

>\_apt/get.defence

# Spectre SOC

**Le persone giuste, a  
proteggere il tuo business  
24/7**



>\_apt/get.defence

# Chi siamo

>\_apt/get.defence

**AptGetDefence** è un'azienda di consulenti in cybersecurity specializzata in servizi di sicurezza gestiti, attività offensive, difensive, forensi e GRC.



**Spectre** è il nostro **Security Operation Center as a Service**: un team di analisti reali, non solo strumenti, che monitora, investiga e risponde alle minacce per conto tuo.

Azienda certificata **ISO/IEC 27001** e **ISO 9001** con sede alle porte di Venezia.

# Il vero problema non è la tecnologia

Quasi tutte le aziende hanno già firewall, antivirus, EDR. Il problema è un altro.

## Quello che manca davvero

- Non c'è nessuno che guardi gli alert **alle 3 del mattino**
- Trovare, formare e trattenere analisti esperti è **difficile e costoso**
- Gli attacchi non rispettano l'orario d'ufficio
- Un alert ignorato per giorni è la differenza tra un incidente gestito e una violazione

## La conseguenza

Gli strumenti da soli producono **segnali**, non **decisioni**. Servono competenze umane per trasformare un log in un'azione corretta, al momento giusto.

Non servono altri tool. Serve un team che sappia leggere tra le righe.

# La nostra risposta: Spectre SOC

Non solo MDR. Spectre è un XDR technology-agnostic, gestito interamente dal nostro team: raccoglie segnali da qualsiasi fonte, non solo dall'endpoint, e li trasforma in risposta reale.

## Cosa facciamo

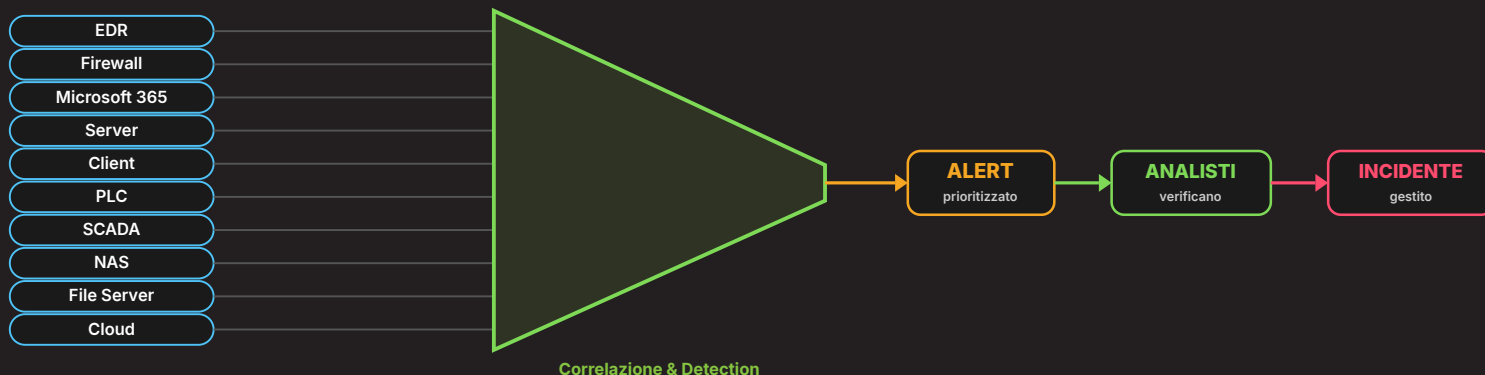
- Ingestion multi-sorgente: endpoint, cloud, rete, OT, senza vincoli di vendor
- Monitoraggio attivo H24, 7 giorni su 7
- Analisi e triage degli alert da parte di analisti reali
- Gestione completa degli incidenti (IR)
- Portale dedicato con visibilità totale sulle attività

## Cosa ottieni

- Non devi assumere, formare o trattenere un team SOC
- Nessun lock-in tecnologico: ci integriamo con lo stack che hai già
- Rilevamento immediato, non "quando qualcuno se ne accorge"
- Tracciabilità completa di ogni alert e ogni decisione

# Un XDR technology-agnostic

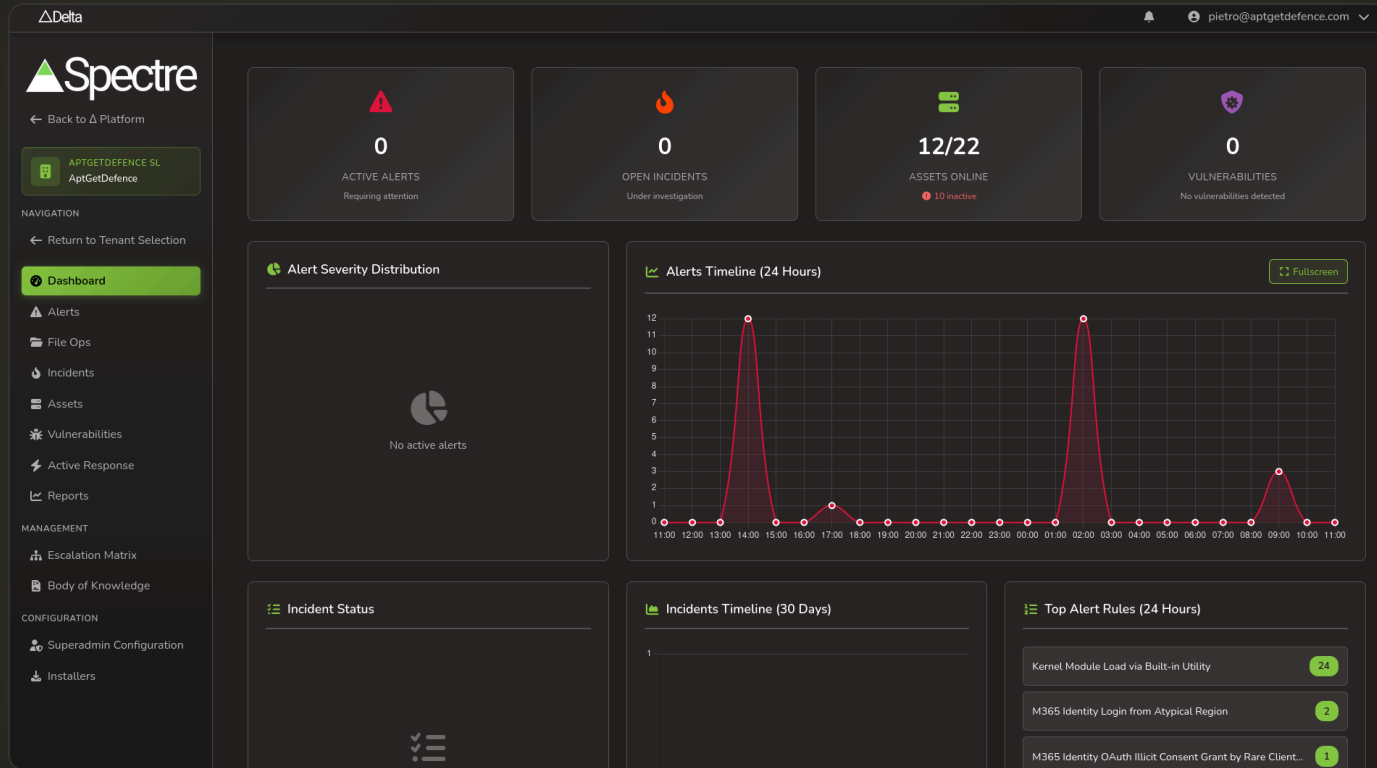
Qualunque sia la tua infrastruttura, Spectre la ascolta. Tutte le fonti confluiscono in un'unica pipeline di correlazione, e dall'altra parte escono alert ad alta affidabilità, verificati dai nostri analisti.



Endpoint, cloud, rete, industriale: qualsiasi fonte, qualsiasi vendor. Meno rumore in ingresso, solo incidenti reali in uscita.

# Delta Platform: la tua finestra sul SOC

Non ti chiediamo di fidarti sulla parola. Questa è la dashboard reale che i nostri clienti usano ogni giorno.



# Il nostro vero vantaggio competitivo: le persone

Chiunque può comprare un SIEM. Non chiunque sa usarlo bene.

## Come è organizzato il nostro team

- **Analisti L1**, monitoraggio continuo e triage degli alert
- **Analisti L2**, investigazione approfondita e gestione incidenti
- **SOC manger**, coordina i team, gestisce i clienti e coordina la risposta in caso di incidenti di sicurezza

## Perché conta per te

Ogni alert che arriva sul tuo ambiente passa attraverso persone che **sanno riconoscere un vero attacco**, non solo software che genera notifiche.

Meno falsi allarmi. Meno rumore. Risposte più rapide su ciò che conta davvero.

# Come lavoriamo: non solo monitoraggio

## Operazioni centralizzate

- Un'unica control room, un'unica visione su tutti gli alert
- Processo di risposta agli incidenti **definito e ripetibile**
- Automazione (SOAR) per ridurre i tempi di intervento manuale

## Protezione a 360°

- Perimetro e rete, ogni host, Linux, Windows, macOS
- Dispositivi mobili, Android e iOS
- Dispositivi IoT/OT, sensoristica building e industriale
- Dati e applicazioni

Servizio modulare e livelli personalizzabili: ti proteggiamo dove e come ne hai davvero bisogno.

# La tecnologia amplifica le competenze, non le sostituisce

| Ambito              | Cosa gestiamo per te                                     |
|---------------------|----------------------------------------------------------|
| Endpoint Protection | Antivirus e agenti EDR di nuova generazione              |
| AI                  | Arricchisce gli alert dando contesto agli analisti       |
| Vulnerabilità       | Inventario sulle vulnerabilità passive dei dispositivi   |
| SIEM & SOAR         | Motore di detection e playbook di risposta automatizzata |
| Gestione incidenti  | Piattaforma dedicata per alert e reportistica            |

Location e residenza dei dati GDPR compliant **Data Center Park Falkenstein, Germany** con retention a 90 giorni

# SLA di esempio

Un impegno chiaro su tempi di presa in carico e gestione, per livello di severità.

| Severità | Presa in carico | Escalation / Chiusura           |
|----------|-----------------|---------------------------------|
| Critica  | 15 minuti       | Escalation entro 30 minuti      |
| Alta     | 30 minuti       | Chiusura/escalation entro 1 ora |
| Media    | 2 ore           | Chiusura entro 4 ore            |
| Bassa    | 8 ore           | Gestita entro il turno          |

Valori indicativi, basati sui nostri standard operativi interni

# Perché scegliere Spectre

## Competente

Analisti esperti dietro ogni alert, non solo automazioni

## Completo

Intercetta e risponde a ogni tentativo di intrusione

## Veloce

Attivazione rapida, protezione da subito

## Flessibile

Servizi combinabili sulla tua reale esigenza

## Affidabile

Team qualificato, processi tracciabili e verificabili

## Trasparente

Visibilità completa su ogni attività, sempre

Le organizzazioni con una capacità di incident response strutturata risparmiano in media **1,49 milioni di dollari per violazione** rispetto a chi non ce l'ha.

— IBM Cost of a Data Breach Report

# Come iniziare

Dal contratto all'operatività: il tuo SOC entra in servizio così, e da lì, non si ferma mai.



>\_apt/get.defence

**Parliamone**

>\_apt/get.defence

**Spectre SOC, competenza, prima di tutto**

customer@aptgetdefence.com · [www.apptgetdefence.com](http://www.apptgetdefence.com)

AptGetDefence · Spectre SOC