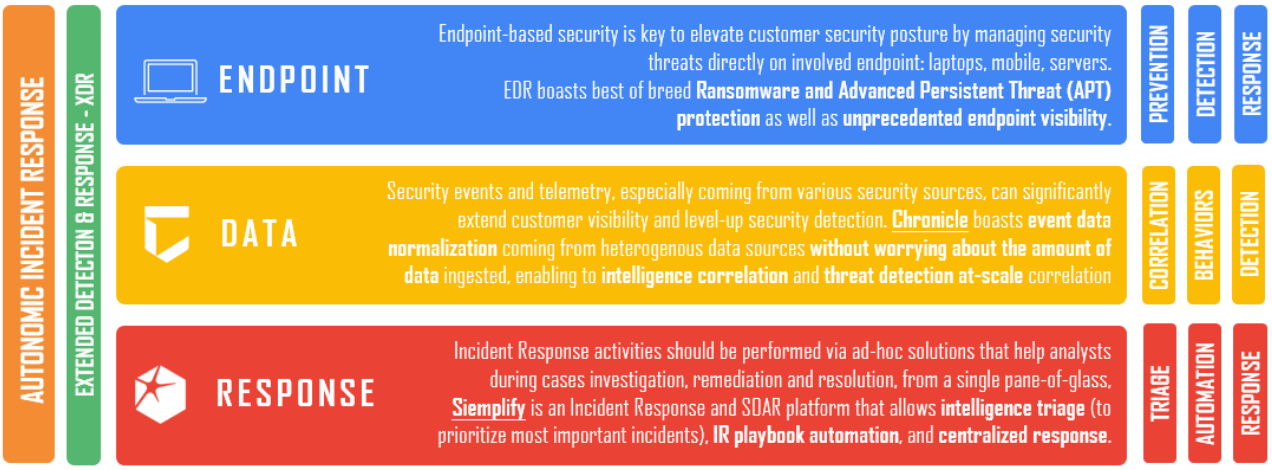
# *Scheda tecnica*

# *Servizio MDR Managed Detection & Response*

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

## 1. Descrizione prodotti e funzionalità

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*

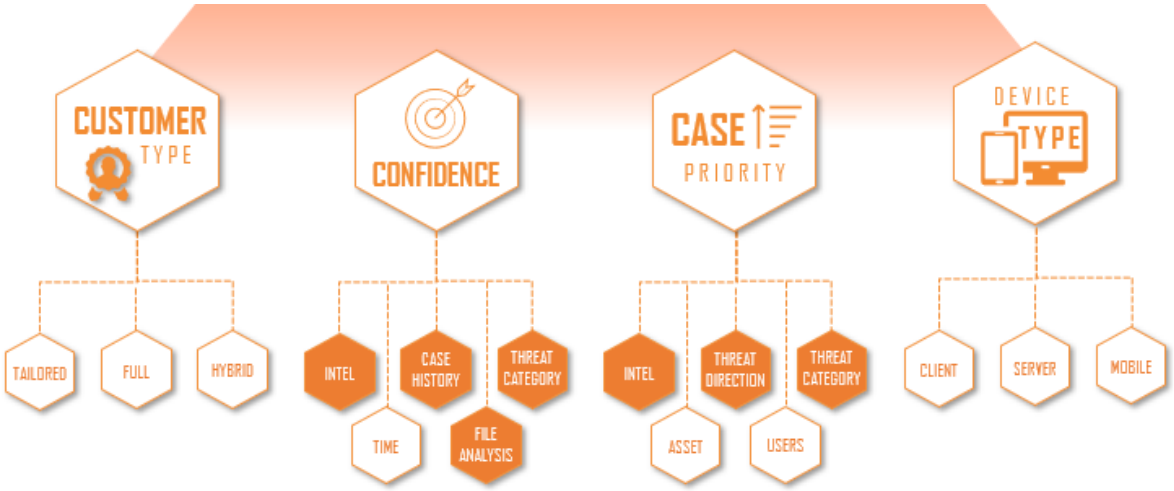
Il Servizio XDR dal SOC verrà erogato da remoto.

### 1.1 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.

### *1.2 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".

### *1.3 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".

### *1.4 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.<br>I dati sensibili si trovano nei sistemi colpiti. |
| **Medium** | 8 h | Notifica/ Risposta | Nessun sistema critico compromesso.<br>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.<br>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. |