CYBERFERO

SOC as a Service [EDR]

The solution to unify and automate security.

SOCaaS [EDR] is the service that relieves your company of all the management of looming threats.

A 360° active-passive service that includes:

- Monitoring
- Analysis and control
- Attack prevention and detection
- Constant calibration based on events
- Updates on all new threats

www.cyberfero.com

How does it work SOC as a Service?

Software agents

Software agents are installed on all Endpoints.

Configuration

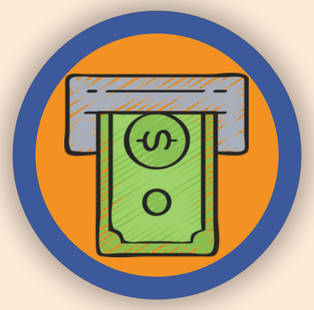
They are custom configured based on the characteristics of the infrastructure.

Activation

The agents activate and begin their collection and alert work.

Passive action

Agents block known threats and enrich logs.



Active action

The most important threats generate an alert to our staff who actively intervenes to resolve the problem.

Safety assured

In conclusion, the best passive-active solution.

What is a SOC

A SOC, an acronym for Security Operations Center, is a team of experts dedicated to protecting organizations from cyber attacks.

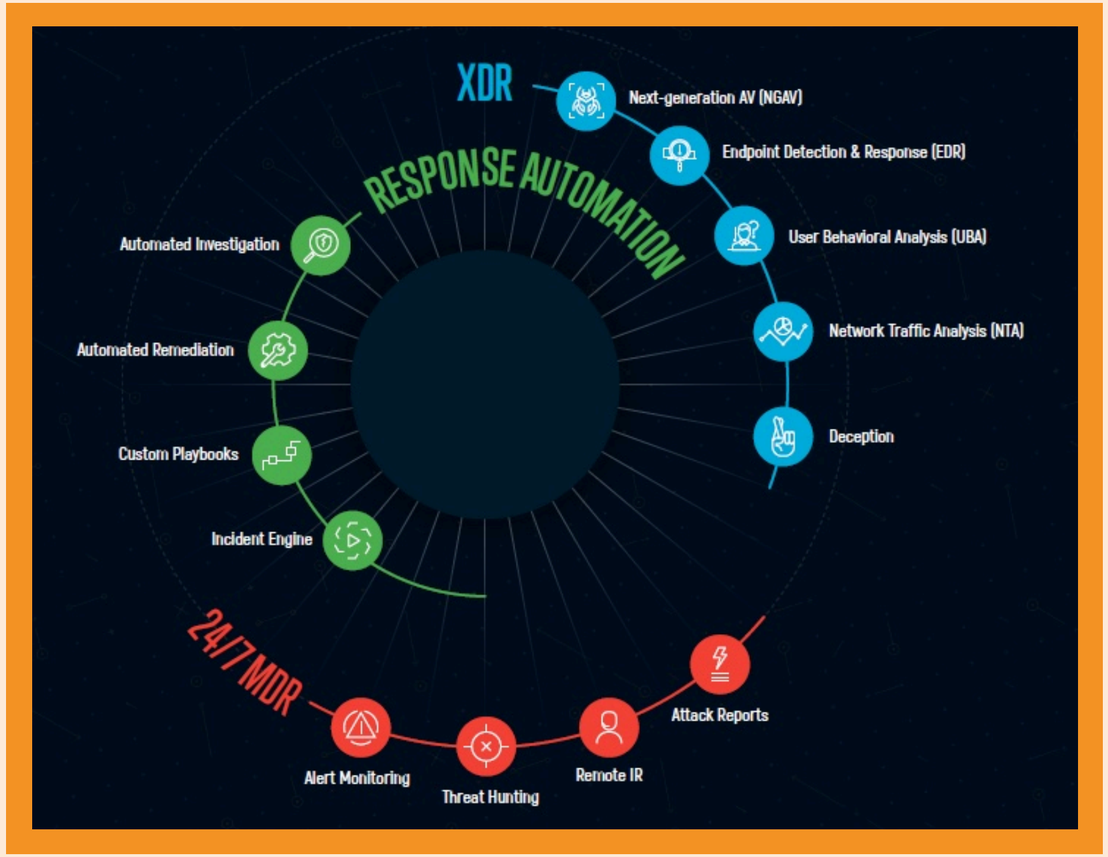
Imagine the SOC as a symbiosis of:

Technical implementations

Such as log analysis, artificial intelligence, constant updates.

Expert Staff

Which intervenes ad hoc when the threat requires a real intervention.



What SOCaaS can do for your business

Our “SOC as a Service” system integrates different intervention methods to reduce threats.
Combining technical implementations and real people creates a security system that improves over time and will adapt to the types of threats your business may experience.

The main features

VULNERABILITY ASSESSMENT

Detection and patching of missing security updates occurs regularly and significantly reduces exposure to the risk of off-the-shelf exploits

FILE INTEGRITY MONITORING

Ideal for a closed, deterministic environment. Any change in the state of files known to be free of threats is immediately brought to the operator's attention by an alert.

INVENTORY MANAGEMENT

Granular visibility and reporting of all outbound entities – hosts, installed software, etc. – are essential for various IT security and management needs.

COLLECTION AND STORAGE OF LOGS

Retaining records for an unlimited period of time allows organizations to comply with various regulatory requirements

360° VIEW WITH ALERTS

Instantly view threat activity status across your entire environment: files, network, users and hosts.

SOC as Service [NGS] it is the brother of the [EDR] solution.

A Security Operations Center (SOC) with Endpoint Detection and Response (EDR) focuses on protecting endpoints, such as computers and mobile devices, using behavior-based threat detection techniques. Instead, a SOC with NGS (Next-Generation SIEM) focuses on analyzing real-time data from a wide range of sources, including endpoints, networks and applications, to identify threats and respond to them more quickly. In summary, an EDR SOC is more specific while an NGS SOC is broader and more integrated.

The union between the two systems allows us to reach a level of security that was unthinkable until recently, with the effectiveness of updated technical measures and a real and competent staff.

The steps in detecting a problem

The typical SOAR (Security Orchestration, Automation and Response) process that we put into practice is represented by the steps illustrated and schematized below. There are various systems and technologies put into practice, including the aforementioned SDL and UEBA, which make up the SOC. But those are just the machine part of SOAR.

Added to these are the staff made up of ethical hackers who constantly check the data that could identify a cyber threat, intervening, if necessary, to block the breach.

Collection of log files

Analysis of data coming from agents

Anomaly detection

Manual actions

Possible problem

Customer Notification

I already have other security systems, why should I activate SOC as a Service?

The activation of the SOC as a Service service as a complement to existing defense systems helps to make the company's security more complete and resilient.
It perfectly complements the solutions already in place to increase the overall security of the system.

Cyber Services Overview

CYBERFERO

For over 10 years a leader in the Cybersecurity and Security sector

Cyberfero is a Managed Security Service Provider (MSSP) specializing in providing comprehensive security solutions for businesses of all sizes. As a trusted partner, we offer a broad range of security services designed to protect your organization from cyber threats, data breaches and other security risks.

Website

Contacts

+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