit ricostruita · dati fittizi

La lettura dei messaggi, da sola, può rientrare nell’attività legittima o di sincronizzazione.

Giorno 2 · 10:12 — Compare una regola Exchange.

EXCHANGE ONLINE

Nuova regola: spostare le risposte del fornitore in una cartella poco visibile.

SPIEGAZIONE POSSIBILE

«Sta organizzando la posta.»

Il legame con il login Device Code non è ancora riconosciuto.

Anche una regola Exchange è lecita di per sé. Diventa un indizio solo nel contesto.

Giorno 3 · 02:41 — Il dettaglio che cambia tutto.

02:41

Entra ID: nuovo dispositivo registrato.

Account contabilità, ora notturna, origine di hosting.

L’analista sospetta un tentativo di persistenza.

Microsoft Entra · Audit Logs — Demo tenant

Register device — Success

Activity	Register device
Timestamp	Giorno 3 · 02:41:00
Actor	amministrazione@azienda.example
Origine / ASN	**Provider cloud / hosting non abituale**
Device display name	DESKTOP-A4C91B
Result	Success
Contesto SOC	**Nuovo device · orario notturno · alert basso**

RICOSTRUZIONE · DATI FITTIZI

Vista Entra Audit Logs ricostruita · dati fittizi

Un device sconosciuto non prova l’attacco: è la possibile persistenza che avvia l’indagine.

Quattro domande davanti a un device sconosciuto.

01 IDENTITÀ

Un utente contabilità registra un dispositivo nuovo

02 ORARIO

Registrazione alle 02:41, senza attività IT prevista

03 ORIGINE

IP / ASN di hosting non abituale per quell’utente

04 ACCESSO

Come ha ottenuto l’autorizzazione per registrarlo?

Ipotesi da verificare: un accesso rubato viene trasformato in persistenza.

Alle 03:06 l’analista guarda indietro.

G3 · 02:41	Dispositivo registrato	TRIGGER
G2 · 10:12	Regola sul fornitore	NUOVA DOMANDA
G2 · 09:18	Accessi alla mailbox	RICOGNIZIONE?
G1 · 18:56	Device Code + MFA	POSSIBILE ACCESSO

Alle 03:06 collega gli eventi: da Entra a Exchange, fino al Device Code iniziale.

DISCIPLINA INVESTIGATIVA

Che cosa sa davvero? Che cosa deve ancora provare?

EVIDENZE NEI LOG

- ✓ Device Code Flow raro per questa identità
- ✓ Nuovo device alle 02:41 da origine inconsueta
- ✓ Regola Exchange sui messaggi del fornitore
- ✓ Accessi mailbox inconsueti il giorno 2

IPOTESI DA VERIFICARE

- ? Dispositivo sotto controllo di terzi
- ? Token usato da infrastruttura criminale
- ? Regola creata dall’attaccante
- ? Tentativo di frode nei pagamenti

La qualità del SOC è anche distinguere dato, inferenza e conferma.

CRONOLOGIA RICOSTRUITA

Ora i cinque eventi diventano una sola storia.

G1 · 18:52	G1 · 18:56	G2 · 09:18	G2 · 10:12	G3 · 02:41
Email fornitore	**Device Code + MFA**	**Lettura mailbox**	**Regola Exchange**	**Nuovo dispositivo**
Nessun alert	Nessun alert	Nessun alert	Bassa priorità	Alert basso

3 GIORNI · 1 IDENTITÀ · PIÙ SORGENTI · 1 IPOTESI VERIFICABILE

La diagnosi è tecnica. La decisione è anche umana.

CONTENIMENTO TECNICO

- → Revocare sessioni e refresh token
- → Bloccare temporaneamente l’account se necessario
- → Rimuovere dispositivi e regole malevole
- → Verificare consensi e metodi di autenticazione

GIUDIZIO DELL’ANALISTA

- → Contattare l’utente per conferma
- → Valutare coinvolgimento del fornitore
- → Avvisare Finance/Amministrazione del cliente
- → Cercare altre vittime e messaggi nel tenant

Automatizzare le verifiche ripetibili. Lasciare all’analista le decisioni ad alto impatto.

Il Modern SOC mette il contesto a disposizione.

RACCOLTA

Entra ID · M365 · Exchange
Endpoint · Rete · Cloud

→

CORRELAZIONE

Normalizzazione
Arricchimento · CTI
Ricerca temporale

→

INDAGINE

Identità · Timeline
Evidenze · Ipotesi
Decision support

ANALISTA

DECIDE

L’AI accelera triage e ricerca. L’analista resta responsabile delle scelte e migliora le detection.

Da quell’indagine nasce una nuova detection.

1

INGRESSO

Device Code Flow raro o nuovo per l’utente

2

RICOGNIZIONE

Accesso anomalo alla mailbox

3

OCCULTAMENTO

Regola Exchange sul fornitore

4

PERSISTENZA

Nuovo device alle 02:41 · correlazione 72 h

Segnali su 3 giorni: legarli per identità e sequenza consente di qualificare il rischio.

EVOLUZIONE OPERATIVA

La volta dopo: dall’investigazione alla correlazione.

PRIMA · SENZA CORRELAZIONE

3 giorni

di storia da ricostruire

Tracce su più sorgenti. L’analista ricostruisce l’accesso iniziale.

DOPO · REGOLA VALIDATA

Minuti

per proporre un caso correlato

Un solo caso arricchito, pronto da verificare e contenere.

*Obiettivo operativo simulato; il tempo reale dipende da ingestione, regole e latenza dei log.

Per renderlo reale servono cinque ingredienti.

01	**LOG GIUSTI**	Entra sign-in, non-interactive, audit e M365/Exchange
02	**IDENTITÀ COERENTE**	UPN / Object ID, session e token ID dove disponibili
03	**BASELINE**	Orari, device attesi, app OAuth e ASN usuali
04	**CORRELAZIONE**	Finestre multi-giorno, contesto e tuning per tenant
05	**RISPOSTA**	Runbook e autorizzazioni per il contenimento

PREVENZIONE **Limitare il Device Code Flow con Conditional Access dove non necessario.**

Il valore non è vedere più alert. È capire prima.

La macchina vede i segnali.

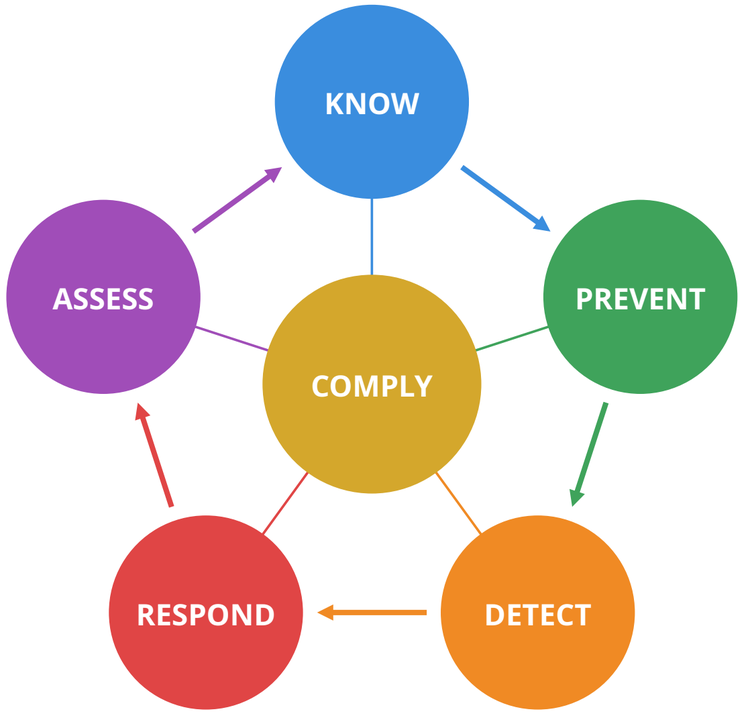
L’analista riconosce la storia.

Insieme trasformano una scoperta in una difesa ripetibile.

Human on top: AI nella velocità, responsabilità umana nelle decisioni.

Un ciclo di vita unificato della cybersecurity.

Ogni servizio ReeVo ha un posto preciso nel ciclo, con la conformità al centro



KNOW Conoscere la minaccia

Cyber Risk Assessment · Attack Surface Management · Vulnerability Assessment · CTEM

PREVENT Ridurre la superficie di attacco

MFA · Security Awareness · protezione dei documenti (IRM)

DETECT Vedere l'invisibile

SOC Open XDR H24 · EDR, NDR, ITDR gestiti

RESPOND Agire in tempo

SOC H24 · incident response

ASSESS Misurare il rischio

Penetration Test · Phishing Simulation

COMPLY NIS2, DORA, GDPR: ogni fase produce evidenze per la conformità

Agentic AI Cybersecurity Platform · SOC ReeVo

Rileva. Correla. Rispondi. Una visione unificata per proteggere l'intera superficie di attacco

FONTI DI DATI · TELEMETRIA

Endpoint
EDR e workstation, server, mobile
- CROWDSTRIKE
- SentinelOne
- Defender

Rete
NDR, firewall, IDS/IPS, proxy
- Fortinet
- Palo Alto
- Cisco
- VECTRA AI

Cloud
IaaS, PaaS, SaaS e container
- AWS
- Azure
- Google Cloud

FONTI DI DATI · IDENTITÀ E SISTEMI

Identity
Directory, IdP, MFA e accessi
- Entra ID
- Okta
- Active Dir.

SaaS e app
Email, collaboration, business app
- M365
- Workspace
- Salesforce
- GitHub

Log e sistemi
OS, database, virtualizzazione, OT
- Linux
- Windows
- VMware

Ingestion e parsing

Flusso telemetria

Agentic AI

CYBERSECURITY PLATFORM

Unified intelligence engine
Log, segnali e threat intel normalizzati (ECS), arricchiti e correlati in un unico motore

Detect · Detection agent
Analisi comportamentale, 1.200+ regole Sigma su ATT&CK e ragionamento AI per alert ad alto contesto

Hunt · Hunting agent
Caccia guidata dalla CTI integrata, anche retroattiva, per seguire le campagne avversarie

Investigate · Investigation agent
Process tree, tracce di rete, intel e alert correlati raccolti in una timeline in pochi secondi

Respond · Playbook adattivi
Isolamento host, blocco credenziali e contenimento: autonomi o con approvazione degli analisti ReeVo H24

Alert qualificati

Azioni di risposta

RISPOSTA & AUTOMAZIONE

Agisci rapidamente per contenere e risolvere

Playbook & automazione
SOAR integrato: workflow di risposta ripetibili e misurabili

Incident response
Gestione degli incidenti con gli analisti ReeVo H24

Azioni di contenimento
Isola endpoint, blocca IP, revoca accessi e credenziali

Ticketing & workflow
Casi tracciati nel portale CyberGrid e nei sistemi del cliente

Reporting & forensic
Timeline, evidenze e report dettagliati per ogni incidente

Visibilità e KPI

SOC & DASHBOARD CYBERGRID

Visibilità completa, decisioni migliori

Dashboard centralizzate
Postura, alert e attività del SOC in un'unica vista

Threat hunting
Ricerca avanzata sugli eventi, anche retroattiva

Alerting intelligente
Prioritizzazione per rischio, meno rumore

KPI, metriche e compliance
SLA, MTTD/MTTR e evidenze per audit e NIS2

BENEFICI CHIAVE

Rileva. Correla. Rispondi.

- Visibilità completa su tutta la superficie di attacco
- Rilevazioni avanzate e meno falsi positivi
- Risposta più rapida con automazione
- Efficienza operativa per il SOC
- Piattaforma aperta e best-of-breed

Grazie.

Domande?

Emanuele Briganti | Presale Manager EMEA

ReeVo S.p.A. · presale@reevo.it

SECURITY SUMMIT · VERONA · 28 OTTOBRE 2026

Contatti:

presale@reevo.it · Venite a trovarci al nostro Stand!

REEVO

Fonti e riferimenti tecnici.

MICROSOFT · EVILTOKENS

Unmasking EvilTokens: Getting to the root of device code phishing

microsoft.com/en-us/security/blog/2026/09/22/

HUNTRESS · REPORT 2026

EvilTokens and the Rise of AI-Powered Phishing

huntress.com/resources/eviltokens-ai-powered-phishing-report

MICROSOFT LEARN

Authentication flows in Conditional Access

learn.microsoft.com/en-us/entra/identity/conditional-access/concept-authentication-flows

CERT-AGID · AVVISO 08/04/2026

Phishing via Device Code Flow: l’allerta per la PA italiana

CERT-AGID · Leggi l’avviso originale (08/04/2026)

Il caso SOC è una simulazione. Email, login e log riprodotti come esempi didattici, basati sulle ricerche citate.