MDR Managed Detection & Response

Protezione completa 365 giorni l'anno

Il servizio Managed Detection & Response prevede il monitoraggio, notifica e risposta a eventi di sicurezza in modalità 365x7x24h attraverso l'utilizzo di tecnologie d'avanguardia.

OBIETTIVI

Gestione dei rischi e degli allarmi, in maniera gestita, con un team di analisti dedicati ed esperti che rispondono ai casi e adottano misure di risposta.

VANTAGGI

- Team analisti cyber dedicati
- Ambiente creato ad-hoc
- Risposta attiva agli attacchi
- Rapido intervento
- Reportistica specifica

Caratteritiche	
Framework AIR proprietario	Servizio EDR dal SOC erogato da remoto
Team analisti cyber su due livelli	Tre tipologie di interazione
Reportistica dedicata e programmata	EDR Cybereason

FOCUS

Servizio di sicurezza gestito che combina **monitoraggio h24**, rilevamento avanzato e risposta rapida alle minacce. Unisce tecnologie di difesa e analisi umana esperta per proteggere reti, endpoint e cloud in tempo reale. Ideale per aziende che vogliono **cyber resilienza** senza gestire un SOC interno.

CONTATTACI

SOC Cyber Defense SA
091 611 70 00
info@soccd.swiss
WWW.SOCCD.SWISS
Via Cantonale 23c, 6928 Manno
Ticino (CH)

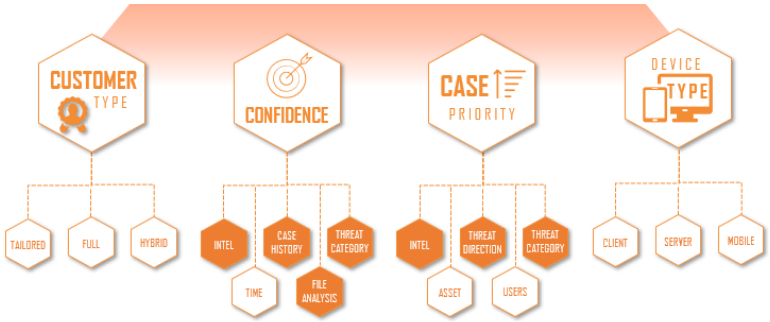
Caratteristiche tecniche

STACK TECNOLOGICO COMPLETO

- ❑ **Framework (AIR):** Copertura e detection tramite mapping con tecniche MITRE ATT@CK e applicazione framework proprietario di **A**utonomic **I**ncident **R**esponse, in grado di identificare e qualificare gli allarmi provenienti dalle telemetrie dei sistemi del cliente.
- ❑ Chronicle **SOAR** e **SIEM** per «incident response» e «security data lake»
- ❑ Sistema **EDR:**
  - **Defender:** protezione integrata con l'ecosistema Microsoft 365 Premium
  - **Cybereason:** con intelligenza artificiale e visibilità profonda per una risposta rapida e autonoma alle minacce
- ❑ Servizio **XDR con SOC** erogato da remoto

METODOLOGIA AIR:

Il framework AIR (Autonomic Incident Response) permette di evitare l'incertezza durante la risposta, riduce il numero di falsi positivi, possiede un approccio modulare.



BASATO SU 4 DIMENSIONI:

Tipologia di cliente, confidenza, priorità del caso, tipo di dispositivo; parametri definiti in modo analitico e deterministico, con l'obiettivo di prendere decisioni solide durante la gestione degli incidenti.

TIPO DI MONITORAGGIO E RISPOSTA

L'incidente e il servizio MDR viene gestito da team di analisti Livello 1 e Livello 2. L'istanza Chronicle e la tecnologia EDR permette di agire in maniera mirata sul caso e prevede tre tipologie di interazione.

Notifica

Invio notifica di individuazione incidente via:

- Mail
- Piattaforma Siemplify

Chiamata

- Chiamata di escalation verso il responsabile lato cliente
- Chiamata telefonica di informazione su specifiche response intraprese

Response

Risposta immediata all'incidente tramite:

- Individuazione di una minaccia
- Conferma da parte del cliente

Report

Report periodico dettagliato sulla gestione di:

- Incidenti
- Comportamenti anomali
- Avvenimenti di sicurezza

Il servizio gestito **MDR è una protezione attiva h24 con rilevamento avanzato**, analisi esperta e risposta immediata alle minacce. Sicurezza gestita, efficace e scalabile.