Servizio di: **Cybersecurity SOC**

Il livello più avanzato per la protezione e sicurezza

Protezione locale e Centro operativo di sicurezza SOC

• Il servizio Managed Detection and Response (MDR) assicura un'efficace protezione avanzata, 24 ore su 24, nei confronti del crescente volume di minacce informatiche, in grado di eludere i sistemi automatizzati di prevenzione e rilevamento.

• Le eccellenti capacità di rilevamento e risposta sono supportate da uno dei team di analisti migliori del settore, con oltre 20 anni di esperienza nella prevenzione di malware e minacce informatiche.

Protezione locale
(Endpoint protection)

Servizio MDR

PROTEZIONE COMPLETA!

030 2306877 info@secoges.com Via Achille Grandi, 8 - 25125 Brescia (BS) Italy

Perchè il servizio SOC per la tua organizzazione

- Protezione dalle minacce informatiche
- Prevenzione delle fughe di dati
- Identificazione immediata degli attacchi in corso

Grazie al servizio di **Threat Intelligence** coadiuvato da sistemi di **intelligenza artificiale** e **apprendimento automatico**, la consapevolezza di essere costantemente protetti anche dalle minacce più complesse e avanzate

PROTEZIONE

- Threat hunting e investigation proattivi 24 ore su 24, 7 giorni su 7
- Avvisi di sicurezza in tempo reale
- Analisi retrospettiva dell'incidente
- Incident reponse guidata e automatizzata
- Visibilità degli asset e controlli di integrità della sicurezza
- 1 anno di archiviazione della cronologia incidenti
- 1-3 mesi dei dati non elaborati

RISPOSTA

- Isolamento host
- Quarantena dei file
- Rimozione dei file
- Interruzione processi compromessi
- Analisi files specifici

COMUNICAZIONE

- Notifiche del portale
- Messaggistica istantanea
- E-mail
- Schede Asset
- Reportistica

Come funziona

• Convalida degli avvisi di sicurezza generati dal sistema di protezione, al fine di garantire la piena efficacia delle funzionalità di prevenzione automatica;

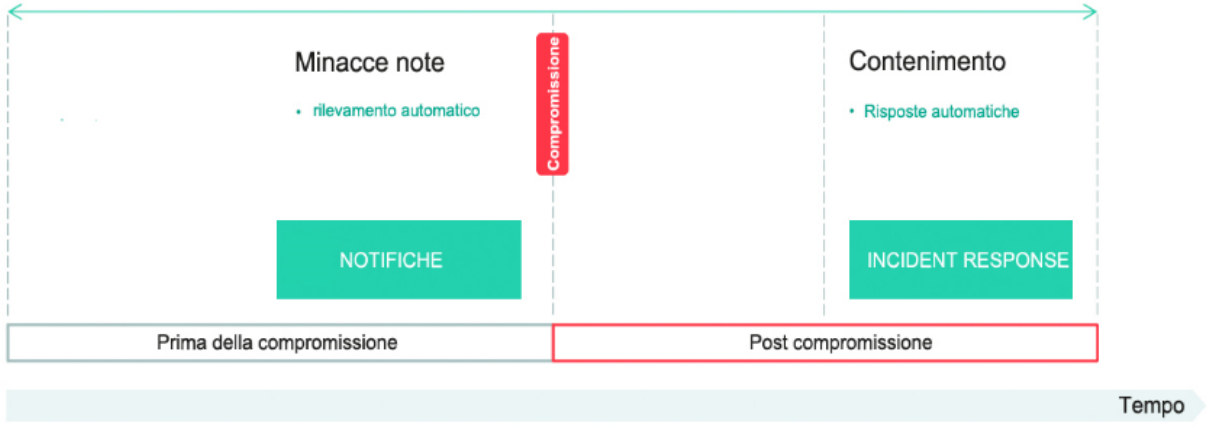
• Analisi proattiva dei metadati relativi all'attività di sistema, per rilevare eventuali comportamenti correlabili ad un attacco attivo o imminente;

• I metadati vengono raccolti tramite il sistema di protezione, per poi essere automaticamente correlati in tempo reale con la Threat Intelligence impiegata dal sistema, allo scopo di identificare tattiche, tecniche e procedure utilizzate dagli autori dell'attacco;

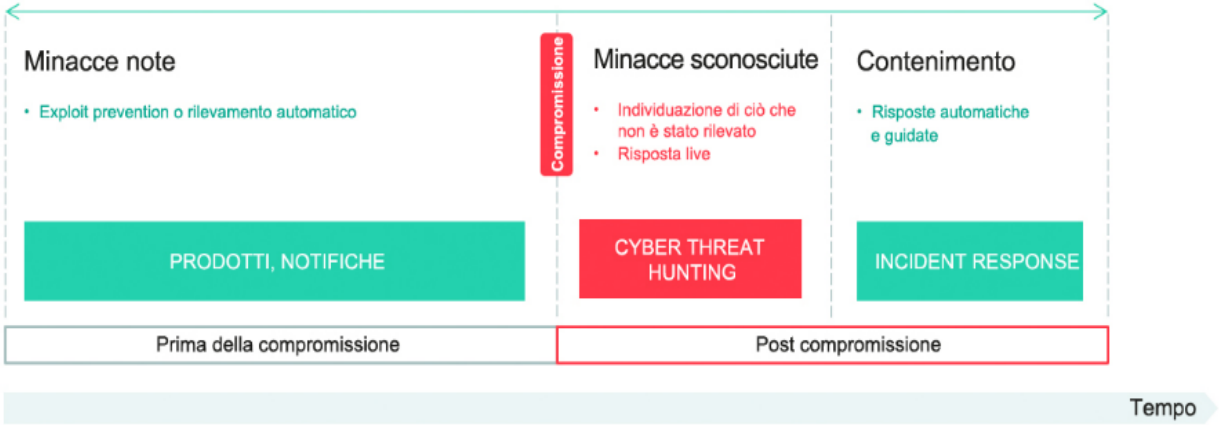
• Gli indicatori di attacco basati su sistemi di machine learning consentono il rilevamento di minacce malwareless, in grado di emulare attività legittime. Nell'arco delle prime 2-4 settimane la soluzione si adatta pienamente all'infrastruttura IT aziendale, per garantire un tasso di falsi positivi tendente a zero.

Differenza tra protezione cyber con approccio tradizionale e con servizio MDR

APPROCCIO TRADIZIONALE



MANAGED DETECTION AN RESPONSE



Descrizione del servizio

Il servizio aumenta istantaneamente la sicurezza IT senza la necessità di investire in personale o competenze aggiuntive e fornisce resilienza agli attacchi elusivi attraverso la sua rapida implementazione chiavi in mano.

Il servizio include:

- Monitoraggio proattivo 24x7
- Ricerca automatica delle minacce e valutazione degli avvisi
- Playbook di risposta e IR automatico
- Controllo dello stato di sicurezza e visibilità delle risorse
- Portale web MDR con dashboard e reportistica
- Archiviazione della cronologia degli incidenti di 1 anno
- 1 mese di archiviazione dei dati telemetrici raccolti

Incident management

Rilevamento di un evento potenzialmente malevolo o uno stato anomalo di un sistema o servizio.

Analisi dell'evento da parte dell'intelligenza artificiale e del team di analisti per la valutazione del livello di rischio e l'analisi della tipologia di minaccia.

Tramite l'applicazione di indici di rischio e criteri di valutazione viene pubblicato l'incident sull'apposito portale e avvisato il personale di riferimento, comprensivo dei dettagli della minaccia e possibili attività di remediation.

Intervento coordinato per prevenire, mitigare o ridurre i possibili danni derivanti dall'evento malevolo.

Fonte dell'evento	Possibili criteri di incidenti	Possibili Remedation actions
Endpoint + network	▶ Fase attiva dell'attacco che non è stata prevenuta automaticamente ▶ Evidenze di persistenza dannosa nel sistema ▶ Evidenze di compromissioni passate ▶ Attività anomale anche se apparentemente legittime ▶ Evento di sicurezza confermato dall'endpoint	▶ Rilevamento dei problemi tramite il sistema di protezione e controllo dell'efficienza della remediation automatizzata (se tecnicamente possibile) ▶ Raccomandazione di azioni correttive manuali ▶ Azioni correttive automatiche necessarie ▶ Raccomandazioni per aumentare la sicurezza dei dati ▶ Informazione al cliente

Incident Priority Level

Priority level	Description
High	▶ Può essere assegnato a incidenti che, a giudizio del fornitore, possono causare gravi interruzioni o accesso non autorizzato alle risorse del Cliente coperte da MDR. Esempio: Tracce identificate di un attacco mirato o di una minaccia sconosciuta, che richiedono ulteriori indagini utilizzando metodi forensi digitali
Normal	▶ Può essere assegnato a incidenti che, a giudizio del fornitore, possono influire sull'efficienza o sulle prestazioni delle risorse del Cliente coperte da MDR o portare a singoli casi di compromissione dei dati.
Low	▶ Può essere assegnato a incidenti che, a giudizio del fornitore, non influiscono in modo significativo sull'efficienza o sulle prestazioni delle risorse del Cliente coperte da MDR. Esempio: Identificato potenziale software indesiderato: adware, riskware, non-virus, ecc.

Il livello di priorità predefinito dell'incidente è "Basso".

Recapiti

ENTRA IN CONTATTO CON LA NOSTRA REALTÀ

Richiedi subito una consulenza

Sede: Via Achille Grandi, 8 - Brescia (BS) 25125 - Italy

Tel: (+39) 030 2306877

Fax: (+39) 030 2315512

Mail: info@secoges.com

Sito Web: www.secoges.com

P.IVA e C.F. 02913430985