SECURITY SUMMIT

Security Summit

Verona 28 ottobre 2026

Clusit

ASTREA

Percorso gestione sicurezza

Passato e futuro dei servizi MDR

deda.tech

Giorgio di Grazia | Pre-Sales Specialist, *Deda Tech*
Alessio Pennasilico | Scientific Committee, *Clusit*

Alessio Pennasilico aka -=mayhem=-



CISO

Member of the Board of Directors of the Association of IT Professionals

Member of the Scientific Committee

Senior Partner, Information & Cyber Security Advisor @Security Evangelist & Ethical Hacker

Vice President of the Committee for the Safeguarding of Impartiality

Member of the Scheme Committee

Scientific Director of the publication

Senior Advisor of the Cyber Security & Data Protection Observatory of the Politecnico di Milano

Core faculty

Giorgio di Grazia

Pre-Sales Specialist, Deda Tech



30	Anni di esperienza in ambito IT, **20** di IT Security
10	Anni di esperienza come pentester
7	Anni come assessor PCI DSS (PCI QSA)
6	Anni come Technical Product Manager e Pre-Sales (Threat Detection and Response, MDR)

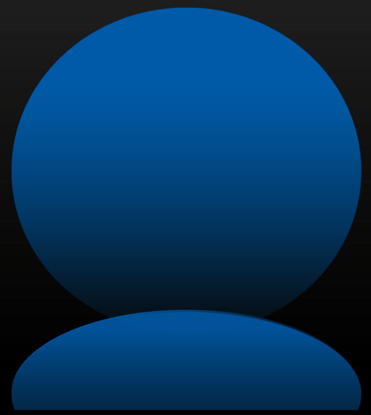
https://www.linkedin.com/in/giorgiodigrazia

deda.

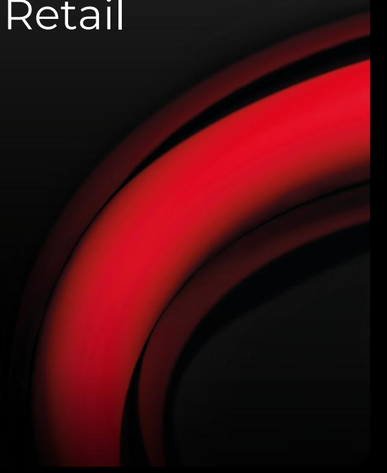
AREE STRATEGICHE

Servizi e competenze per far crescere le organizzazioni

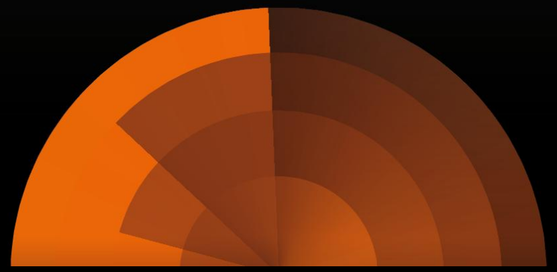
Financial Services



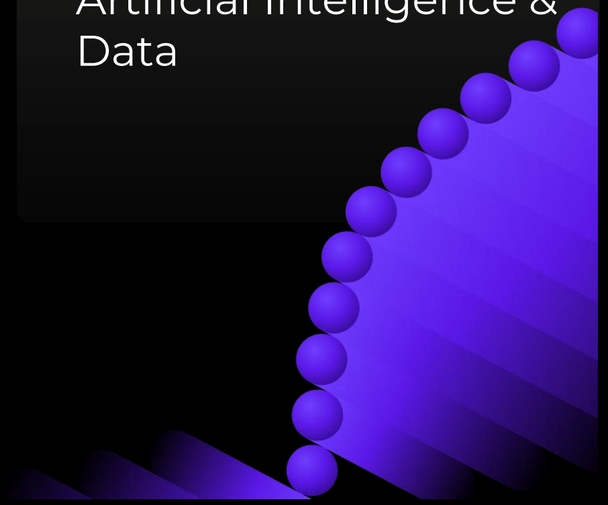
Fashion &
Luxury Retail



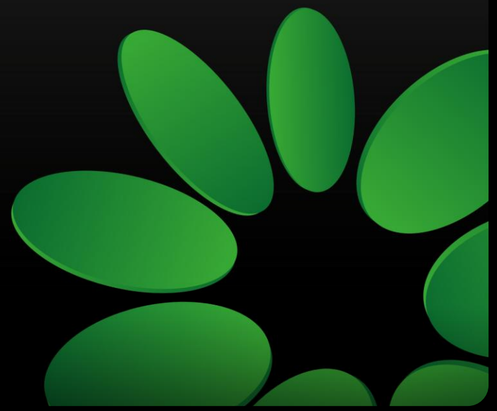
Public Services



Artificial Intelligence &
Data



Cloud &
Cybersecurity



Digital Business



deda.tech

Offerta cyber

Data Security	Identity Governance Administration (IGA)
OT Security	Governance, Risk, and Compliance (GRC)
Offensive Security	Continuous Defense Validation (AEV)
CISO Office aaS	Continuous Control Monitoring (CCM)
Blue Team, DFIR	Managed Detection & Response (MDR)
Security Awareness	Cyber Threat Intelligence (CTI)

Breve evoluzione dei servizi MDR

Gartner: definizione dei servizi MDR (2021)

”

Managed detection-and-response (MDR) servicesooooooo ksksssksk remotely delivered oooooooooooooooooooooooooooooooofunctions allow ooooooooooooo detect, analyze, investigate and actively respond t

o oooooooooooooooooooa turnkey experience, using a sosososoooos skskskskskskosososs that commonly coversooooooon to deliver outcomes that.

Market Guide for Managed Detection and Response Services, October 2021

Photo by Pixabay

Gartner: definizione dei servizi MDR (2025)

> *[...] Cybersecurity leaders should use this research to identify MDR services that meet their business-driven risk requirements. Mandatory Features: [...] 24/7 staffing that recognises customer-specific cyber-risk-based use cases, engages daily with individual customer data.*

Market Guide for Managed Detection and Response Services, October 2025

Com’era il mercato nel 2022-2023 in Italia?

ELEVATA MATURITÀ → **BASSA MATURITÀ**

MDR Provider (pure play)

Offre una managed security chiavi in mano con molteplici data source, non vincolata a tecnologie specifiche. Servizio human-led supportato da un SOC multitier maturo, con service layer che variano dal livello base a quello completo.

Il threat hunting è incluso nel servizio standard. Possono offrire ulteriori funzioni di security operations, tra cui CTEM e DFIR (es. **incident retainer**).

Altri offrono una piattaforma di sicurezza **proprietaria** (aggregatore di dati, XDR, ecc.) utilizzata per centralizzare tutte le informazioni.

Vendor (es. EDR)

Aziende vendor che offrono servizi MDR basati sulla propria tecnologia (principalmente **EPP/EDR**).

Attorno a essa è strutturato un **SOC 24x7**, ma sono prive di ulteriori servizi professionali rilevanti o di estese capacità di ingestion per tecnologie third-party.

Le comunicazioni sono principalmente in **lingua inglese**.

NOC/MSSP mascherati

Ex network operations center (**NOC**) o **MSSP** di base (focalizzati su uno specifico managed service, come firewall/IDS/IPS) che hanno deciso di espandere la propria clientela offrendo un livello di servizio MDR da basso a medio.

Non svolgono attività di threat hunting e incident response e **inoltrano** principalmente gli **alert** al cliente, il quale deve gestire gli incidenti senza alcun supporto. Sfruttano fortemente la tecnologia (EDR, NDR, ecc.).

Spesso **rivendono** le soluzioni MDR dei vendor senza servizi professionali.

Nota: la maturità illustrata può variare in modo significativo. I vendor ad esempio potrebbero eccellere in questo ambito (dipende dalla tecnologia adottata, dalla maturità del SOC, dalle capacità della rete dei partner sul territorio ecc.).

Forrester: EDR Is Dead, Long Live XDR



EDR Is Officially Out, And XDR Still Won't Solve Your SIEM Problems

Allie Mellen, Principal Analyst NOV 28 2023

FORRESTER®

Adapt Or Die: XDR Is On A Collision Course With SIEM And SOAR

EDR Is Dead, Long Live XDR

Allie Mellen and six contributors

Apr 28, 2021

28 aprile 2021

Forrester prevede l'evoluzione degli **EDR**: *EDR Is Dead, Long Live XDR*. Anticipa che non parlerà più di EDR.

28 novembre 2023

Dichiara che il momento è arrivato e ritira la *The Forrester Wave™: Endpoint Detection And Response Providers* (ma gli XDR **non** sostituiranno i SIEM).

24 giugno 2025

In *The Forrester Wave™: Security Analytics Platforms, Q2 2025*, Mellen nota come a differenza di molti SIEM presenti sul mercato, gli XDR manchino di flessibilità (**data ingest**, **manipulation** e **use case** di **compliance**).

SOC visibility: triad or quad?

Cloud native environments? CDR?

Identity visibility?

Application visibility is probably the 4th pillar!

(ADR)

LOGS
(SIEM/UEBA)



ENDPOINT
(EDR)

NETWORK
(NDR)



Anton Chuvakin
Computer security specialist

Le tecnologie e le necessità evolvono.
I rischi anche.

Assumersi i rischi

> *La cybersecurity non è una semplice questione di scelte tecnologiche, ma significa sapersi assumere i giusti rischi aziendali.*

Microsoft, The Cost of Inaction, 2023

MDR is a human-led service

Cosa chiedere ai servizi MDR e quale maturità offrire

Fate tutto voi? No.



Photo by Mark Farías (Unsplash)

Clusit

SECURITY SUMMIT

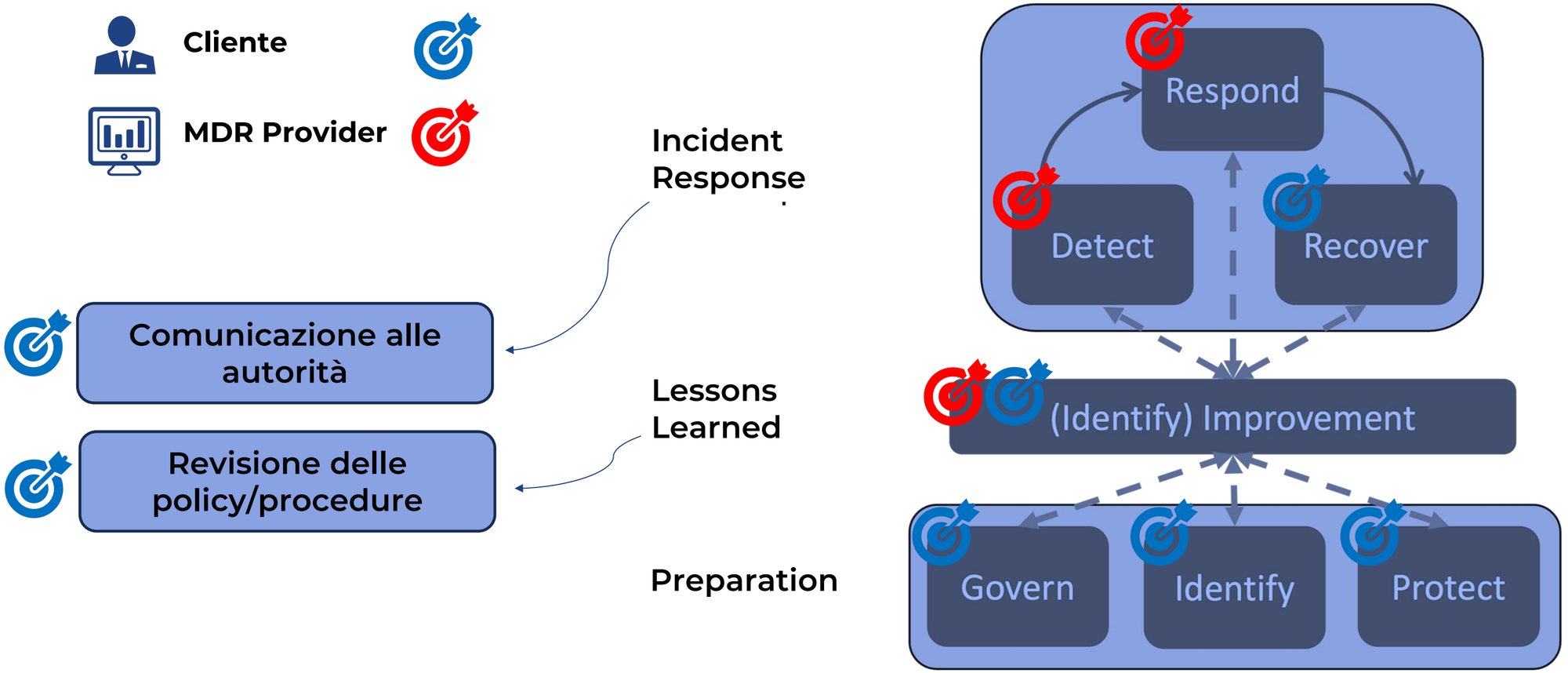
deda.tech
YOUR SAFE IT

ASTREA



Regola # 1: la gestione di un incidente informatico non inizia quando scatta l'allarme. Inizia molto prima.

Gestione di un incidente informatico (MDR)



NIST *Incident Response Recommendations and Considerations for Cybersecurity Risk Management* (April 2025)

La maturità del cliente e il paradosso MDR



Le fondamenta non si esternalizzano: l'igiene IT di base, il patching e l'inventario degli asset sono prerequisiti, non compiti del fornitore MDR.



Il contesto di business è sovrano: l'MDR è cieco senza il cliente; serve maturità nel definire i sistemi critici e le catene di approvazione per gli interventi notturni.



Integrazione dei processi interni: l'MDR contiene l'attacco (es. isolando un server), ma il ripristino operativo e il clean-up richiedono un team IT interno (o un MSP) preparato.



Acceleratore, non bacchetta magica: l'MDR colma il divario verso una postura di sicurezza avanzata, ma fallisce se usato per compensare la totale assenza di processi aziendali.

Regola # 2: se il cliente non sa cosa proteggere, l'MDR non saprà dove guardare.

Il consiglio di un cliente

”

Il consiglio principale ai potenziali clienti è di assicurarsi di avere una profonda *comprensione dei requisiti di cybersecur*ity della propria organizzazione e di come il servizio MDR possa aiutare a soddisfarli. Per ottenere il massimo, è fondamentale disporre di una *roadmap* ben definita per la corretta implementazione e utilizzo del servizio.

Security and Risk Management Professional, Service Sector, Gartner Peer Insights

Photo by Pixabay

Cosa chiedersi prima di cercare un fornitore

L’obiettivo è predisporre un’autovalutazione per definire un perimetro di delega.

1. Quali sono i rischi e le minacce di **business** che rappresentano in assoluto la nostra massima priorità?
2. Disponiamo delle **risorse IT** interne (o di un partner fidato) per eseguire le azioni di ripristino e remediation che l'MDR non copre?
3. Siamo disposti, a livello politico e operativo, a delegare azioni di **contenimento** dirette (come spegnere un server critico) a un team esterno?
4. Quale stack tecnologico possediamo attualmente e vogliamo mantenerlo (approccio **bring-your-own-tech**) o siamo pronti a sostituirlo?
5. Siamo in grado di fornire costantemente al fornitore il nostro **contesto** aziendale (asset critici, vulnerabilità, modifiche dell’infrastruttura ecc.)?
6. Quali **vincoli** normativi, di conformità o di residenza dei dati dobbiamo obbligatoriamente rispettare?

Le domande da porre al fornitore MDR

Come smascherare i finti servizi gestiti e misurare il vero valore.

1. Qual è l'esatto perimetro delle azioni di **mitigazione** e contenimento che potete eseguire in autonomia sui nostri sistemi?
2. In che modo acquisite, mantenete aggiornato e utilizzate operativamente il nostro **contesto** aziendale durante un'indagine?
3. Quale percentuale delle vostre attività di threat hunting è realmente basata su ipotesi (**hypothesis-driven**) e guidata da esseri umani rispetto a quella basata su allarmi automatici?
4. Vi impegnate su metriche di servizio basate sui tempi effettivi di contenimento della minaccia anziché sui semplici tempi di notifica?
5. Come strutturate il processo di **onboarding**, quanto dura in media e quanto effort richiederà al nostro personale interno?
6. In caso di **incidente** grave, avremo accesso diretto agli analisti di livello avanzato che stanno gestendo l'emergenza? Avremo accesso ai dati *raw*? Possiamo vedere un **esempio** anonimo?

Autonomous SOC: un mito?

Lista dei vendor AI SOC (ottobre 2026)

177	8	4	2
All Active Products	Active Acquired	Acquired Absorbed	Pivoted away

Independent and acquired products, excluding those confirmed absorbed.

Core categories

79
AI SOC as Capabilities

AI triage, investigation, and response as a layer inside a broader platform

CAPABILITY DEFINITION

67
AI SOC Pure Play

AI SOC as the entire product, vendor agnostic by architecture

☆ PRIMARY ONLY

CAPABILITY DEFINITION

31
AI SOC Supporting Capability

Every other SecOps tool that helps an AI SOC work, such as data, detection, context, automation or resilience, without offering AI SO...

CAPABILITY DEFINITION

Fonte: SecOps Unpacked, https://secops-unpacked.ai/research/ai-soc-vendors?category=AI+SOC+Pure+Play

Frontier AI Era

> *Security fundamentals matter more than ever in the age of AI.*

ENISA’s view on Cybersecurity in the Frontier AI Era (July 2026)

Il contesto

Perché tutti parlano di AI? Perché la velocità degli attaccanti è decuplicata.

- Modelli come **Claude Mythos** possono completare autonomamente il *takeover* di un'intera rete aziendale simulata in pochi minuti.
- La velocità della **difesa** deve necessariamente eguagliare quella dell'**offesa** per essere efficace.
- Il vero pericolo oggi risiede nel tempo che intercorre tra l'emissione dell'allarme e l'azione umana; l'AI serve ad **azzerare** questa latenza.
- L’algoritmo non si stanca e non ha bisogno di **vacanze**.

Da notare che i modelli **Frontier** (o **Closed-Weight**) non sono disponibili pubblicamente (attaccanti inclusi). Ma i modelli **Open-Weight** sì (coding, sviluppo di exploit ecc.)



Photo by Jason Rosewell (Unsplash)

I numeri dell’AI nel SOC

No governance

Il **79%** dei SOC utilizza oggi strumenti di AI, ma solo il **36%** li ha integrati in un flusso di lavoro definito. Usi individuali (*Shadow AI*).

Il rischio non è il tool

Il rischio più grande nel SOC non è un cattivo strumento di AI, ma un analista che si fida ciecamente di esso.

Consumo passivo

Il **38%** dei team usa i prodotti AI dei vendor in modalità "out-of-the-box" senza alcuna personalizzazione, né creazione di valore.

Fiducia bassa

I vendor vantano tassi di adozione enormi, ma nascondono il fatto che le decisioni e l'autorità di "chiusura" dell'incidente restano saldamente, e necessariamente, umane.

Fonti: SANS SOC Survey 2026, SOC-CMM Maturity Report 2026, "When Marketing Fails: AI SOC and the curious gap between vendor claims and user experience“ (Anton Chuvakin & Oliver Rochford, Mar 2026).

Il mito dell’Autonomous SOC

Sostituire gli umani con le macchine è una fantasia pericolosa

1.

Rimpiazzare interamente gli umani è irrealistico, perché non si può ritenere **responsabile** un algoritmo per aver spento per errore un server critico.

2.

Usare l'AI ovunque e senza vincoli operativi per generare risposte automatiche (**vibe-coding**) espone l'azienda a rischi inaccettabili.

3.

Nessun SOC maturo permette all'AI di eseguire azioni distruttive (es. isolamento host) senza una validazione umana (**human-in-the-loop** e **human-on-the-loop**).

4.

Entro il 2028 ci sarà il 50% di ingegneri in più rispetto agli analisti; l'AI non taglia il personale, ma ne sposta le competenze (**Gartner**).



L'obiettivo dell'automazione è potenziare gli analisti, non sostituirli.

La soluzione? Il controllo umano

Il futuro dell’analista

L'analista di primo livello non smisterà più allarmi, ma evolverà completamente in un "validatore di casi", con il compito di confermare l'accuratezza delle indagini già svolte dall'AI e fornire *feedback* per migliorarla. Più capacità ingegneristiche.

Il rischio formativo

Automatizzare integralmente le attività di base rischia di privare le nuove leve della "palestra" fondamentale per imparare a valutare l'impatto degli incidenti complessi, introducendo un rischio formativo.

Il giudizio umano

L'AI accelera la raccolta del contesto (*enrichment*), ma durante gli incidenti reali il giudizio umano resta l'unico fattore determinante per l'escalation e la risposta (*mandatory human checkpoints*).

La partnership

Il vero valore dell'MDR moderno sta nell'usare l'AI per estendere lo spettro delle indagini, lasciando agli esperti umani il controllo e la responsabilità delle azioni sul business. (*augmentation over replacement*).

Foto di Diego Jimenez (Unsplash)

Il futuro è una partnership

> *I fornitori che vi dicono che l'AI gestirà il vostro SOC per voi vi stanno vendendo una fantasia. I fornitori che vi dicono che l'AI è solo una moda vi stanno vendendo il passato. Puntate tutto sulla sinergia uomo-macchina.*

Dave Merkel, Co-founder, Expel

Q&A

deda.tech

Venite a trovarci al nostro stand!

Contatti:



giorgio.digrazia@deda.com
https://www.dedatech.com