CYBERFERO

# SOC as a Service [EDR]

## La soluzione per unificare e automatizzare la sicurezza.

SOCaaS [EDR] è il servizio che sgrava la tua azienda da tutta la gestione delle minacce incombenti.
Un servizio a 360° attivo-passivo che include:

- Monitoraggio
- Analisi e controllo
- Prevenzione e rilevamento degli attacchi
- Taratura costante in base agli eventi
- Aggiornamenti su tutte le nuove minacce

www.cyberfero.com

# Come funziona SOC as a Service ?

## Agenti

Vengono installati gli agenti software su tutti gli Endpoint.

## Configurazione

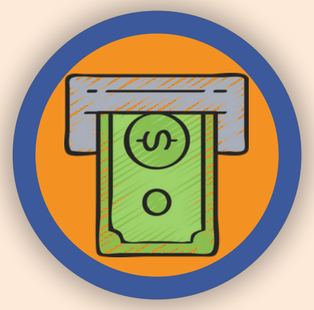
Vengono configurati su misura in base alle caratteristiche dell'infrastruttura.

## Attivazione

Gli agenti si attivano e iniziano il loro lavoro di raccolta e alert.

## Azione passiva

Gli agenti bloccano le minacce conosciute e arricchiscono i log.



## Azione attiva

Le minacce più importanti generano un alert al nostro Staff che interviene attivamente per risolvere il problema.

## Sicurezza assicurata

In conclusione, la migliore soluzione passiva-attiva.

# Cos'è un SOC

Un SOC, acronimo di Security Operations Center, è un team di esperti dedicato a proteggere le organizzazioni dagli attacchi informatici.

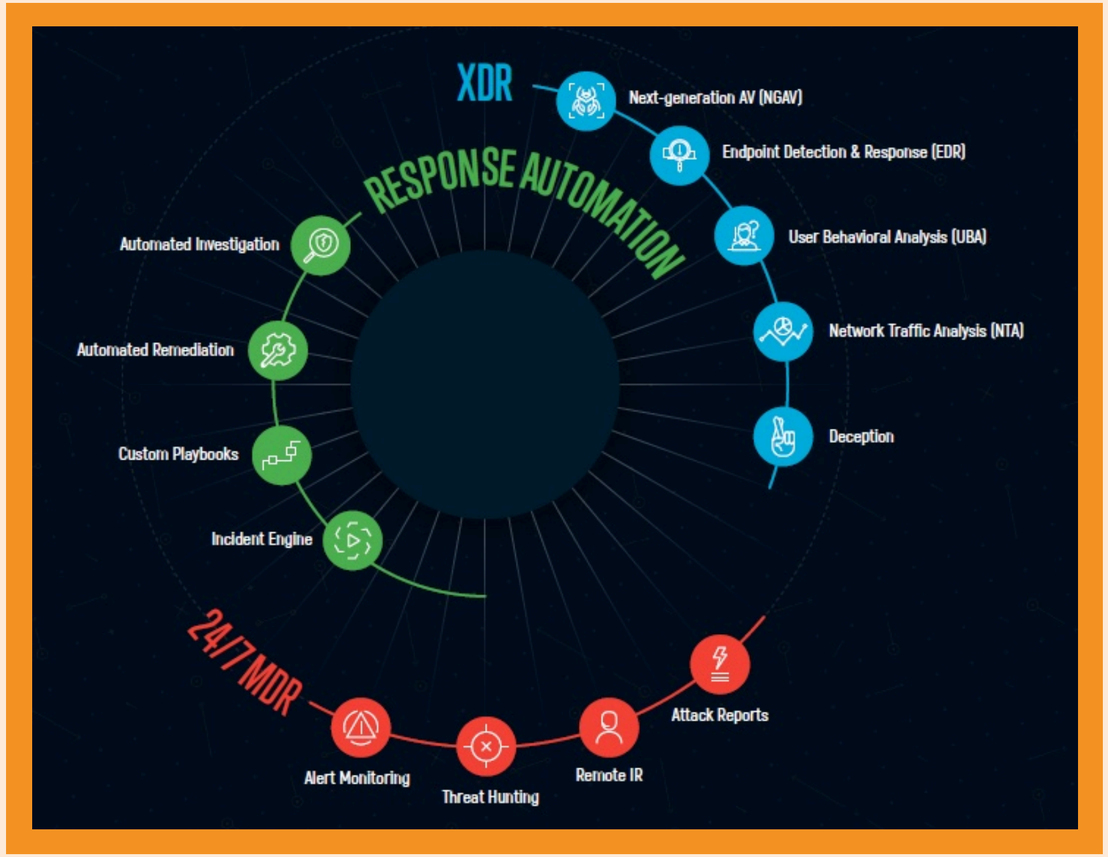
**Immagina il SOC come una simbiosi di:**

## Implementazioni tecniche

Come analisi dei log, intelligenza artificiale, aggiornamenti costanti.

## Staff Esperto

Che interviene ad hoc quando la minaccia richiede un reale intervento.




# Cosa può fare un SOCaaS per la tua azienda

Il nostro sistema “SOC as a Service” integra diverse modalità di intervento per abbattere le minacce.
L’unione di implementazioni tecniche e personale reale crea un sistema di sicurezza che migliora nel tempo e che si adatterà ai tipi di minacce che la tua azienda può subire.

# Le principali funzionalità

## VALUTAZIONE DELLE VULNERABILITÀ

Il rilevamento e l'applicazione di patch per gli aggiornamenti di sicurezza mancanti vengono eseguiti regolarmente e riducono in modo significativo l'esposizione al rischio degli exploit standardizzati

## MONITORAGGIO DELL'INTEGRITÀ DEI FILE

Ideale per un ambiente chiuso e deterministico. Qualsiasi cambiamento di stato dei file notoriamente privi di minacce viene segnalato immediatamente all'attenzione dell'operatore da un avviso.

## GESTIONE DELL'INVENTARIO

Una visibilità granulare e il reporting di tutte le entità in uscita – host, software installato, ecc. – sono fondamentali per varie esigenze di sicurezza e gestione IT.

## RACCOLTA E CONSERVAZIONE DEI LOG

La conservazione dei registri per un periodo di tempo illimitato consente alle organizzazioni di conformarsi a vari requisiti normativi

## VISTA A 360° CON AVVISI

Visualizzazione immediata dello stato di attività delle minacce attraverso l'intero ambiente: file, rete, utenti e host.

# SOC as Service [NGS] è il fratello della soluzione [EDR].

Un SOC (Security Operations Center) con EDR (Endpoint Detection and Response) si concentra sulla protezione degli endpoint, come computer e dispositivi mobili, utilizzando tecniche di rilevamento delle minacce basate sul comportamento. Invece, un SOC con NGS (Next-Generation SIEM) si concentra sull'analisi dei dati in tempo reale provenienti da una vasta gamma di fonti, tra cui endpoint, reti e applicazioni, per identificare le minacce e rispondere ad esse più rapidamente. In sintesi, un SOC con EDR è più specifico mentre un SOC con NGS è più ampio e integrato.

L'unione fra i due sistemi permette di raggiungere un livello di sicurezza impensabile fino a poco tempo fa, con l'efficacia di misure tecniche aggiornate e uno staff reale e competente.

# I passaggi nella rilevazione di un problema

Il tipico processo SOAR (Security Orchestration, Automation and Response) che mettiamo in pratica è rappresentato dai passaggi illustrati e schematizzati qui sotto. Diversi sono i sistemi e le tecnologie messe in pratica, tra cui i già citati SDL e UEBA, che compongono il SOC. Ma quelli non sono che la parte macchina del SOAR.

A questi si aggiunge il personale composto da hacker etici che costantemente verificano i dati che potrebbero identificare un cyber threat, intervenendo, se necessario, per bloccare il breach.

**Raccolta dei log file**


**Analisi dei dati provenienti dagli agent**

**Rilevamento anomalia**

**Azioni manuali**

**Possibile problema**

**Notifica al cliente**

# Dispongo già di altri sistemi di sicurezza, perché dovrei attivare la SOC as a Service ?

L’attivazione del servizio SOC as a Service come complemento ai sistemi di difesa esistenti contribuisce a rendere la sicurezza dell’azienda più completa e resiliente.
**Si affianca perfettamente alle soluzioni già in essere** per aumentare la sicurezza complessiva del sistema.

Panoramica Servizi Cyber

# CYBERFERO

## Da oltre 10 anni leader nel settore Cybersecurity e Sicurezza

CYBERFERO è un Managed Security Service Provider (MSSP) specializzato nella fornitura di soluzioni di sicurezza complete per aziende di tutte le dimensioni. In qualità di partner di fiducia, offriamo un'ampia gamma di servizi di sicurezza progettati per proteggere la tua organizzazione da minacce informatiche, violazioni dei dati e altri rischi per la sicurezza.

Visita il sito web

## Contatti


+39 0522 1685330

https://www.cyberfero.com

info@cyberfero.com

Via Statuto 3, 42123 - Reggio nell'Emilia (RE)


Information Security Management System
ISO 27001
Certified