

security care



Security Care è una suite di servizi offerta da Enforcer (Gruppo Easynet) il cui obiettivo è garantire le attività propedeutiche alla gestione e manutenzione della sicurezza del cliente anche in relazione al regolamento europeo GDPR e ad altri standard (quali la direttiva 285 di Banca d'Italia, PCI-DSS, ISO 27001).

A COSA SERVE

Security Care è un sistema integrato di gestione degli asset aziendali e dei flussi operativi in ottica di cyber security e compliance GDPR.

Gli asset all'interno di Security Care possono infatti essere trattati secondo le modalità previste dal GDPR e, se abbinati a sistemi interni alla rete aziendale o che espongano servizi su Internet, gestiti all'interno di un sistema di Vulnerability Management che tiene traccia delle criticità esistenti e delle opportune procedure di risoluzione.

Il sistema è in grado di monitorare costantemente e a vari livelli i sistemi, le problematiche di sicurezza presenti e tutti i log rilevanti, allo scopo di identificare tempestivamente eventuali violazioni. Queste possono essere gestite all'interno di Security Care da un sistema di Ticketing che mantiene il cliente sempre informato sullo stato delle operazioni.

PRINCIPALI FUNZIONALITÀ

GESTIONE ASSET

Permette di identificare, definire e gestire l'elenco degli asset, a livello logico e fisico tramite identificazione automatica degli asset: server, postazioni di lavoro e apparati collegati alla rete ("Network Discovery")

VULNERABILITY ASSESSMENT

I sistemi selezionati sono sottoposti a scansioni periodiche delle vulnerabilità eventualmente presenti. Le procedure sono seguite da analisti di Enforcer e possono essere configurate in base a specifiche esigenze del cliente.

OPEN SOURCE INTELLIGENCE (OSINT)

Il servizio proposto aiuta a migliorare la sicurezza della propria azienda attraverso la raccolta di informazioni pubbliche o presenti nel "Dark Web" che possono essere sfruttate dai criminali in qualsiasi momento. Attraverso una completa gestione della superficie d'attacco è possibile riscontrare avvenute compromissioni o evitarne future, verificare il furto di dati e password, tenere sotto controllo l'integrità del marchio e la proprietà intellettuale aziendale, mitigare gli attacchi di Phishing "mirato", e ridurre drasticamente il fattore di rischio Cyber.

SISTEMA TICKETING NATIVO

Il sistema di ticketing può essere legato sia ad esigenze emerse da VA (preventive) che in seguito a problemi e vulnerabilità realmente subite dal sistema (risposta proattiva). Opzionalmente integrabile con applicazioni di terze parti.

NOC Network Operation Center

Struttura che monitora le infrastrutture critiche dell'azienda per verificarne uptime, eventuale criticità sistemica (cpu, processi non funzionanti), controlla switch ed interruzioni su connessioni di rete. In caso di problematiche riscontrate, può essere attivata tramite software/matrice di contatto.

PATCH LEVEL ASSESSMENT

Analisi del livello di aggiornamento di server, client e/o apparati di rete in relazione ai bollettini di sicurezza rilasciati dai rispettivi produttori. Sono effettuate tramite accesso autenticato ai sistemi sottoposti ad analisi per ridurre l'impatto sugli ambienti di rete e fornire risultati più accurati.

PASSWORD CHECK

Questo modulo permette di verificare la robustezza delle credenziali locali Windows, dei domini Active Directory e dei sistemi Unix.

VULNERABILITY MANAGEMENT

Il sistema consente gestire i risultati, gli eventuali falsi positivi, effettuare comparazioni tra diverse scansioni e mostrare gli andamenti nel tempo delle procedure di risoluzione, fornire report e statistiche e segnalare le violazioni tramite sistema di Ticketing.

SOC DEFENSIVE Security Operation Center

Struttura che eroga servizi di sicurezza personalizzati in base ai processi del cliente, ai suoi bisogni e alle specifiche minacce del settore in cui il cliente opera. L'individuazione preventiva e la gestione in tempo reale degli incidenti sono fattori di primaria importanza per garantire alle aziende un adeguato livello di protezione delle reti, dei dati e dei servizi. In caso di problematiche critiche, può essere attivata tramite sistema di ticketing o matrice di escalation definita.

SOC OFFENSIVE Security Operation Center

La presenza di evidenze critiche nei moduli di Vulnerability Assessment e Phishing è monitorata dal nostro Security Team, che può essere coinvolto tramite Ticketing.

PHISHING

Permette di valutare il grado di security awareness, sensibilità e reattività degli utenti attraverso l'invio controllato di messaggi contenenti codice malevolo e/o link a sistemi esterni e ad un sistema di controllo e reportistica dei vettori di attacco andati a buon fine.

LIVELLI DI SERVIZIO

SERVIZIO	FUNZIONALITÀ STANDARD	MODULI OPZIONALI
Sonda fisica o virtuale ¹	✓	
Sistema Ticketing	✓	
Gestione asset	✓	
Vulnerability Assessment	✓	
Vulnerability Management	✓	
SOC Offensive	✓	
Password Check	✓	
GDPR Bulletin	✓	
Servizio NOC		✓
Simulazione di phishing		✓
Servizio SOC difensivo		✓
OSINT		✓
Sessioni di formazione specifiche in ambito cybersecurity erogate da SETA		✓

¹ La selezione della sonda è valutata in base alle esigenze ed alla configurazione selezionata. La configurazione viene effettuata da personale qualificato Enforcer in base alle reali esigenze e non tramite wizard precompilati



Enforcer nata nel 2004, è una società di consulenza specializzata nelle problematiche di sicurezza informatica e "vendor independent". Soci fondatori sono Igor Falcomatà e Matteo Falsetti, riconosciuti in Italia come punti di riferimento del settore della sicurezza informatica e della comunità degli ethical hacker con clienti operanti in vari ambiti (telecomunicazioni, finanza/bancari, servizi terziari, ecc). Enforcer è una società del Gruppo Easynet.



Easynet S.p.a. dal 1995 propone alle Aziende soluzioni d'integrazione tra sistemi informativi e tecnologie internet-based, con un cammino di crescita sempre più orientato alla fornitura di soluzioni avanzate sia nell'ambito dei sistemi IT che della sicurezza informatica e l'ottenimento delle certificazioni ISO/IEC 20000, ISO/IEC 27001 e ISO/IEC 27018.



SETA.

Security talent academy

SETA è la società del Gruppo Easynet, specializzata nella formazione in ambito sicurezza informatica e business continuity. SETA, con un corpo docenti di esperti operativi nel settore cybersecurity attivamente coinvolti nelle più importanti organizzazioni pubbliche e private italiane, è il punto di riferimento nella formazione sulla sicurezza informatica e la business continuity.

Enforcer s.r.l.

Sede di Lecco C.so Promessi Sposi 25/D 23900 Lecco

www.enforcer.it

securitycare@enet.it