

[www.infonet.ge.it](http://www.infonet.ge.it)



# CYBERSECURITY INTELLIGENTE: MDR E IA IN AZIONE

**FEDERICO UMBRELLA**  
RESPONSABILE QUALITÀ E MARCHIO  
INFONET S.A.S.

10 Ottobre 2024





**Federico Umbrella**  
**Responsabile marchio e qualità Infonet s.a.s.**





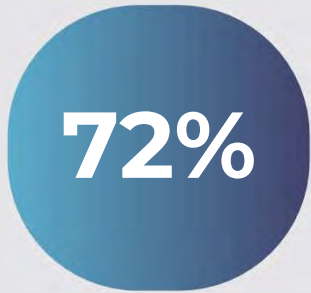
## Chi è INFONET

Infonet nasce dall'idea di semplificare l'accesso alle tecnologie avanzate per le piccole e medie imprese (PMI). In un mondo sempre più digitale, abbiamo visto il bisogno crescente di soluzioni informatiche su misura, che migliorino l'efficienza e riducano i costi operativi. La nostra missione è offrire servizi innovativi, sicuri e scalabili, permettendo alle PMI di competere su un piano tecnologico pari a quello delle grandi aziende. Innovazione, personalizzazione e supporto dedicato sono i pilastri su cui costruiamo il successo dei nostri clienti.

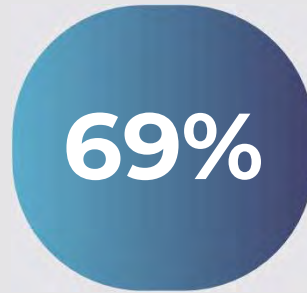




**La cybersecurity è così complessa, così difficile, e si muove così velocemente, che la maggior parte delle organizzazioni non è in grado di gestirla efficacemente in maniera autonoma**



delle organizzazioni  
ha visto un  
incremento nel  
volume/  
complessità/  
impatto dei  
cyberattacchi lo  
scorso anno



dei professionisti IT  
hanno visto il proprio  
impegno contro i  
cyberattacchi  
aumentare nell'anno  
passato



costo medio per la  
decontaminazione da  
attacco ransomware



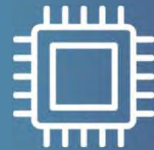




Abilità e  
competenze:

### Persone

- In casa: Ho le giuste competenze e numero di persone per coprire un servizio 24/7/365?
- **Acquisto: Quali skill devo cercare?**



Strumenti tecnologici  
per la cybersec:

### Tecnologia

- In casa: Sono in grado di sincronizzare tutti gli eventi tra tutte le piattaforme che utilizzo?
- **Acquisto: Quali requisiti minimi mi servono?**



Qualità del servizio:

### Processi

- In casa: Cosa posso ottenere con le mie risorse attuali?
- **Acquisto: A quale normativa mi devo adeguare?**





## MDR: Managed Detection and Response

Un servizio attivo 24/7, costituito da esperti specializzati nella ricerca e risposta ai cyber attacchi che le soluzioni tecnologiche da sole non possono prevenire

## Chi è SOPHOS

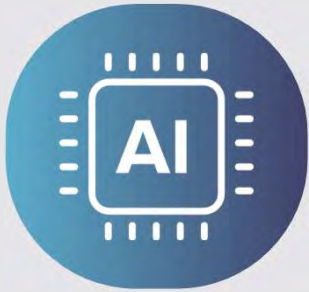
Global leader nella Cybersecurity as a service,  
AI-enabled endpoint, reti, email e cloud security



# SOPHOS







## Threat hunting

Threat Hunting proattivo eseguito da analisti altamente qualificati che scoprono ed eliminano rapidamente più minacce di quelle che i prodotti di sicurezza possono rilevare da soli



## Threat Detection

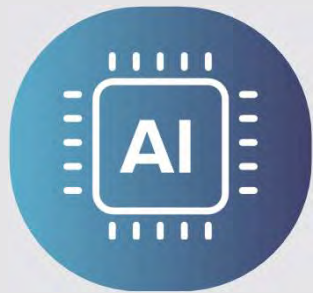
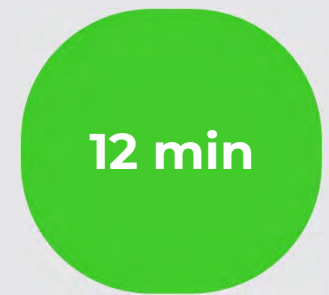
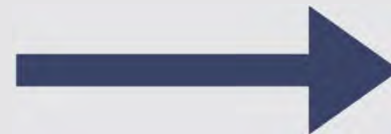
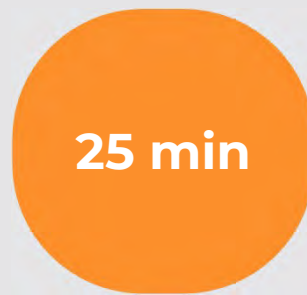
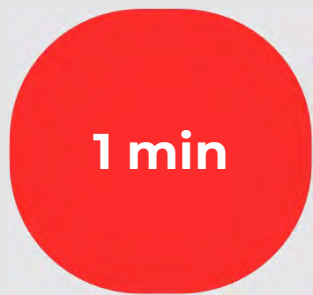
Grazie al XDR (Extended Detection and Response) che rileva minacce note e comportamenti potenzialmente dannosi ovunque risiedano i tuoi dati



## Incident Response

I nostri analisti rispondono alle minacce in pochi minuti, sia che tu abbia bisogno di una risposta agli incidenti su vasta scala o di assistenza per prendere decisioni più accurate

## Tempi medi per la Risoluzione delle Minacce



**Threat hunting**

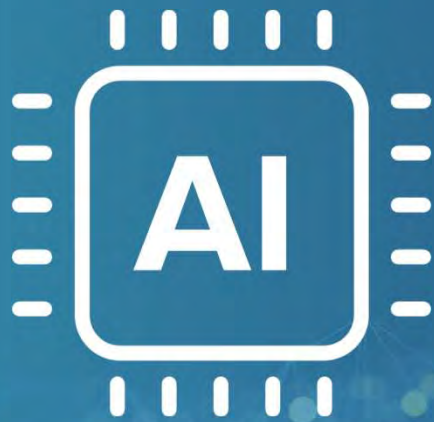


**Threat Detection**



**Incident Response**





**L'intelligenza artificiale è la vera forza trainante dietro l'MDR di Sophos. Utilizza algoritmi di machine learning e deep learning per analizzare grandi volumi di dati in tempo reale, identificando comportamenti sospetti che potrebbero sfuggire ai controlli manuali.**

## Come viene utilizzata l'IA?



### Rilevamento delle minacce avanzate

L'IA permette di rilevare comportamenti anomali, minacce zero-day, e attacchi che altrimenti potrebbero passare inosservati. Grazie al machine learning, il sistema può analizzare milioni di eventi ogni giorno, identificando schemi o attività insolite che potrebbero rappresentare una minaccia.

### Risposta automatica e mitigazione

Grazie alla sua capacità di apprendere continuamente, il sistema può rispondere automaticamente ad alcune minacce. Ad esempio, se viene rilevato un attacco ransomware, l'IA può immediatamente isolare il dispositivo infetto dalla rete per impedire la diffusione dell'attacco.

### Correlazione dei dati e analisi avanzata

L'MDR di Sophos raccoglie dati da endpoint, firewall, e-mail, e altri sistemi di sicurezza. L'IA analizza questi dati insieme per ottenere una visione completa di ciò che sta accadendo nell'intera infrastruttura.



## Cybersecurity as a service





## Costi ridotti

Accesso a tecnologie avanzate di sicurezza senza l'investimento iniziale per infrastrutture costose



## Scalabilità

Servizi adattabili alle esigenze dell'azienda, permettendo di crescere o ridurre le risorse di sicurezza secondo necessità



## Monitoraggio continuo

Protezione 24/7 con interventi tempestivi grazie a monitoraggio e gestione costante delle minacce



## Esperti specializzati

Accesso a team di esperti senza necessità di assunzioni o formazione interna



## Aggiornamenti costanti

Soluzioni sempre aggiornate contro le minacce più recenti, garantendo una protezione efficace e attuale



## Esempio pratico di intervento dell'MDR

Un esempio recente è stato il rilevamento di un attacco ransomware in un'azienda manifatturiera di medie dimensioni. Gli aggressori avevano compromesso un server interno e stavano preparando la distribuzione del ransomware attraverso la rete. Grazie al sistema AI di Sophos, il comportamento sospetto è stato immediatamente identificato come anomalo. La rapidità della risposta è stata determinante: in pochi minuti, il team MDR ha isolato la minaccia, impedendo che il ransomware si diffondesse su tutti i sistemi critici. In questo caso, senza l'intervento congiunto dell'IA e degli esperti di sicurezza, i danni avrebbero potuto paralizzare le operazioni dell'azienda per giorni o settimane, con costi elevati in termini di tempo e denaro.



**GRAZIE PER  
L'ATTENZIONE**

**INFONET S.A.S.**

Indirizzo	Via Armando Diaz 1/18
Telefono	+39 010 857 0207
Email	info@infonet.ge.it
Web	www.infonet.ge.it



[www.infonet.ge.it](http://www.infonet.ge.it)

