Scheda tecnica

Servizio XYLER

SOC Cyber Defense SA, Via Cantonale 23c, CH 6928 Manno
T +41 91 611 70 00, info@soccd.swiss - www.soccd.swiss

1. *Descrizione generale*

Il servizio denominato XYLER protegge l'ecosistema End Point e, in aggiunta, l'ambiente collaborativo Cloud based MS365/GWS.

La proposta tecnologica si basa sulla piattaforma di CSS a supporto del framework proprietario Autonomic Incident Response (AIR) per l'implementazione di un sistema eXtended Detection & Response - XDR:

- Google Chronicle SOAR – Security Orchestrator Automation Response (SOAR)
- Google Chronicle SIEM – Autonomic Security Datalake (SIEM)
- Cybereason EDR-NGAV – Endpoint Detection and Response (EDR)

Relativamente al prodotto per la protezione degli End Point, si integrerà la soluzione Cybereason EDR o in altro su tutti i nodi della rete che permettono questa possibilità.

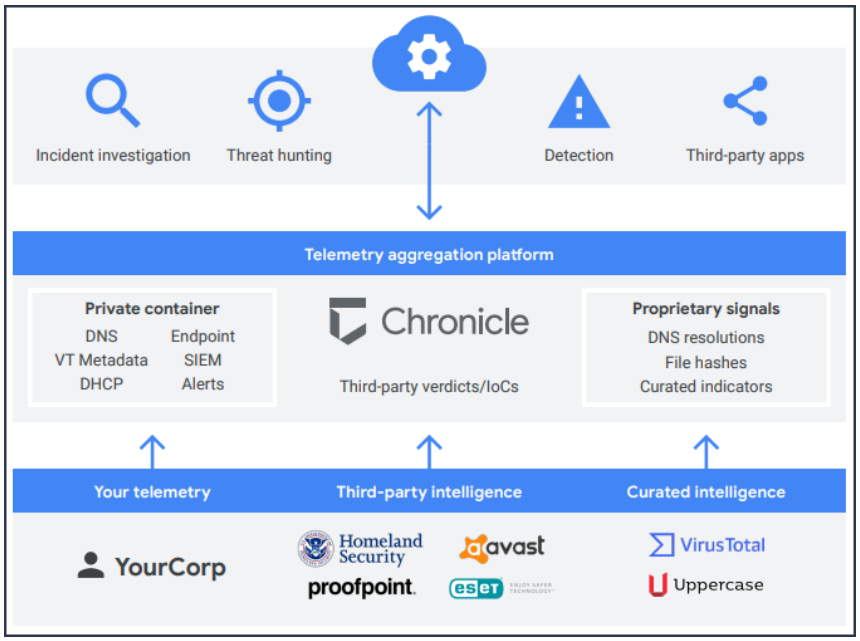
2. *Descrizione prodotti e funzionalità*

2.1 Chronicle SIEM

Chronicle è un SIEM di nuova generazione, completamente sviluppato in SaaS, disegnato per il mondo entreprise e specializzato nella raccolta, gestione ed analisi di grandi mole di dati di sicurezza e di rete.

Lo scopo principale di Chronicle è quello di offrire una piattaforma nella quale convogliare tutta la telemetria/eventi di sicurezza, in maniera scalabile: il modello, infatti, prevede la possibilità di includere qualsiasi dato di tipo corporate, e normalizzarlo tramite il framework interno denominato **Unified Data Model (UDM)**, rendendolo disponibile live per **12 mesi di retention**.

L'UDM consente di normalizzare tutti i metadati generati dalle telemetrie in modo che sia le regole di detection, sia le query di investigation & threat hunting possano essere effettuate in maniera agnostica alle tecnologie sottostanti.



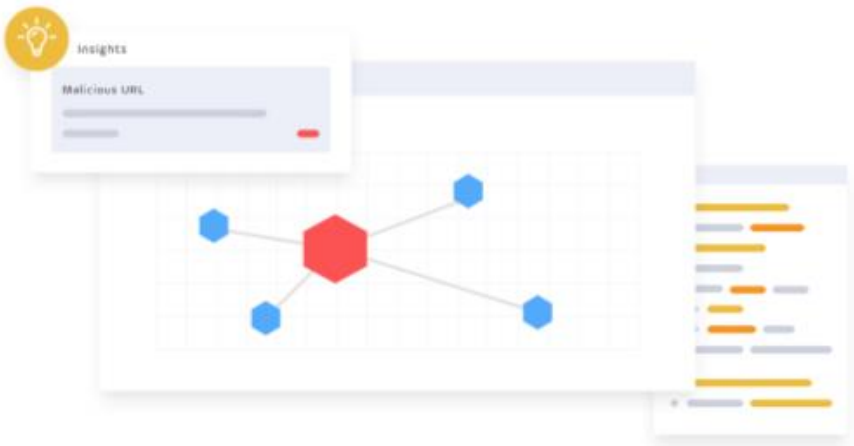
Analisti possono concentrarsi sulle attività di Cyber Security senza dover tenere in considerazione le necessita di scalabilità che queste piattaforme solitamente richiedono: è Google, infatti, che garantisce la scalabilità del layer tecnologico sottostante.

Chronicle, inoltre, offre **capabilities di matching di IoC automatico** (direttamente sugli eventi, non solo sugli allarmi derivanti dalle rule) tramite la possibilità di agganciare Curated/3rd parties intel

2.2 Chronicle SOAR

Chronicle SOAR è uno strumento di Security Orchestration, Automatino & Response che offre le seguenti features peculiari:

- **Case Management & Alert Normalization:** possibilità di collezionare, raggruppare, normalizzare le informazioni derivanti gli allarmi delle tecnologie di sicurezza, garantendo una minore proliferazione di casi da gestire e una correlazione tra sistemi di sicurezza.
- **Playbooks & Enrichment:** creazione di procedure automatizzate e integrate a molteplici tecnologie di sicurezza, per automatizzare ed efficientare task di triage e context enrichment, nonché response sui sistemi target
- **Collaboration & Investigation:** tramite l'utilizzo di utenze collaborative, è possibile avere una nuova esperienza di comunicazione MSSP – Cliente, che può prevedere il coinvolgimento e l'ingaggio puntuale del cliente direttamente su casi importanti e prioritarie.
- **Use Cases & Out Of The Box Integrations**: offre oltre cento integrazioni Out of the Box che permettono di essere installate e configurate in pochi istanti grazie al market place



2.3 Cybereason EDR

Cybereason è una soluzione di Endpoint Detection and Response (EDR) che si distingue per le sue eccezionali capacità di rilevamento e risposta alle minacce informatiche. Nelle valutazioni MITRE ATT&CK del 2024, Cybereason ha ottenuto risultati straordinari, tra cui:

- **Rilevamento del 100% delle minacce:** ha identificato con successo tutti i 79 passaggi di attacco associati a Clop, LockBit e minacce DPRK, senza generare falsi positivi.
- **Visibilità completa:** ha fornito una mappatura completa al framework MITRE ATT&CK, offrendo trasparenza totale sulle tattiche, tecniche e procedure (TTP) degli avversari.
- **Precisione del 100%:** nessun falso positivo in 20 scenari, dimostrando l'affidabilità e l'accuratezza della piattaforma.
- **Efficienza del SOC al 100%:** ha generato solo 18 avvisi critici o di alto livello, il numero più basso tra tutti i fornitori partecipanti, garantendo una risposta agli incidenti più efficiente per i Security Operations Center.

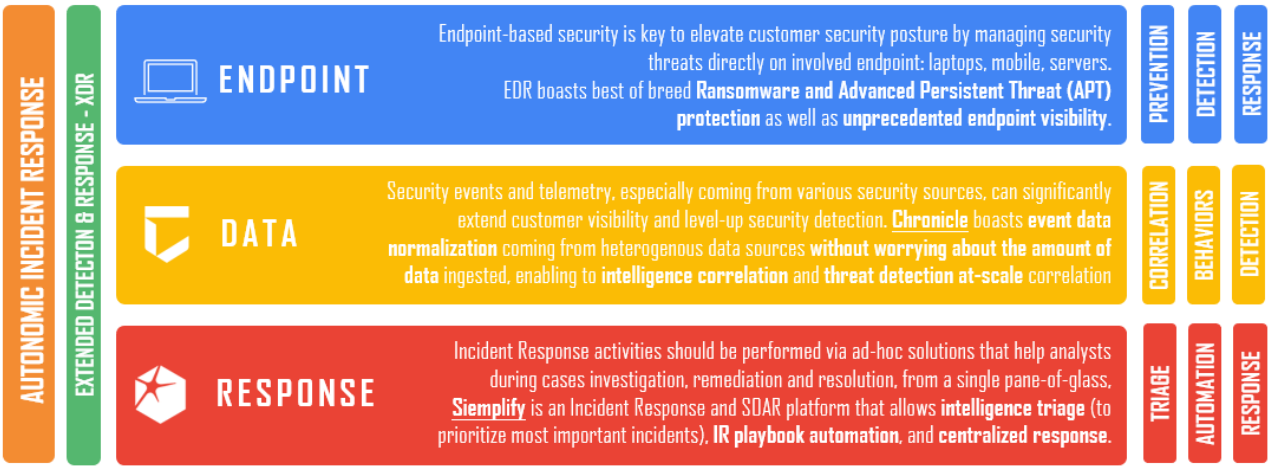
Questi risultati evidenziano come Cybereason offra una protezione avanzata e immediata per ambienti Windows, Linux e macOS, senza necessità di configurazioni aggiuntive. La piattaforma è progettata per identificare rapidamente le minacce con un alto grado di accuratezza, utilizzando l'analisi comportamentale e correlazioni tra diversi endpoint in tempo reale.

Inoltre, Cybereason consolida le informazioni su ogni attacco in una "Malop" (operazione malevola), fornendo una visione contestualizzata e dettagliata dell'intera sequenza di un attacco. Ogni Malop organizza i dati rilevanti in un'interfaccia grafica interattiva e di facile lettura, offrendo una timeline completa, il flusso dell'attacco nella rete e qualsiasi comunicazione malevola.

In sintesi, Cybereason si afferma come una soluzione EDR di alto livello, capace di fornire una protezione efficace e una visibilità completa sulle minacce, come dimostrato dalle eccellenti performance nelle valutazioni MITRE ATT&CK.

2.4 *Servizio Managed Detection & Response*

Il servizio Managed Detection & Response prevederà monitoraggio, notifica e response di eventi di sicurezza in modalità 365x7x24h attraverso l'utilizzo del seguente stack tecnologico:



- *Framework (AIR): Copertura detection tramite mapping tecniche framework MITRE ATT&CK e applicazione framework proprietario di Autonomic Incident Response, in grado di identificare e qualificare gli allarmi provenienti dalle telemetrie dei sistemi/tecnologie del cliente in perimetro*
- *SOAR / Incident Response - (owner tenant MSSP)*
- *SIEM / Security Data Lake- (owner tenant MSSP)*
- *Sistema EDR Cybereason*

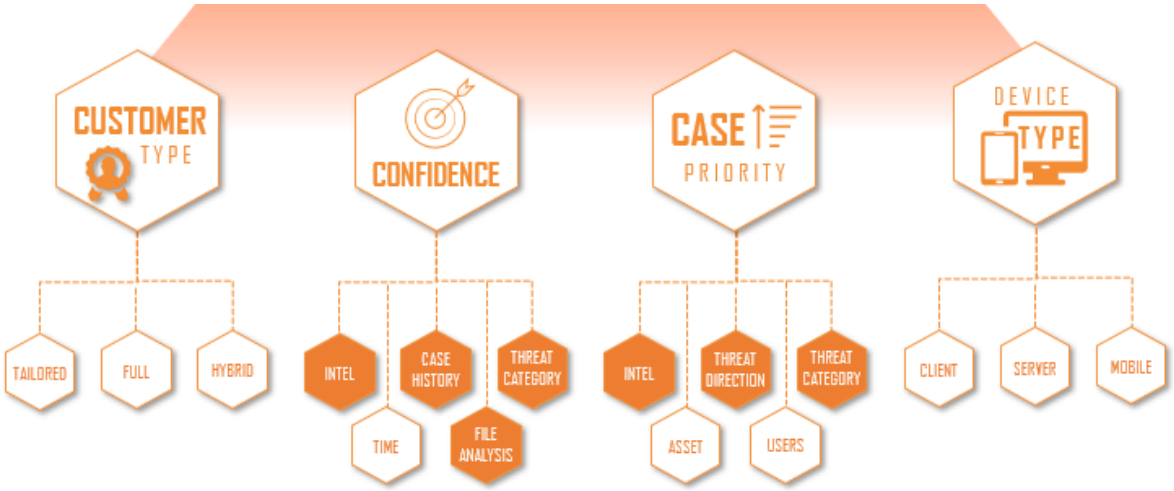
Il Servizio XDR dal SOC verrà erogato da remoto.

2.5 *Metodologia – AIR*

Il primo obiettivo durante l'analisi di un Caso riguarda la valutazione del contesto degli eventi in esso contenuti. Il Framework proprietario si propone di normalizzare le caratteristiche di un Case in maniera da efficientare la prima Response.

Tale Framework si chiama AIR – Autonomic Incident Response, e permette di:

- *Evitare l'incertezza durante la risposta*
- *Ridurre il livello di falsi positivi*
- *Definire un approccio modulare adatto a diversi livelli di clienti*



L'AIR Framework si basa sull'utilizzo di 4 dimensioni (Tipo di Cliente, Fiducia, Priorità del caso, Tipo di dispositivo) definite nel modo più analitico e deterministico possibile, con l'obiettivo di avere parametri normalizzati e informazioni oggettive che possano essere utilizzate per prendere decisioni durante le fasi di risposta agli incidenti.

2.6 Tipo di Monitoraggio

Il servizio di Managed Detection & Response verra' erogato **da Team di Analisti Cyber Tier-1 e Tier-2** qualificati che gestiranno il monitoraggio dei Casi (come da SLA descritte nel capitolo dedicato) direttamente dalla piattaforma MSSP Siemplify, sulla quale un Environment dedicato al Cliente (all'interno della piattaforma) sarà istanziato e configurato con playbook ed integrazioni dedicate al Cliente.

L'istanza di Chronicle, così come la tecnologia EDR, saranno utilizzate da Analisti Tier-1 e Tier-2 per effettuare investigazioni di tipo mirato e threat hunting.

All'individuazione di un Caso di tipo Incident, il servizio prevede 3 tipologie di interazione principali con il Cliente, nessuna delle quali esclude le altre:

- **Notifica:** invio notifica di individuazione di un nuovo incidente, tramite mail (o direttamente in Siemplify nel caso il Cliente abbia una utenza collaborativa e lo desideri)
- **Response:** attività di risposta all'incidente che può scaturire immediatamente all'individuazione di un threat o successivamente ad una conferma del Cliente (da discutere e definire nel documento di ingaggio - Rule of Engagement) ad avvio servizio
- **Chiamata:** chiamata telefonica di escalation verso il reperibile/responsabile del Cliente, oppure chiamata telefonica per informare che specifiche Response con significativo impatto su uno o più utenti sono state intraprese (da discutere e definire nel documento di ingaggio - Rule of Engagement)

Un report dettagliato di quanto è stato gestito ed individuato (incidenti, comportamenti anomali, …) verrà inviato periodicamente al personale indicato dal Cliente all'interno del documento di ingaggio "Rule of Engagement".

2.7 Tipo di Response

Durante l'erogazione del servizio, gli analisti saranno in grado di rispondere ad allarmi o incidenti seguendo un processo di notifica e response definito, condiviso e sottoscritto dal Cliente, che prevede specifiche tipologie di risposta definite nel documento "Rules of Engagement".

2.8 Service Level Agreement

Il servizio proposto è di tipo H24 con una copertura di 365 giorni/anno.

Priorità	Presa in carico	Azioni possibili	Esempi
Critical	1 h	Notifica/ Risposta / Chiamata	Sistema(i) critico(i) compromesso(i) con possibile esfiltrazione di dati. Sistema Mission Critical attaccato.
High	4 h	Notifica/ Risposta / Chiamata	Asset confermati o molto probabilmente compromessi. Nessun sistema Mission Critical coinvolto. I dati sensibili si trovano nei sistemi colpiti.
Medium	8 h	Notifica/ Risposta	Nessun sistema critico compromesso. Pochi o nessun dato sensibile si trova su di esso (probabilmente si tratta di un endpoint del cliente, come un desktop, un portatile, ecc.)
Low	1 Giorno Lavorativo	Notifica	Sono state identificate attività o comportamenti sospetti di utenti/asset, che possono essere sintomo di fasi preliminari di attacco (accesso iniziale, Recon). I sistemi coinvolti non sono critici e molto probabilmente sono client. Identificazione di PUA (Potential Unwanted Software) sui sistemi, da verificare con il cliente.
Info	1 Giorno Lavorativo	Notifica	Identificazione di potenziali vulnerabilità, percorsi di attacco, file obsoleti o pericolosi non ancora utilizzati per lo sfruttamento o l'attacco. Il cliente riceverà una notifica e un suggerimento su come procedere alla bonifica dell'applicazione/degli asset.

3. Descrizione del Modello Progettuale

INFRASTRUCTURE BUILDUP	Activity	Requirements
Attivazione XYLER	- Installazione, Configurazione e Connessione dell'ambiente EDR Cybereason con il backend SOAR del SOC - Connessione dell'istanza O365/GWS nell'istanza SIEM del SOC - Attivazione del monitoraggio come descritto nei paragrafi successivi	Disponibilità di un referente tecnico del Cliente
Milestone	Ambiente Cloud EDR e SAAS Collaborativo O365/GWS e EDR integrato nel backend del SOC	
Deliverables	Attivazione servizio XYLER	

MDR SERVICE ACTIVATION

Le attività necessarie per l'attivazione dei prodotti e dei servizi hanno una durata stimata di circa 3 giorni lavorativi