STORMSHIELD

XDR

Migliora l'efficenza operativa della tua infrastruttura informatica

Di fronte alla specializzazione dei criminali informatici e al loro *modus operandi*, le aziende stanno moltiplicando l'impiego di prodotti destinati alla sicurezza. Tuttavia, il successo ricorrente di questi attacchi dimostra l'inefficacia di tale approccio. Infatti, la molteplicità dei punti di protezione della rete e dei terminali, insieme a una politica di sicurezza eterogenea, determinano una scarsa reattività nei confronti degli attacchi.

Il proliferare di soluzioni di rilevamento richiede configurazioni sempre più complesse, genera eventi multipli e numerosi con comportamenti difficili da interpretare e correlare per gli amministratori. Questa mancanza di visibilità limita la reattività, che di fatto si traduce in un livello di protezione inferiore.

XDR **by Stormshield**

In qualità di operatore di fiducia nel settore della sicurezza informatica, Stormshield presenta una nuova offerta per:

- ridurre i rischi e migliorare la produttività delle operazioni informatiche,
- colmare le lacune inerenti all'integrazione di soluzioni di sicurezza eterogenee,
- proporre una soluzione completa per la sicurezza della vostra infrastruttura,
- correlare gli eventi segnalati dal sistema di protezione della rete (SNS) e delle postazioni di lavoro (SES),
- avvisare in tempo reale,
- gestire gli elementi di risposta e correzione.

Controllo di tutti gli elementi XDR

Gestione degli incidenti di sicurezza da un'unica postazione

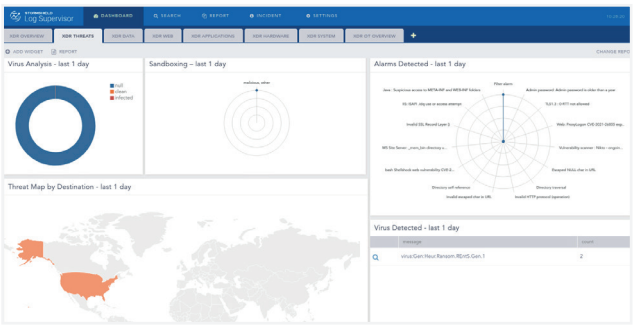
Miglioramento della produttività e dell'efficienza operativa

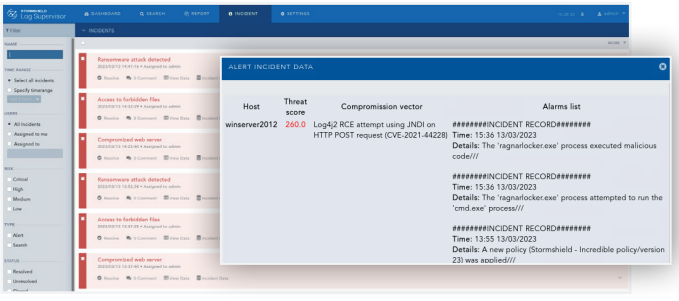
Un'offerta XDR **completamente integrata e gestita**

La sintesi perfetta di Stormshield Network Security per la protezione della rete e Stormshield Endpoint Security per la protezione degli endpoint, supportata dall'esperienza di Stormshield nella Threat Intelligence per anticipare le minacce.

Il tutto orchestrato da Stormshield Log Supervisor per allertare in tempo reale e garantire una risposta rapida e sostenibile sia sulla rete che sui terminali.

In breve: una soluzione di protezione 100% europea, 100% affidabile.





Stormshield XDR

CONTROLLO • PRODUTTIVITÀ • COERENZA

#01

FILE INFETTO

Attacco

- Apertura del file malevolo ricevuto via e-mail
- Esecuzione di un "dropper"
- Recupero della carica virale e innesco dell'attacco

Risposta

- Azione correttiva mediante isolamento della postazione di lavoro dalla rete.
- Arresto dei processi malevoli sul terminale

#02

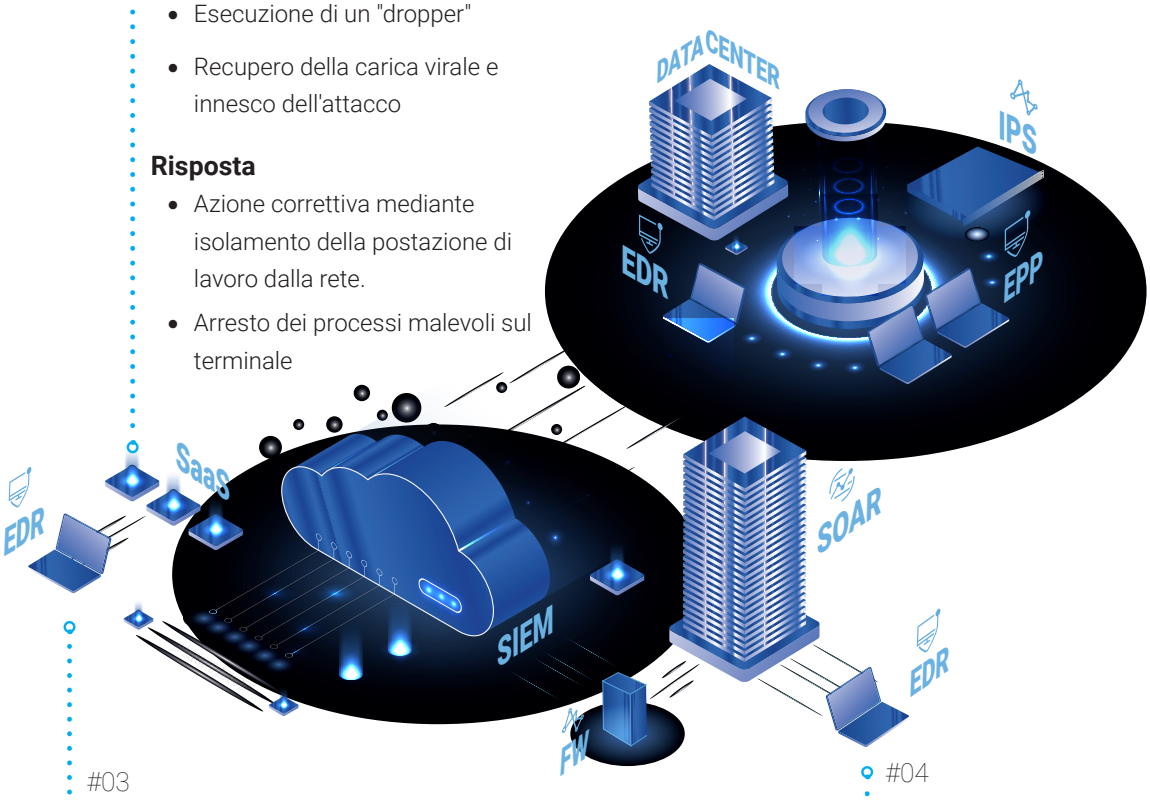
SERVER WEB CHE SUBISCE un attacco DDoS

Attacco

- Invio di una moltitudine di connessioni che saturano il server

Risposta

- Limitazione alle sole connessioni affidabili
- Limitazione delle connessioni sul server per proteggerne l'integrità.



#03

CHIAVETTA USB INFETTA

Attacco

- Introduzione di un dropper nel PC
- Connessione a un server di Command & Control (C2)
- Recupero della carica virale dal server
- Tentativo di compromissione della postazione di lavoro e avvio della lateralizzazione dell'attacco

Risposta

- Arresto del processo malevolo sul terminale
- Azione correttiva mediante isolamento della postazione di lavoro dalla rete.
- Blocco della chiavetta USB su altre postazioni di lavoro
- Blocco IP C2 sulla protezione della rete

#04

SCOPERTA DELLA RETE INTERNA DA PARTE DELL'AGGRESSORE

Attacco

- Scansione della rete interna
- Scoperta della rete e delle sue vulnerabilità
- Verifica di exploit noti su server critici (AD o Exchange)
- Tentativo di assumere il controllo di risorse critiche

Risposta

- Isolamento della postazione di lavoro compromessa
- Abilitazione dell'IPS sulle connessioni critiche

Soluzione proprietaria

Operiamo nel settore della sicurezza informatica da oltre 15 anni, offrendo soluzioni conformi ai requisiti europei.

Certificazioni

Le nostre tecnologie, certificate secondo gli standard europei più elevati, garantiscono la massima protezione delle informazioni strategiche e sensibili dei nostri clienti.

Ecosistema

Collaboriamo con soggetti terzi per sviluppare soluzioni comuni, condividere informazioni sulle minacce e migliorare collettivamente le difese dei nostri clienti.

www.stormshield.com

Stormshield, scoprite la nostra linea di prodotti:

Sicurezza informatica delle reti e delle infrastrutture IT

Tramite le loro funzionalità di base, le soluzioni Stormshield Network Security garantiscono una sicurezza completa e una protezione della rete ad alte prestazioni. **Per una sicurezza efficiente e scalabile**.

Sicurezza informatica delle postazioni di lavoro

Stormshield Endpoint Security è in grado di modificare in maniera **dinamica le proprie operazioni di sicurezza in base all'ambiente circostante** e di analizzare contestualmente l'accesso alle applicazioni e alle risorse aziendali in base alla posizione della postazione di lavoro.

Sicurezza informatica dei dati sensibili

La soluzione Stormshield Data Security, basata sulla crittografia dei dati end-to-end, si configura come un'offerta completa per **il controllo dei dati sensibili all'interno dell'azienda e della privacy** delle e-mail.