

SecurityARCHITECT®

SECURITY OPERATIONS CENTER

Sfrutta al massimo il tuo tempo, liberati dai problemi di rete e di sicurezza informatica.

Identifichiamo, indaghiamo e risolviamo problemi di sistema.

Il ruolo del Security Operations Center è quello di tenerti al sicuro, gestire gli incidenti che potrebbero ostacolare la sicurezza dei dati.

Pensa al SOC come al team di tutori aziendali contro le minacce esterne per il tuo business e i tuoi clienti.





Cosa è il SOC?

Vulnerability assessment, security incident detection, continuous monitoring, incident response in un'unica soluzione.

Un SOC è un centro operativo tramite il quale vengono garantiti i servizi di gestione, analisi, monitoraggio e difesa della sicurezza IT di un'azienda. Attraverso un team di professionisti, un SOC può analizzare l'intero flusso dei dati ed esercita un controllo su tutti i dispositivi aziendali, compresi quelli cloud e di terze parti, individuando e contrastando gli attacchi e le minacce alla cyber security per evitare che abbiano un impatto sull'azienda.

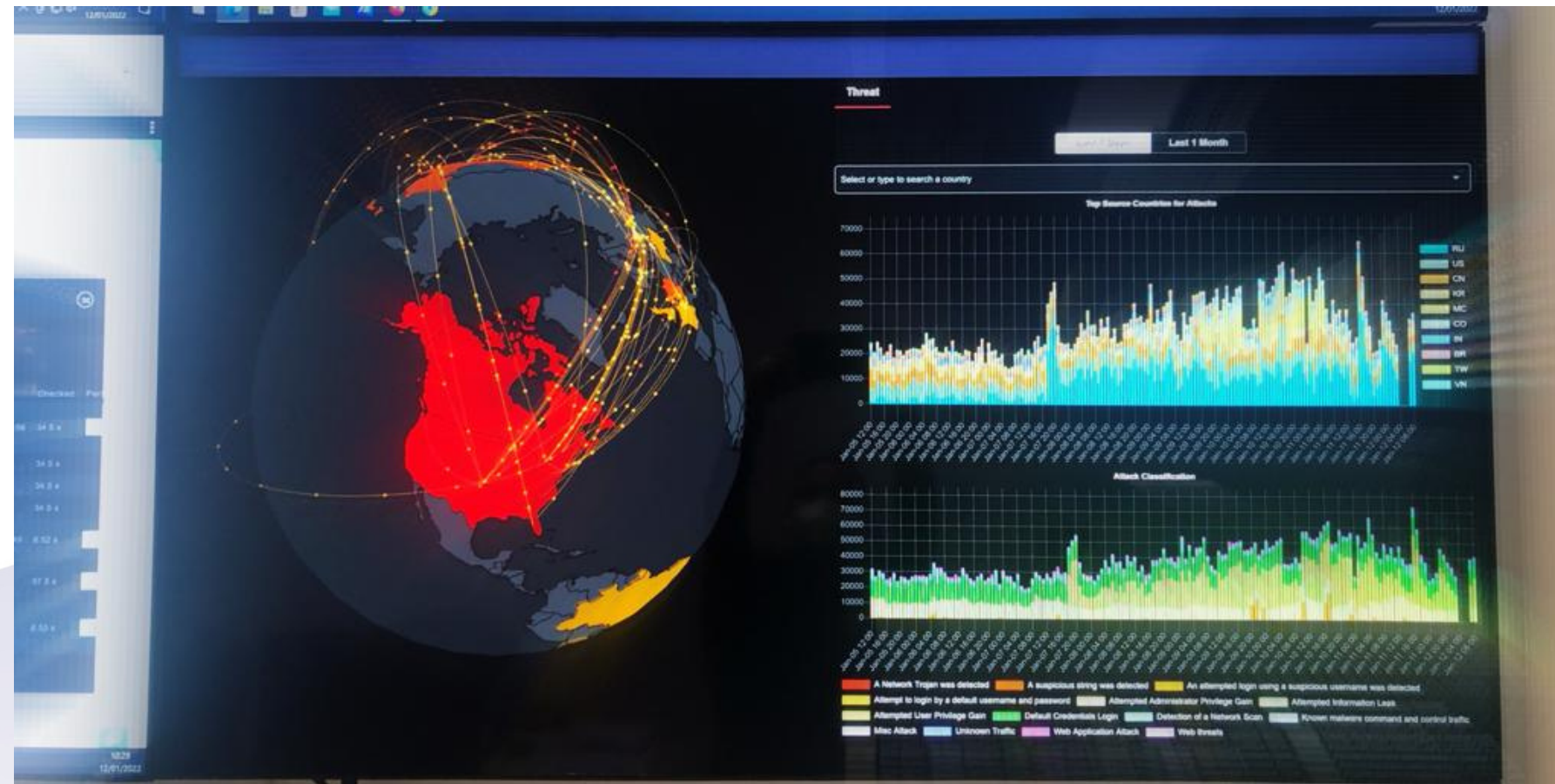
Security *ARCHITECT* Operations Center

Il nostro Security Operations Center è composto dal team interno responsabile del rilevamento, della prevenzione, dell'indagine e della risposta alle minacce informatiche e dalle tecnologie necessarie per renderlo *live, fast, effective!*



Il nostro SOC può eseguire il monitoraggio 24/7 della rete di un'organizzazione e affronta le potenziali minacce ai dati sensibili, ai sistemi informatici e alle altre risorse IT e digitali di un'organizzazione.



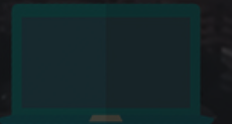


Security Architect propone un servizio completo di continuous monitoring dei network aziendali e un'ulteriore possibilità che coinvolge 3 livelli del SOC: **VULNERABILITY ASSESSMENT, SECURITY INCIDENT DETECTION, CONTINUOUS MONITORING e INCIDENT RESPONSE.**

SECURITY OPERATION CENTER AS A SERVICE



SecurityARCHITECT
www.securityarchitect.it



Perché il SOCaaS?

Con la crescente minaccia di attacchi informatici, un SOC è fondamentale per la capacità di un'organizzazione di sostenere la continuità operativa, rimanere redditizia e raggiungere e mantenere la conformità alle normative.



Il raggiungimento di un alto livello di maturità della sicurezza tramite un SOC interno è costoso, richiede molto tempo, skills settoriali e iper-specialistiche.


Diviene, quindi, per una PMI o per un'impresa che si occupa di tutt'altro, impossibile assicurare tale livello di sicurezza informatica.

Per questo motivo, molte organizzazioni stanno prendendo in considerazione servizi di sicurezza in outsourcing, sfruttando la nostra soluzione di un SOC-as-a-Service (Security Operations Center as a Service).



Numerosi fattori eterogenei influiscono sulla capacità di un'organizzazione di gestire internamente un SOC efficace e maturo.

La carenza di talenti per la sicurezza informatica rende difficile e costoso attrarre e trattenere personale qualificato. Inoltre, una sicurezza informatica efficace richiede investimenti in una serie di soluzioni tecnologiche progettate per affrontare e mitigare un'ampia varietà di potenziali minacce.



Security Architect Srl è provider SOC-as-a-Service: ci occupiamo di monitoraggio live e difesa della rete, di tutti i network e i servizi web, facendo le diagnosi necessarie per proteggere le aziende dalle moderne minacce informatiche.

Responsibilities of a security operations center (SOC)



Quasi tutte le organizzazioni subiranno una violazione della sicurezza dei dati quest'anno.

È il modo in cui rispondi che fa la differenza!



I vantaggi del Soc as-a-service

I vantaggi dell'outsourcing

Potenziamento delle aziende e delle imprese

AZIONI E CONSIGLI EFFICACI PER UN'AZIENDA SICURA

La partnership con un provider SOC gestito significa che un'organizzazione può integrare e colmare le lacune nel proprio team, evitando di dover effettuare importanti investimenti in ulteriore personale qualificato nel settore cyber security.

ACCESSO A COMPETENZE DI SICUREZZA SPECIALIZZATE

Le organizzazioni spesso richiedono l'intervento di un esperto per mitigare le conseguenze di un incidente o di un attacco, necessitano di analisti malware, architetti della sicurezza cloud, Security Engineer... Questi set di abilità sono rari e difficili da mantenere all'interno dell'azienda. Un fornitore di SOC-as-a-Service può offrire ai propri clienti l'accesso a specialisti esperti di sicurezza informatica quando necessario.

SICUREZZA AGGIORNATA

Tenersi aggiornati con gli strumenti e le funzionalità SOC più recenti può essere difficile.

Un provider SOC gestito è *costretto* a tenere sempre aggiornato il proprio set di strumenti e conoscenze, offrendo i vantaggi di una sicurezza all'avanguardia ai propri clienti.

REPUTAZIONE AZIENDALE MIGLIORATA

Indicatore per dipendenti e clienti che l'azienda prende sul serio la sicurezza e la privacy.

La reputazione aziendale migliorata da un SOC ben gestito può aumentare l'interesse dei clienti attuali e di quelli potenziali.

ABBATTIMENTO DEI COSTI

L'implementazione, la manutenzione e il funzionamento di un SOC completo in-house è proibitivo. Con un SOC gestito, le organizzazioni possono affidarsi al provider che possiede attrezzature e personale all'altezza del compito. Ciò riduce sia il capitale che le spese operative (CapEx/OpEx) di un ecosistema sicuro.

INNALZAMENTO DELLA SECURITY POSTURE

Costruire le soluzioni per un programma di sicurezza informatica maturo è un processo esteso. La collaborazione con un provider SOC-as-a-Service può aiutare ad abbreviare questo processo fornendo a un'organizzazione l'accesso allo stack di soluzioni del provider e agli esperti di sicurezza.

I vantaggi del SOC

Un miglioramento quotidiano

Supervisione di tutte le attività di gestione delle funzionalità di sicurezza legate alla rete, ai sistemi e alle applicazioni.

monitoraggio in tempo reale l'infrastruttura IT per individuare tempestivamente tentativi di intrusione e di attacco informatico.

progettazione di misure di sicurezza per eventuali incidenti e attacchi informatici - *Disaster Recovery plans*.

Fornitura di supporto anti-virus, report degli alert in tempo reale, Digital onboarding.

SecurityARCHITECT®

Nata nel 2005 dalla passione e dall'esperienza nel settore informatico, Security Architect Srl è diventata importante riferimento di molte grandi aziende. Da 16 anni opera nel settore ICT, cyber security.

Grazie al costante aggiornamento, agli alti standard qualitativi, all'innovazione e all'affidabilità delle soluzioni offerte riesce ad essere sempre un passo avanti rispetto ai propri competitors.

CLIENTS

PARTNER



info@securityarchitect.it



securityarchitect.eu



080 671053 - 080 8756269



Via Salvatore Matarrese, 36
70124 Bari (BA), Italia

