dinova
innovation does

Gerardo Costabile - Alessandro Aresi

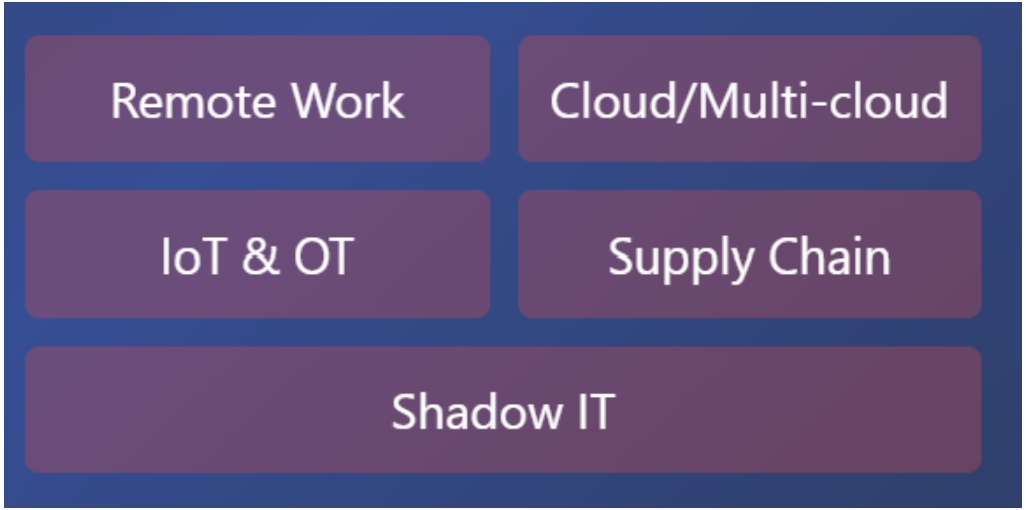
Cybersecurity a 360°: integrazione EDR e NDR, orchestrazione, threat intelligence e gestione operativa

Viterbo, 24 ottobre 2025

Alcuni numeri

Saltando le statistiche sugli attacchi cyber (di cui abbiamo piena la pancia ☺), siamo tutti d'accordo che..

...la superficie di attacco si espande



E già questo è un primo «problema».

Inoltre, l'approccio frammentato fallisce

- ✓ **Blind spots:** strumenti isolati non comunicano tra loro
- ✓ **Tempi di risposta lenti:** investigazioni manuali attraverso tool diversi
- ✓ **Attaccanti più veloci:** si muovono lateralmente mentre i difensori su soffermano nelle analisi
- ✓ **Alert fatigue:** SOC sommersi da migliaia di alert giornalieri non correlati

Un attaccante impiega 1-2 ore per il lateral movement, un SOC tradizionale anche 24-48 ore per correlarli

Limiti dell'EDR da solo: blind spot nella rete

Cosa l'EDR NON *(necessariamente)* vede:

- ✓ **Traffico di rete est-west:** comunicazioni laterali tra dispositivi che non passano dall'endpoint
- ✓ **Dispositivi non gestiti:** stampanti, IoT, dispositivi guest, BYOD senza agent
- ✓ **Network-based attacks:** attacchi che sfruttano vulnerabilità di rete (es. ARP spoofing, DNS tunneling)
- ✓ **Command & Control (C2) evasivo:** traffico C2 che bypassa l'endpoint usando protocolli legittimi
- ✓ **Esfiltrazione via rete:** dati che escono attraverso canali di rete non monitorati dall'endpoint
- ✓ **Lateral movement stealth:** movimenti tra sistemi usando credenziali legittime rubate
- ✓ **Attacchi fileless in memoria:** che non toccano il disco e usano solo la rete per propagarsi

Integrazione EDR/NDR

L'integrazione EDR-NDR non è una semplice «unione» di telemetrie, ma un **sistema di correlazione bidirezionale** che genera contesto operativo attraverso l'arricchimento reciproco degli eventi.

- ✓ **EDR «aiuta» l'NDR - Esempio:** Alert NDR su traffico anomalo → EDR fornisce: processo responsabile, user context, command line, parent-child relationship

- ✓ **NDR «aiuta» EDR – Esempio:** Alert EDR su processo sospetto → NDR fornisce: destinazioni network, volume dati, protocolli, geolocation

Più di un «aiutino»: il SOAR

Overload nel SOC

- ✓ 1.000+ alert/giorno da strumenti multipli
- ✓ Analisti sommersi da task ripetitivi
- ✓ Correlazione manuale lenta ed error-prone
- ✓ Attaccanti si muovono più velocemente dei difensori

L’analista SOC vi ringrazierà!

I tre pilastri del SOAR

- ✓ **Orchestration**: collega tool diversi in un unico workflow
- ✓ **Automation**: esegue azioni ripetitive senza intervento umano
- ✓ **Response**: coordina contenimento e remediation multi-tool

L’importanza della CTI

Strategica
- ✓ **Target**: Executive, decision maker, board
- ✓ **Contenuto**: Trend minacce, threat actor, motivazioni, rischio geopolitico
- ✓ **Scopo**: Guida investimenti e priorità di sicurezza
- ✓ **Orizzonte temporale**: mesi/anni

Tattica
- ✓ **Target**: SOC, threat hunters, detection engineers
- ✓ **Contenuto**: TTPs (Tactics, Techniques, Procedures), MITRE ATT&CK
- ✓ **Scopo**: Detection engineering, threat hunting, gap analysis
- ✓ **Orizzonte temporale**: settimane/mesi

Operativa
- ✓ **Target**: SOC analysts, incident responders, automation
- ✓ **Contenuto**: IOCs (IP, domini, hash, URL), campagne attive
- ✓ **Scopo**: Blocking immediato, SIEM/EDR/NDR/Firewall feeds
- ✓ **Orizzonte temporale**: ore/giorni
- ✓ **Sintesi**: Strategica guida decisioni, Tattica costruisce difese, Operativa blocca attacchi

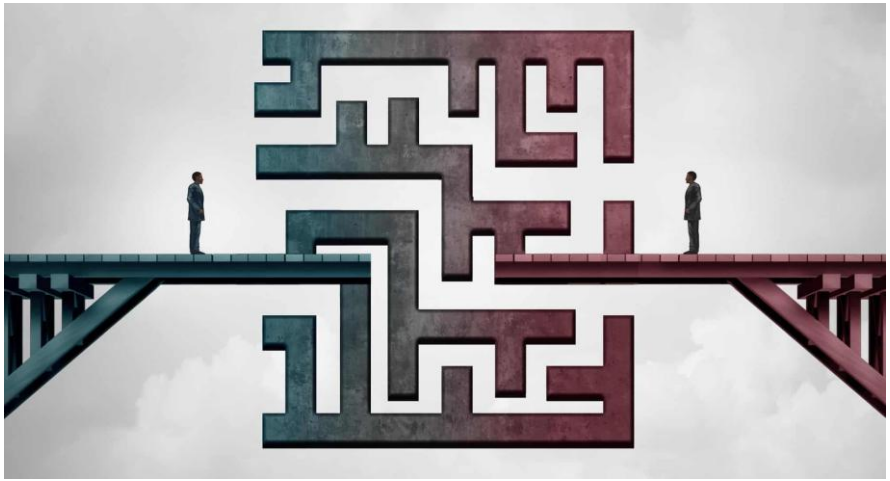
Le 4 sfide di un SOC interno

1) **Numero di persone**: per attivare un SOC 24/7 servono circa 10/12 persone → problema turn over circa 20/30% annuo

2) **Costi:** 1,2-2Mln euro primo anno → Ipotizzabile per <5% delle aziende italiane

3) **Tempistiche:** 5/8 mesi primi risultati; 9/12 mesi full operation

4) **Gap expertise:** Vedi solo i tuoi attacchi (ovvero circa 50 incidenti all'anno vs migliaia di incidenti all'anno che vede un MDR). La telemetria aggregata porta una cross-fertilizzazione abilitante.

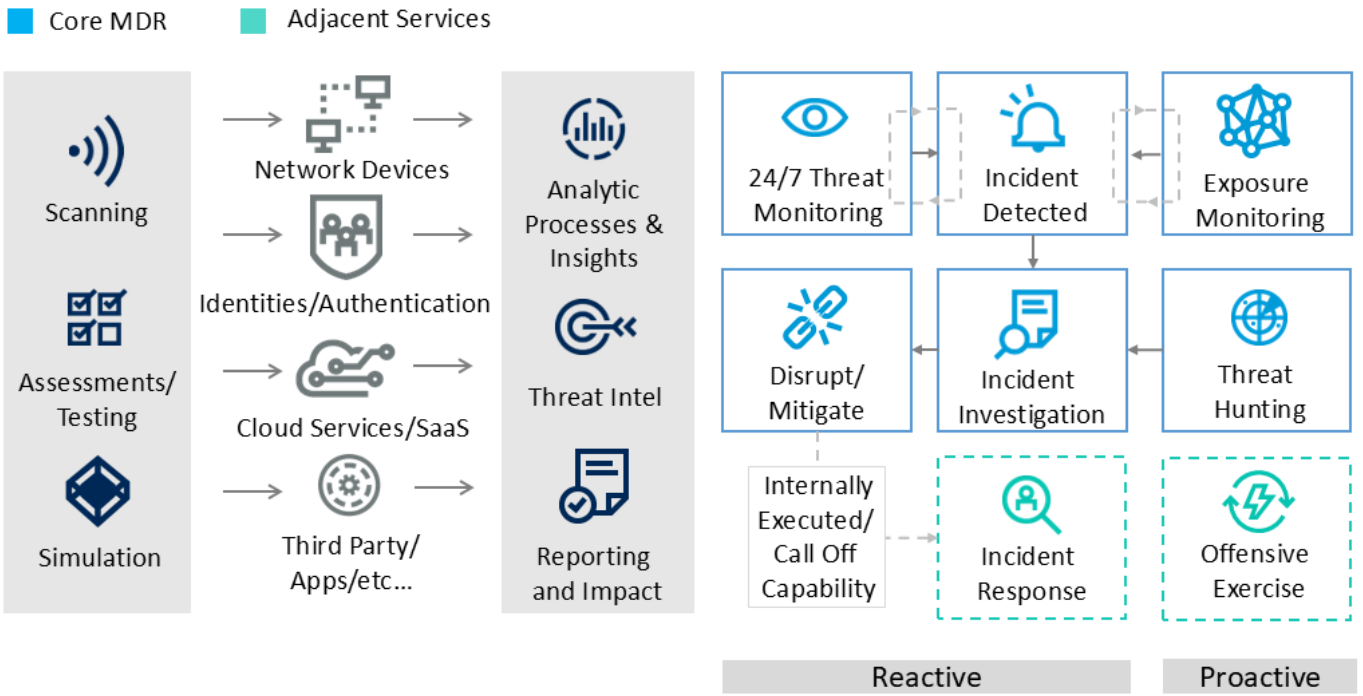


E «infine», SOC o MDR? Partiamo da una definizione!

Gartner definisce

«i servizi di rilevamento e risposta gestiti (MDR) come quelli che forniscono ai clienti funzioni di Security Operations Center (SOC) erogate da remoto…Omissis…
***Offrono un'esperienza chiavi in mano**, utilizzando uno stack tecnologico predefinito che generalmente copre endpoint, reti, log e cloud… omissis…*
Il team di analisti del provider MDR esegue quindi la ricerca delle minacce e la gestione degli incidenti ***per fornire le azioni consigliate ai propri clienti**.»*

Core MDR e «servizi adiacenti»



SOC | Metodologia – AIR (utilizzata in Dinova/CSS)

AUTONOMIC INCIDENT RESPONSE - AIR

EXTENDED DETECTION & RESPONSE - {EX}DR

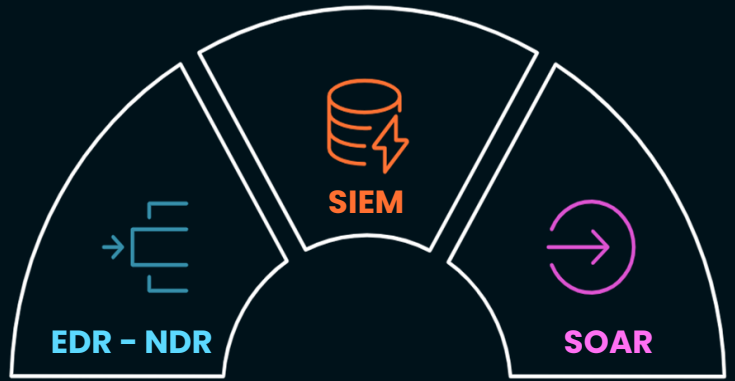
DATA

Raccogliere dati di sicurezza è fondamentale per **correlation**, **behaviors** e **detection**

ENDPOINT e NETWORK

La sicurezza Endpoint, con gli EDR, migliora la postura difensiva con **prevention**, **detection** e **response**.

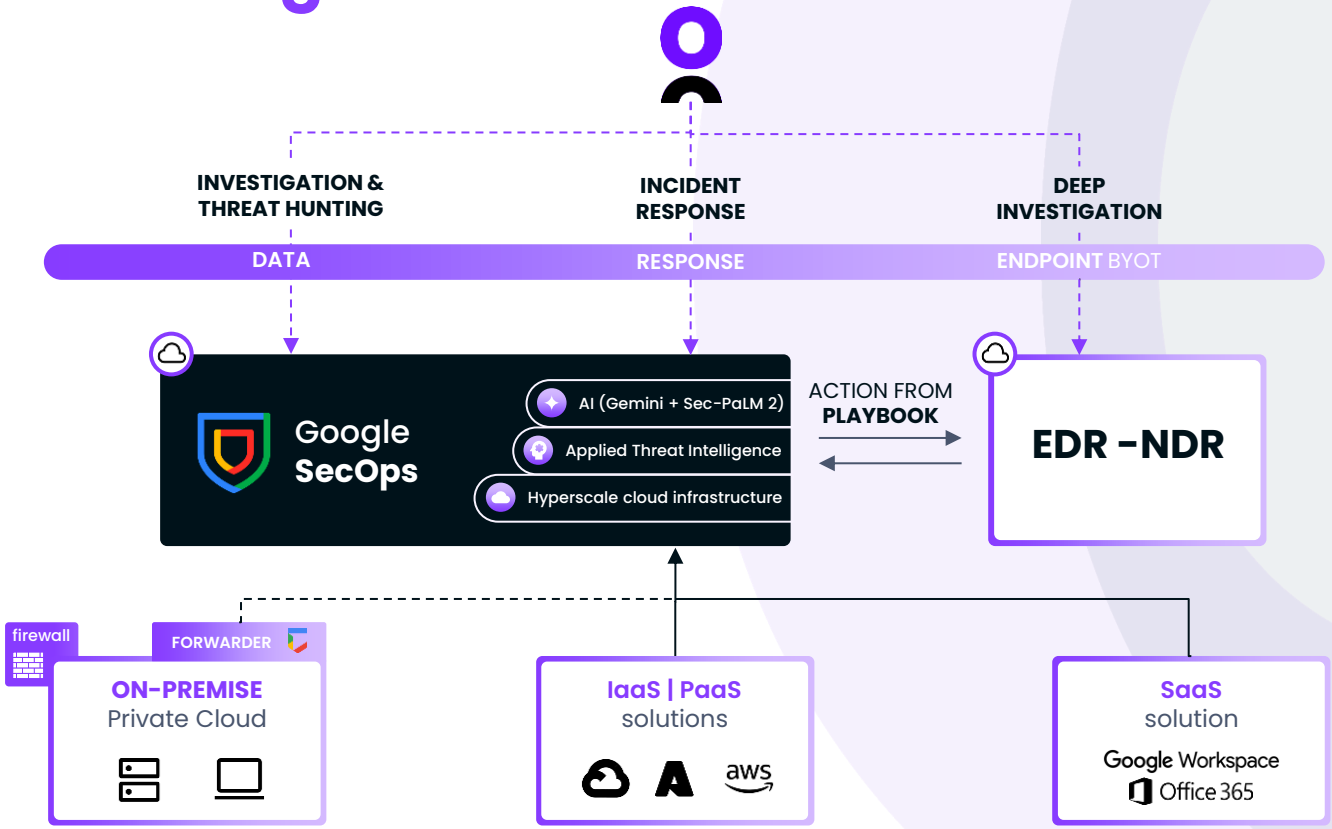
Gli **NDR** forniscono una copertura importante per la componente di Network offrendo visibilità avanzata



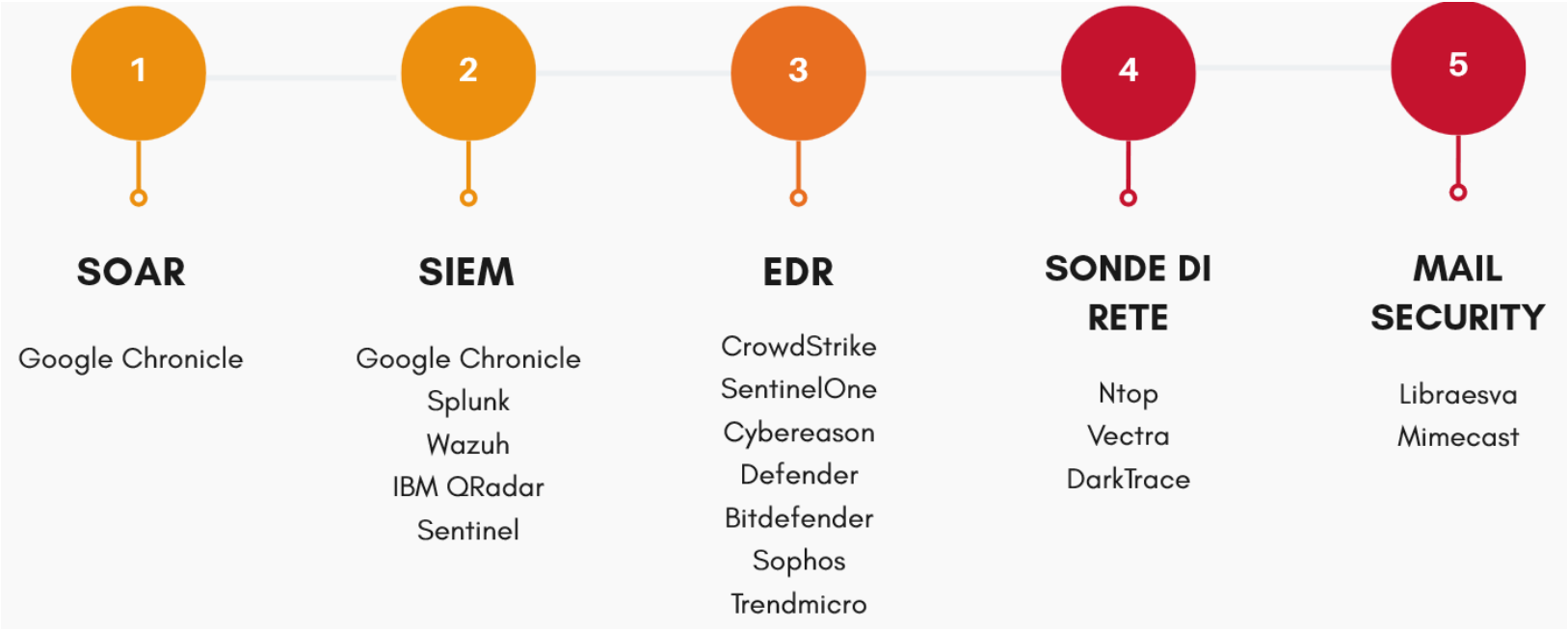
RESPONSE

Incident Response con soluzioni unificate per **triage**, **automation** e **response**. La nostra esperienza permette di velocizzare la risposta tramite automation consolidate

Stack tecnologico



Alcuni nostri strumenti



Una tabella comparativa degli «archetipi di SOC»

Dimensione	Archetipo 1 FULL IN-HOUSE	Archetipo 2 HYBRID	Archetipo 3 CO-MANAGED	Archetipo 4 FULLY MANAGED	Archetipo 5 AUGMENTED
% Organizzazioni	5%	15-20%	25-30%	40-50%	5-10%
Budget annuo	€1.5M-€5M+	€800K-€2M	€250K-€700K	€50K-€250K	€1.1M-€2.3M
Headcount security	15-25	5-10	2-4	0-1	10-20
Technology ownership	100% internal	Internal	Shared	MDR	Internal
SOC operations	100% internal	Tier2/3 internal Tier1 MDR	Primary MDR Strategic internal	100% MDR	Primary internal Gap MDR
Control level	⭐⭐⭐⭐⭐	⭐⭐⭐⭐	⭐⭐⭐	⭐⭐	⭐⭐⭐⭐
Time to operational	18-24 mesi	12-18 mesi	4-8 settimane	2-4 settimane	6-12 mesi
Customization	⭐⭐⭐⭐⭐	⭐⭐⭐⭐	⭐⭐⭐	⭐⭐	⭐⭐⭐⭐⭐
Cross-customer intel	❌	⭐⭐⭐	⭐⭐⭐⭐	⭐⭐⭐⭐	⭐⭐⭐
Operational burden	⭐⭐⭐⭐⭐ (massimo)	⭐⭐⭐	⭐⭐	⭐ (minimo)	⭐⭐⭐⭐
Vendor lock-in risk	❌	⭐⭐	⭐⭐⭐	⭐⭐⭐⭐⭐ (massimo)	⭐⭐

Alcune riflessioni conclusive

- ✓ I processi delle operazioni di sicurezza **non possono essere completamente esternalizzati.**
- ✓ Far sì che un fornitore MDR rilevi una minaccia **non ha senso senza i propri processi di risposta agli incidenti pianificati in anticipo**.
- ✓ Avere un monitoraggio e una gestione efficace **sono frutto di un lavoro ben più ampio sui «fondamentali» della cybersecurity**, a partire dal log management e passando per tutte le cose citate «di corsa» in questa presentazione.

Thank you!

Dinova
via dei Lapidari 12, 40129
Bologna, Italia
T. +39 051 6120291 E. info@dinova.one