



Proteggere l'intero ecosistema




XYLER protegge l'ecosistema di End-Point e, in aggiunta, anche l'ambiente collaborativo Cloud based MS365/GWS. Si basa sul Framework proprietario AIR al fine di implementare un **sistema interamente gestito**.

## OBIETTIVI

Proteggere gli end-point, integrandosi con la soluzione **EDR Cybereason** su tutti i nodi della rete.

## VANTAGGI

 **Protezione ambienti cloud**  
Office 365 e Google  
Workspace

 **Protezione End-point**

 **Intercettazione immediata**

 **SOC 24/7**

### Caratteristiche

EDR Evoluto (con AI)	Piattaforma Chronicle <b>SIEM</b> per raccolta dei Log
Chronicle <b>SOAR</b> per orchestrazione automatica e risposta	SOC con team di analisti Cyber 365/7/24
Gestione incidenti definita in anticipo	Risposta immediata agli attacchi

## FOCUS

Xyler è creato per intercettare **immediatamente** qualunque tipo di attacco informatico sui tuoi endpoint e sulla tua **piattaforma Cloud**.

Il nostro SOC (Security Operation Center) analizza e risponde tempestivamente alle minacce in atto H24 7/7.

## CONTATTACI

**SOC Cyber Defense SA**

091 611 70 00

[info@soccd.swiss](mailto:info@soccd.swiss)

**[WWW.SOCCD.SWISS](http://WWW.SOCCD.SWISS)**

Via Cantonale 23c, 6928 Manno  
Ticino (CH)

# Caratteristiche tecniche



## PROTEZIONE COMPLETA



### DETECTION

Si basa sul monitoraggio dell'EDR e **sull'analisi dei Log** raccolti dal **SIEM** da parte del nostro team del SOC (Secure Operating Center). Ogni segnalazione di anomalia e di possibile minaccia o attacco informatico, viene così gestita dagli esperti per valutare il passaggio alla fase di **Response**



### RESPONSE

Risposta **immediata** fino all'isolamento del singolo Endpoint per prevenire qualsiasi diffusione di programmi malevoli: malware, ransomware e altre minacce che possono portare al **blocco dell'operatività** aziendale.



### INCIDENT MANAGEMENT

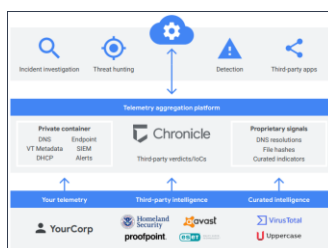
Il processo di Incident Management è **definito all'inizio** della fruizione del servizio Xyler. Con il cliente si concorda la **tipologia di risposta** alle minacce e le regole di ingaggio per un servizio personalizzato e adatto alle singole esigenze.

## TECNOLOGIE PORTANTI



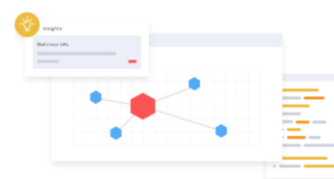
### EDR

EDR (Endpoint Detection and Response) è una tecnologia di sicurezza che monitora continuamente i dispositivi endpoint per rilevare, analizzare e rispondere automaticamente a minacce informatiche avanzate, spesso invisibili agli strumenti tradizionali



### CHRONICLE SIEM

La piattaforma scalabile dove convoglia tutta la telemetria/eventi di sicurezza, inclusi dati di tipo corporate, normalizzandoli tramite il framework Unified Data Model (UDM),



### CHRONICLE SOAR

Una soluzione cloud di Google che automatizza e coordina la risposta agli incidenti di sicurezza, integrando fonti come SIEM, threat intelligence e strumenti di analisi per migliorare l'efficienza operativa del SOC e ridurre i tempi di reazione.

Il servizio Xyler è **flessibile e adattabile** alle singole esigenze. La completezza della configurazione tecnica e la presenza del SOC, senza sosta, ogni giorno dell'anno, ne fanno uno strumento **potente e affidabile** per la propria cybersicurezza.