Security Operations Center (SOC)

[SEC]

Migliora e monitora la postura di sicurezza informatica dell'azienda, proteggendola dai rischi informatici in modo proattivo

Principali benefici

Salvaguardia della continuità di business, confidenzialità e reputazione

Il SOC di S2E è il servizio adatto per l'evoluzione della sicurezza informatica dell'azienda da un approccio reattivo, ad uno proattivo. Attraverso la sinergia tra competenze specializzate, processi e tecnologie specifiche monitoriamo, identifichiamo e indirizziamo le minacce informatiche all'interno dell'azienda, garantendo una governance strutturata delle infrastrutture aziendali finalizzata ad una maggiore sicurezza, prevenzione e reattività di risposta per la salvaguardia della continuità aziendale.

Ambito di applicazione

Il servizio SOC è adatto ad aziende di medie e grandi dimensioni che forniscono risposte a necessità moderne e in evoluzione dei propri clienti, comportando un aumento di complessità e varietà delle proprie infrastrutture informatiche, indipendentemente dal settore in cui l'azienda opera.
La necessità di trattare dati sensibili, così come la partecipazione a mercati ad elevato rischio, richiede che l'azienda si doti di uno strumento adeguato per la salvaguardia delle informazioni aziendali, ottemperando anche a requisiti normativi in crescita.

Le sfide che le aziende incontrano

La digitalizzazione dell'azienda ne espone gli asset a molteplici rischi informatici il cui governo strutturato richiede competenze specifiche difficili da reperire sul mercato.
Le aziende convivono con un senso di incertezza causato dalla non conoscenza delle proprie vulnerabilità e dall'impossibilità di prevedere tempi, modalità ed effetti di un attacco informatico.
Se da un lato le aziende sono consapevoli dei rischi a cui sono costantemente esposte, dall'altro è difficile giustificare investimenti in sicurezza agli occhi degli investitori.

I vantaggi offerti

Il SOC permette di identificare tempestivamente rischi, minacce e vulnerabilità, permettendo di ridurre l'esposizione al rischio e abilitando la possibilità di risposte tempestive agli incident. Il management aziendale salvaguardia la continuità di business e mitiga rischi reputazionali dovuti a fughe di dati e attacchi informatici. Il CISO acquisisce competenze e risorse per svolgere il proprio ruolo di garante della sicurezza dell'informazione aziendale.

S2E: approccio e metodo proposto

Il SOC di S2E è disegnato su misura delle strutture informatiche del cliente, così come dei suoi attuali processi e tecnologie. Attraverso il nostro team di esperti, disegniamo uno strutturato processo sinergico di monitoraggio e risposta che prevede diversi livelli di identificazione e analisi degli alert di sicurezza rilevati, che coinvolgono sia analisti in fase di triage degli alert, sia esperti di digital forensics per gli incident complessi, con l'obbiettivo di analizzare, valutare e classificare gli alert generati dall'infrastruttura informatica in modo accentrato, qualificandone rilevanza e criticità. Ciò permette al cliente di avere visibilità su attività anomale in modo tempestivo, correlandone le causalità per identificare le vulnerabilità dell'infrastruttura informatica.
Grazie al SOC di S2E il cliente acquisisce la possibilità di prevenire gli attacchi informatici attraverso l'analisi delle vulnerabilità, e di rispondere tempestivamente a minacce in corso grazie all'identificazione in tempo reale dell'incident e la conoscenza precisa di quali risorse sono state compromesse, isolandone il perimetro e circoscrivendo la superficie d'impatto.

Vantaggi per lo sviluppo futuro

I vantaggi principali del SOC di S2E sono:

1. Riduzione e mitigazione dei rischi alla continuità di business.
2. Salvaguardia degli asset aziendali da attacchi semplici e numerosi.
3. Riduzione della superficie d'impatto su attacchi complessi e strutturati.
4. Visibilità di alert, incident ed eventi di sicurezza che in precedenza restavano inosservati.
5. Monitoraggio centralizzato e real-time dell'intera infrastruttura aziendale.
6. Generazione di consapevolezza sui rischi aziendali e sua diffusione in azienda.

Un SOC disegnato sulle unicità del cliente permette di fornire una soluzione di sicurezza adattata alle specifiche esigenze e minacce dell'azienda, aumentando la protezione dei dati e riducendo i rischi di violazioni.

Modello di offerta

Il SOC di S2E è un servizio gestito realizzato su misura. Attraverso un assessment iniziale finalizzato alla comprensione delle risorse coinvolte nel perimetro, e dei loro aspetti sia di governance, che funzionali, proponiamo una soluzione ad-hoc per l'implementazione del servizio, che garantisca sia la salvaguardia delle risorse target, sia rispetto di livelli di servizio e intervento adeguati all'importanza e criticità delle risorse che proteggiamo.
Successivamente alla fase di implementazione, gestiamo il SOC realizzato con un team dedicato e a supporto continuo, in modo che l'azienda sia salvaguardata senza necessità di intervento delle strutture organizzative, che sono coinvolte solo in caso di necessità e incident escalation.
Il servizio è erogato a canone annuo.