Secure Online Desktop

Security Operation Center as a Service

Protezione dalle minacce informatiche

Previenzione fughe di dati

Identificazione immediata attacchi in corso

Un'offerta per i Security Manager, CSO, CISO, IT Manager e CTO

Cyber security e minacce
Cosa può fare un SOC per la tua azienda

Un ***Security Operation Center*** **(SOC)** è un centro operativo che **costantemente analizza e confronta i dati** che il complesso sistema IT di un'azienda genera.

Attraverso questo processo si ottengono numerosi vantaggi, tutti orientati ad **aumentare la sicurezza informatica del sistema** e ridurre il rischio di attacchi informatici in generale.

Principali vantaggi di un SOC

- Con l'intelligenza artificiale e il machine learning, **il SOC blocca gli attacchi sul nascere**, analizzando i comportamenti degli utenti.
- Anche gli attacchi in corso sono più facilmente individuabili, perché **il SOC è in grado di riconscere ed eliminare rapidamente i falsi potivi**, facendo risparmiare tempo che sarà meglio speso in operazioni proattive.
- **Il centro operativo genera notifiche in caso di violazioni delle policy interne**, per esempio in caso di *data exfiltration*, dolosa o accidentale.

Chi controlla *davvero* la sicurezza della tua azienda?

Stanno forse pianificando un attacco?

I dati sono rimasti sempre all'interno del perimetro?

Se le risposte sono incerte, la tua azienda dovrebbe valutare un SOCaaS.

Permetterà di mitigare e bloccare gli attacchi informatici, ma non solo.

Può essere molto utile anche con la **compliance degli standard di sicurezza:** per esempio, in caso di *data breach*, i dati raccolti dal SOC saranno indispendabili per individuare dove si debba intervenire e quali dati siano fuoriusciti.

Nelle prossime pagine scopri come funziona e cosa è in grado di fare per la tua azienda un SOC as a Service

Secure Online Desktop

Le componenti di un SOC

Un SOC è composto da molti componenti che cooperano per la rilevazione di *cyber threat* e l'azione in caso di *breach* del sistema informatico.

Questo significa un investimento ingente in hardware e in personale specializzato.

Come è fatto un SOC

Un **centro operativo di sicurezza** si articola in tre principali tecnologie per la gestione e prevenzione dei problemi di un sistema IT.

1. Security Data Lake - SDL

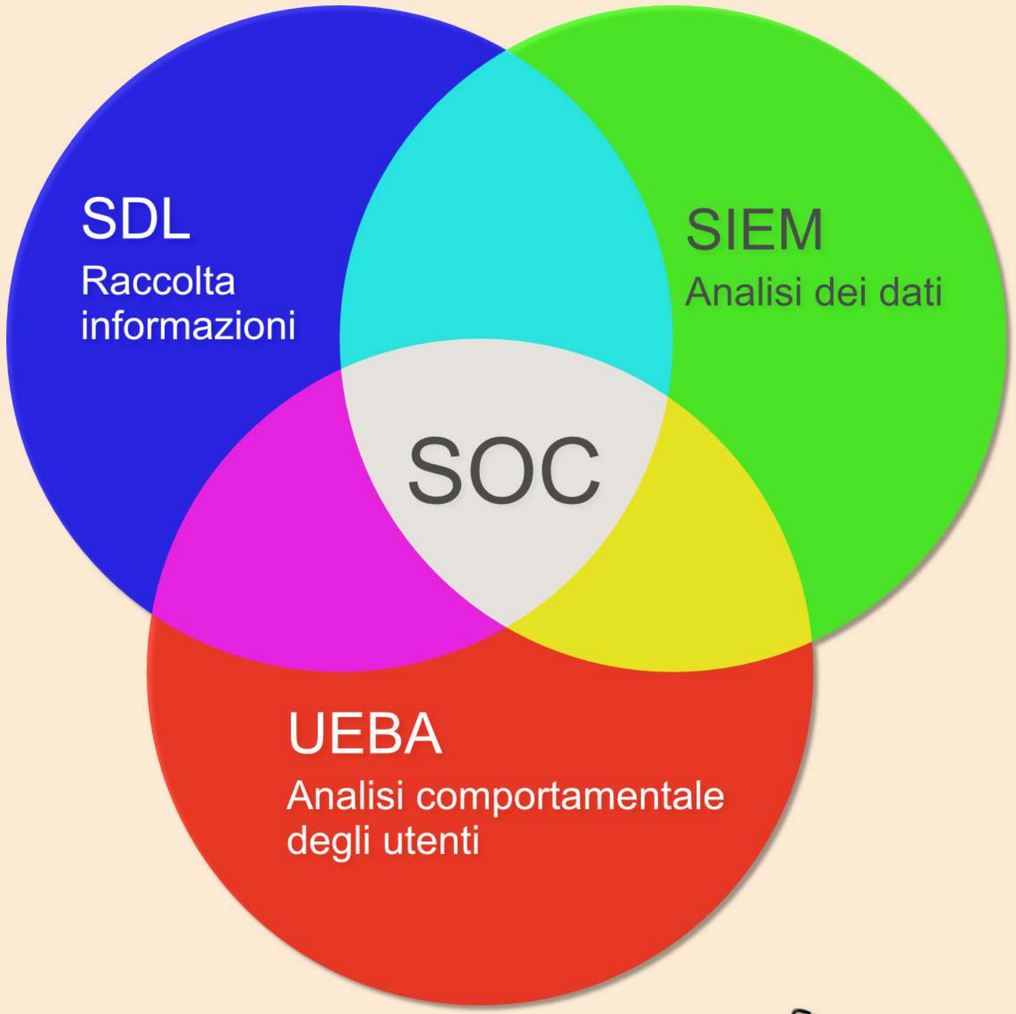
Attraverso l'azione di agenti disseminati in ogni nodo della rete, il SDL si riempie di tutte le informazioni disponibili, che torneranno utili nella fase di analisi.

2. Security Information and Event Management - SIEM

I dati raccolti sono analizzati tramite il SIEM, che **confronta eventi e informazioni con gli indicatori di compromesso conosciuti**. La ricerca delle anomalie comincia da qui e si arricchisce tramite un altro componente.

3. User and Entity Behavior Analytics - UEBA

Tramite questa tecnologia è possibile effettuare un'**analisi proattiva del comportamento degli utenti e delle macchine**. Questo significa che sono individuabili anche i comportamenti sospetti, non solo gli attacchi avvenuti.



Come funziona il SOC as a Service di SOD

Il sistema offerto dal nostro **SOCaaS** è **dotato di intelligenza artificiale**, la quale è impegnata ad analizzare i dati raccolti alla ricerca di comportamenti sospetti.

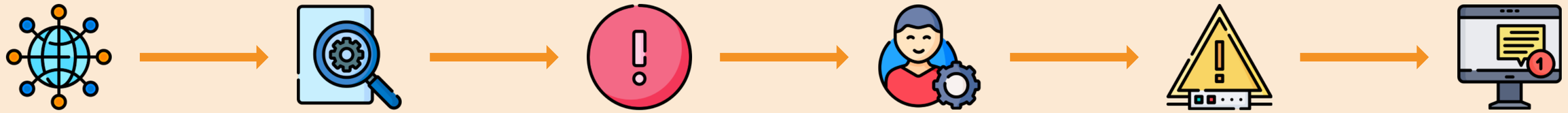
Inoltre, è **sempre disponibile un intervento tecnico specializzato** ad ogni ora del giorno e della notte con compiti specifici. L'intervento si occupa di verificare gli allarmi generati dal sistema per eliminare i falsi positivi, intervenire per risolvere la minaccia e fornire rapporti regolari nel tempo.

Grazie alla **raccolta e arricchimento dei dati, l'analisi automatica effettuata dall'intelligenza artificiale e quella manuale dei tecnici**, il servizio si rivela essere davvero conveniente e completo.

I passaggi nella rilevazione del rischio tramite SOC

Il tipico processo **SOAR (Security Orchestration, Automation and Response)** che mettiamo in pratica è rappresentato nei passaggi illustrati qui sotto. Diversi sono i sistemi e le tecnologie all'opera, tra cui i già citati SDL, SIEM e UEBA, che compongono il SOC. Ma quelli non sono altro che la *parte macchina* del centro operativo.

Alla tecnologia, infatti, bisogna aggiungere **l'intervento essenziale del personale specializzato, composto da ingegneri e hacker etici** che sono costantemente al lavoro per verificare i dati che potrebbero identificare una *cyber threat*, intervenendo, se necessario, per bloccare la minaccia e risolvere il problema.



Raccolta dati e logfile

Arricchimento e analisi dati

Rilevamento anomalia

Controllo manuale

Possibile problema

Notifica al cliente

Secure Online Desktop

SOC as a Service
La sicurezza con un investimento ridotto

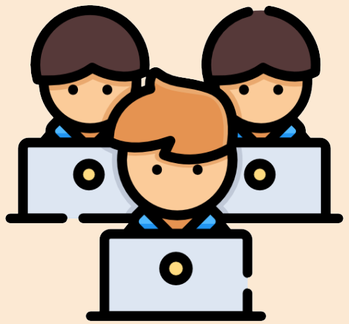
I vantaggi nell'utilizzo di un servizio SOC esterno alla compagnia sono molteplici, tra cui:

1. Risparmio economico sul breve e lungo periodo
La tua azienda eviterà di acquistare hardware dedicato e software specializzato. Inoltre, non dovrai assumere nuovi dipendenti e nemmeno formare o aggiornare quelli che già sono in azienda.

2. Tecnici formati e competenti
I tecnici del servizio fanno parte di una squadra affiatata che quotidianamente lavora e impara sul campo a **combattere nuove tipologie di minacce**. Questa formazione attiva non ha prezzo e non è realizzabile lavorando come dipendente per una sola compagnia.

3. Tecnologia sempre aggiornata
Non bisognerà preoccuparsi di dover aggiornare software o sostituire hardware datato o corrotto. Il servizio solleva da ogni responsabilità di investimenti immediati o futuri in equipaggiamento specifico.

Risparmio economico



Tecnici formati e competenti

Tecnologia al passo coi tempi

Se la tua azienda fosse interessata ad approfondire le funzionalità del SOCaaS di Secure Online Desktop, o se ci fossero delle domande, siamo disponibili a rispondere.

Le informazioni di contatto sono nella prossima pagina.

Secure Online Desktop

Scegli la sicurezza per la tua azienda

Dal 2011 ci occupiamo di tecnologia Cloud e di sicurezza, affidati a dei professionisti esperti!

Scopri il servizio sul sito

Per ulteriori informazioni, i nostri contatti sono:

Via Zacchetti 6, 42124 - Reggio nell'Emilia (RE)
www.secure-od.com

Tel. +39 0522 1685330
Fax. +39 0522 015371
E-mail: info@secure-od.com
PEC: secure-od@pec.it

Secure Online Desktop