CYBERFERO

SOC as a Service [NGS]

Cyber security at your service

A complete service for the security of your company:

- ✔ Data Collection and Enrichment (SDL)
- ✔ Event and Information Management (SIEM)
- ✔ User Behavior Analysis (UEBA)

www.cyberfero.com

The advantages of the service

Automatic data collection

SDL + SIEM Data collection (log files), enrichment and SIEM analysis.

Behavioral analysis

UEBA analysis proactively detects social engineering attacks.

24/7 assistance service

The SOCaaS service has 24/7 support.

Keep up with the times

By entrusting.osi to a SOCaaS you ensure that you always have trained professionals available, capable of identifying any type of threat.

Costs

An internal SOC has high costs which include hardware and dedicated personnel. With SOCaaS these costs are reduced.

Expertise assured

Avoid investing large sums in training specialized cyber security personnel. Trust teams of ethical hackers at your service.

What can SOCaaS do for your business?

The system offered by our SOC as a Service is equipped with **artificial intelligence that continuously analyzes log files to identify threats and mitigate risks.**

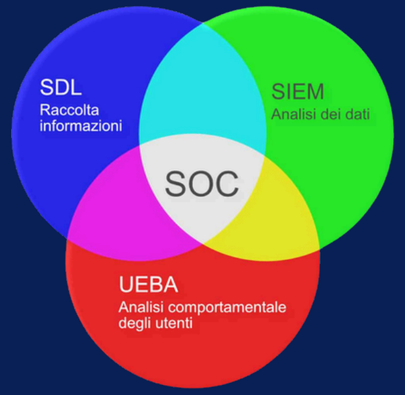
The intervention of a specialized technician, available 24/7, checks potential threats and intervenes to block attacks in their tracks. An alert to the customer is sent if necessary.

A SOCaaS offers the necessary precautions against known techniques and identifies the correlation between data indicating possible attacks with yet unknown techniques.

Continuous improvement

If your company operates on the network and wants to do so in complete security, our SOCaaS defense system against cyber attacks is the most advantageous solution.

If your company operates on the network and wants to do so in complete security, our SOCaaS defense system against cyber attacks is the most advantageous solution.



What is a SOC

A Security Operation Center (SOC) uses 3 technologies to manage and prevent IT problems:

SDL (Security Data Lake)

Collection and enrichment of the information contained in the log files.

SIEM

(Security Information and Event Management)

Collected data is analyzed to identify threats and anomalies.

UEBA

(User and Entity Behaviour Analytics)

Analyzing user behaviors against social engineering attacks.

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, SIEM 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

Data Analytics (SIEM)

Anomaly detection

Manual control

Possible problem

Customer Notification

I already have other security systems in place, why should I activate SOC as Service [NGS]?

The activation of the SOC as a Service [NGS] 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