STORMSHIELD

Attack Surface Management e Security Policy Enforcement

"Un approccio moderno alla sicurezza informatica"

SU DI ME

$ whoami

{

“Name” : Davide,

“Surname” : Pala,

“Nickname” : Skullb0y,

“Role” : Ingegnere di prevendita per il centro sud Italia,

“Description” : Cybersecurity passionate,

“Other” : Cyber Saiyan co-founder,

}

STORMSHIELD

STORMSHIELD

La scelta **EUROPEA** per la cybersecurity.

Parte di **Airbus**, uno dei gruppi industriali più grande del mondo.

Vendor orientato prevalentemente alla realizzazione di tecnologie di sicurezza.

Cosa è sicurezza?

Condizione oggettiva esente da pericoli,
o garantita contro eventuali pericoli.

STORMSHIELD

Il pericolo nel contesto cyber

Attacco

Azioni condotte da terze parti volte a distruggere l’operatività aziendale col fine di estorcere denaro o porre l’organizzazione in situazione svantaggiosa.

Incidente

Risultato di cambiamenti, modifiche od uso improprio e involontario degli asset aziendali che impatta sulla disponibilità o integrità dei sistemi

Furto

Sottrazione di informazioni di valore per l’organizzazione.

La superfice di attacco e la sua gestione

L’insieme degli elementi (canali di comunicazione, entry e exit points o dati) che un attaccante può sfruttare al fine di esfliltrare dati, controllare dispositivi o software.
Il mantenimento della superficie di attacco la più ridotta possibile è alla base delle misure di sicurezza di base.
La gestione della superficie di attacco è quindi il processo di audit, analisi e gestione di tutti gli elementi che la compongono.

Gestione della superficie di attacco

discovery

L’insieme delle attività attive e passive volte ad individuare e mappare gli asset presenti nell’organizzazione

Analysis

Ogni asset va analizzato e catalogato con lo scopo di definire quali asset debbano essere oggetto di remediation

Remediation

In questa fase vengono applicate le azioni correttive volte a mitigare le criticità individuate nella fase di analisi.

ASM e cybersecurity

Come contestualizzare il concetto di ASM nella sicurezza dell’organizzazione.

Cyber kill chain e ciclo di vita dell’attacco

STORMSHIELD

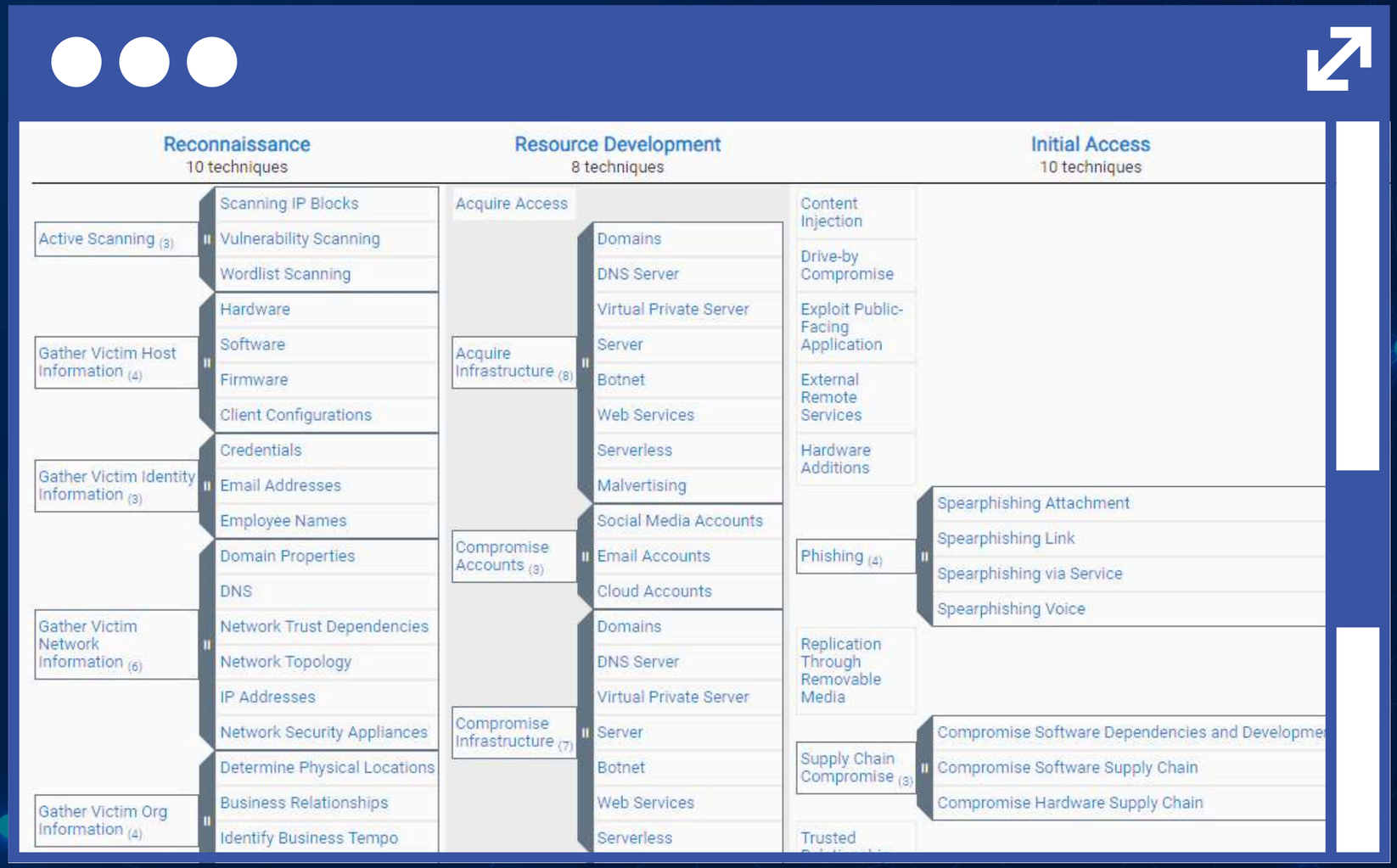
MITRE AT&CK: razionalizzare l’attacco

La **Adversarial Tactics, Techniques, and Common Knowledge** o **MITRE ATT&CK** è un framework per classificare e descrivere i cyber attacchi e le intrusioni creata della Mitre Corporation e rilasciata nel 2013.

STORMSHIELD

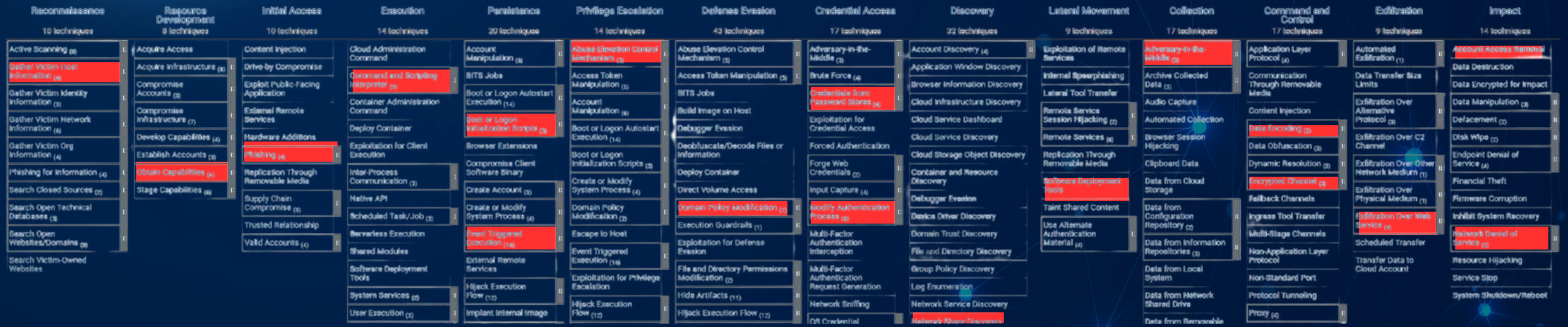
MITRE AT&CK: razionalizzare l’attacco

Contiene:
196 tecniche
411 Sotto tecniche



STORMSHIELD

MITRE AT&CK: razionalizzare l’attacco



L’insieme delle tecniche utilizzate rappresenta l’intero ciclo di vita dell’attacco

STORMSHIELD

MITRE AT&CK: razionalizzare l’attacco

Neutralizzare uno o più tecniche equivale a ridurre o neutralizzare completamente l’impatto dell’attacco

STORMSHIELD

Un nuovo approccio è possibile?

oggi più di ieri abbiamo bisogno di un approccio non proprio nuovo ma sicuramente più efficace!

Il modello CID

Competenza

La competenza è alla base della cybersecurity. La vastità di questo dominio impone una preparazione verticale sul tema.

Importanza

I processi di security, per essere efficaci, devono prevalere sulle dinamiche operative o portare ad un appropriato tavolo di confronto.

Dinamicità

Gli strumenti utilizzati devono rispondere nel modo più dinamico possibile e garantire il pieno controllo sulle tecnologie che implementano.

Il meccanismo di protezione di SES

La soluzione mira ad identificare e bloccare le dinamiche che caratterizzano i malware o le attività potenzialmente dannose, attraverso un’ analisi comportamentale operata direttamente sull’endpoint.

STORMSHIELD

Il meccanismo di protezione di SES

La soluzione mira ad identificare e bloccare le dinamiche che caratterizzano i malware o le attività potenzialmente dannose, attraverso un' analisi comportamentale operata direttamente sull'endpoint.

Meccanismo basato su un granulare sistema di regole che permette un controllo estremamente puntuale. Le regole messe a disposizione dallo SCSL sono integrabili con regole di detection e hardening custom create dagli amministratori.

STORMSHIELD

Il meccanismo di protezione di SES

La soluzione mira ad identificare e bloccare le dinamiche che caratterizzano i malware o le attività potenzialmente dannose, attraverso un' analisi comportamentale operata direttamente sull'endpoint.

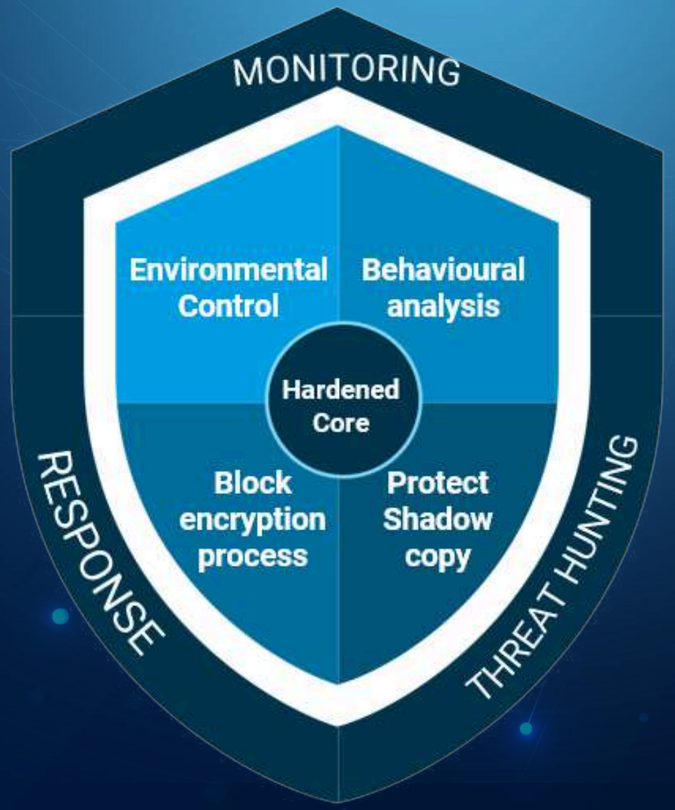
Meccanismo basato su un granulare sistema di regole che permette un controllo estremamente puntuale. Le regole messe a disposizione dallo SCSL sono integrabili con regole di detection e hardening custom create dagli amministratori.

La possibilità di creare politiche di hardening custom in unione con attività di adversary simulation, consente all'organizzazione di sviluppre un meccanismo di difesa su misura estremamente efficace.

STORMSHIELD

Stormshield Endpoint Security

La prima soluzione che consente di costruire la propria, personale, strategia di difesa. Passando dal paradigma della protezione reattiva a quello della protezione proattiva.

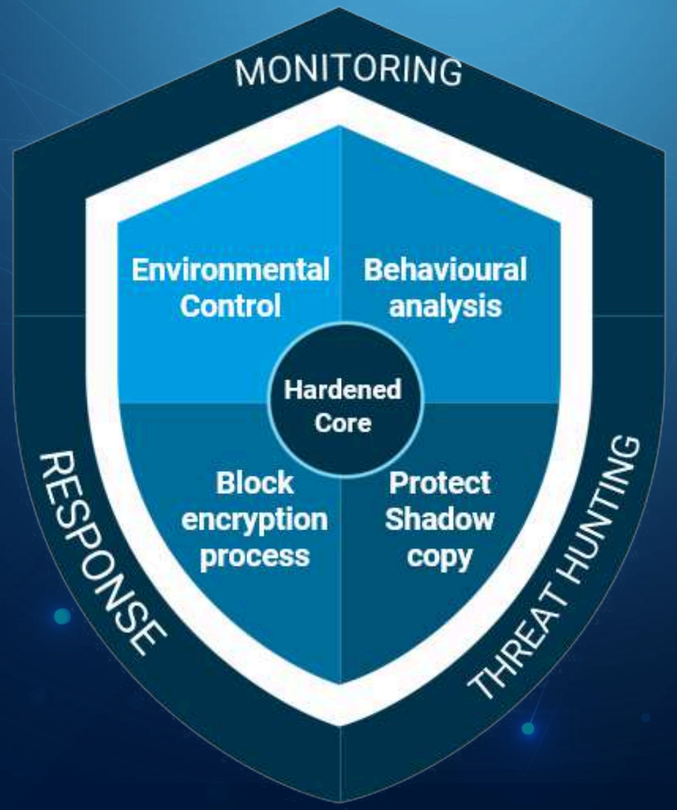


STORMSHIELD

Stormshield Endpoint Security

La prima soluzione che consente di costruire la propria, personale, strategia di difesa. Passando dal paradigma della protezione reattiva a quello della protezione proattiva.

Un’efficace strumento che unisce alle tecniche di hardening, tipiche di un EPP, le funzionalità di detection e reaction caratteristiche degli EDR, garantendo protezione e visibilità.



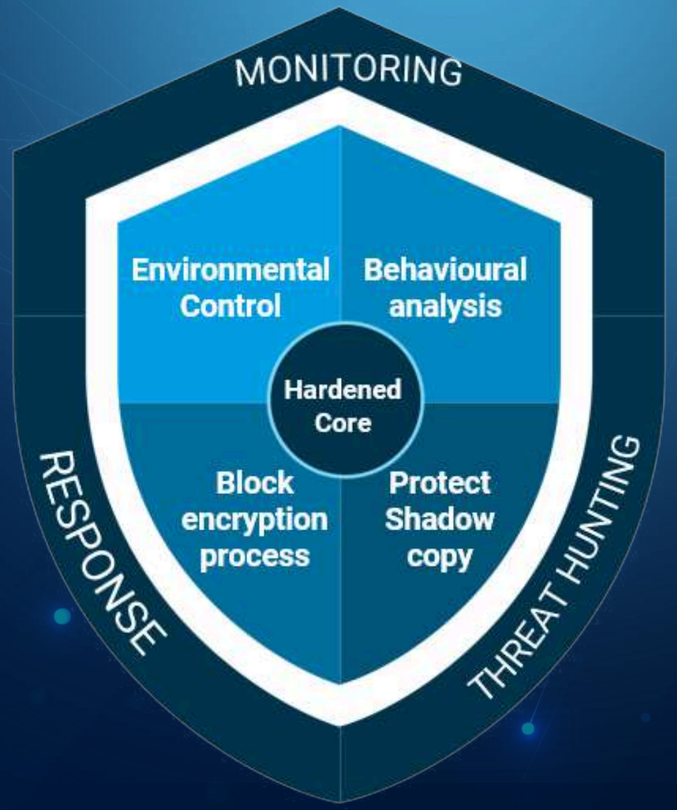
STORMSHIELD

Stormshield Endpoint Security

La prima soluzione che consente di costruire la propria, personale, strategia di difesa. Passando dal paradigma della protezione reattiva a quello della protezione proattiva.

Un’efficace strumento che unisce alle tecniche di hardening, tipiche di un EPP, le funzionalità di detection e reaction caratteristiche degli EDR, garantendo protezione e visibilità.

Agent autonomo in grado di garantire la protezione in qualsiasi condizione, inclusi contesti dove è assente la comunicazione con internet o con il backend.



STORMSHIELD

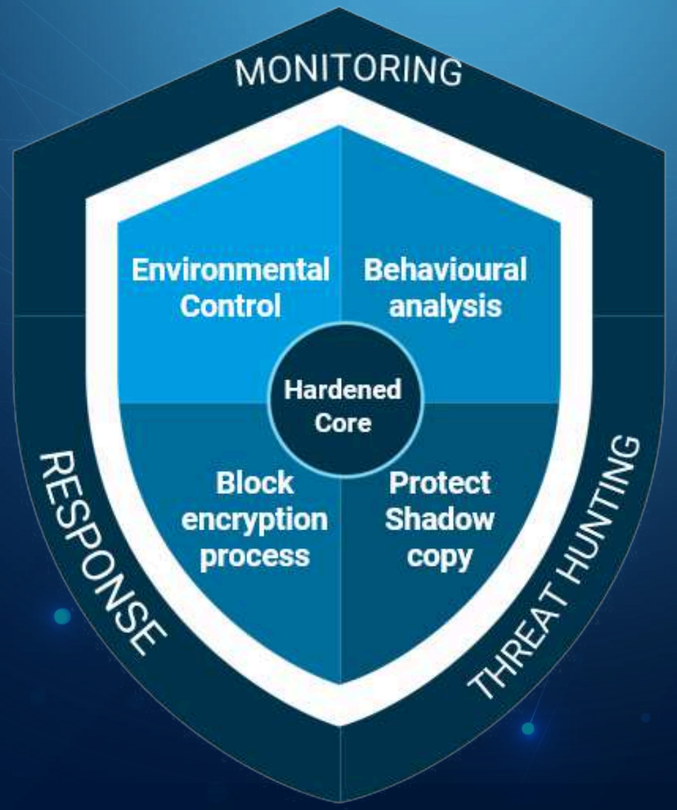
Stormshield Endpoint Security

La prima soluzione che consente di costruire la propria, personale, strategia di difesa. Passando dal paradigma della protezione reattiva a quello della protezione proattiva.

Un prodotto efficace anche nella prevenzione degli attacchi Living Of the Land, grazie all' approccio olistico che valuta il contesto operativo di qualsiasi processo, inclusi quelli dell' OS.

Un'efficace strumento che unisce alle tecniche di hardening, tipiche di un EPP, le funzionalità di detection e reaction caratteristiche degli EDR, garantendo protezione e visibilità.

Agent autonomo in grado di garantire la protezione in qualsiasi condizione, inclusi contesti dove è assente la comunicazione con internet o con il backend.



STORMSHIELD

Stormshield Endpoint Security

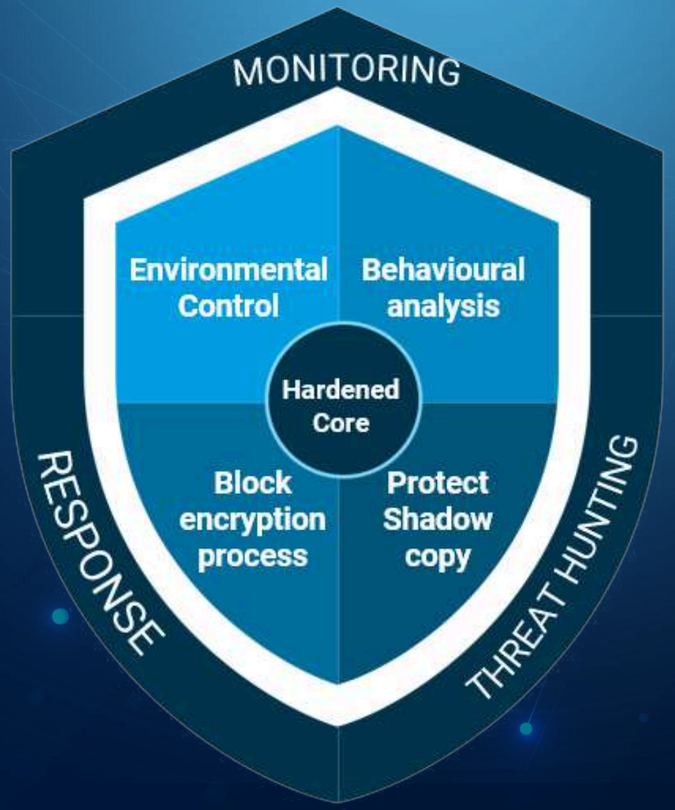
La prima soluzione che consente di costruire la propria, personale, strategia di difesa. Passando dal paradigma della protezione reattiva a quello della protezione proattiva.

Un prodotto efficace anche nella prevenzione degli attacchi Living Of the Land, grazie all' approccio olistico che valuta il contesto operativo di qualsiasi processo, inclusi quelli dell' OS.

Un'efficace strumento che unisce alle tecniche di hardening, tipiche di un EPP, le funzionalità di detection e reaction caratteristiche degli EDR, garantendo protezione e visibilità.

Agent resiliente. Un meccanismo di verifica, operato in modo vicendevole dai singoli componenti dell' agent, permette di rilevare prontamente qualsiasi situazione di malfunzionamento o compromissione.

Agent autonomo in grado di garantire la protezione in qualsiasi condizione, inclusi contesti dove è assente la comunicazione con internet o con il backend.



STORMSHIELD

Stormshield Endpoint Security

La prima soluzione che consente di costruire la propria, personale, strategia di difesa. Passando dal paradigma della protezione reattiva a quello della protezione proattiva.

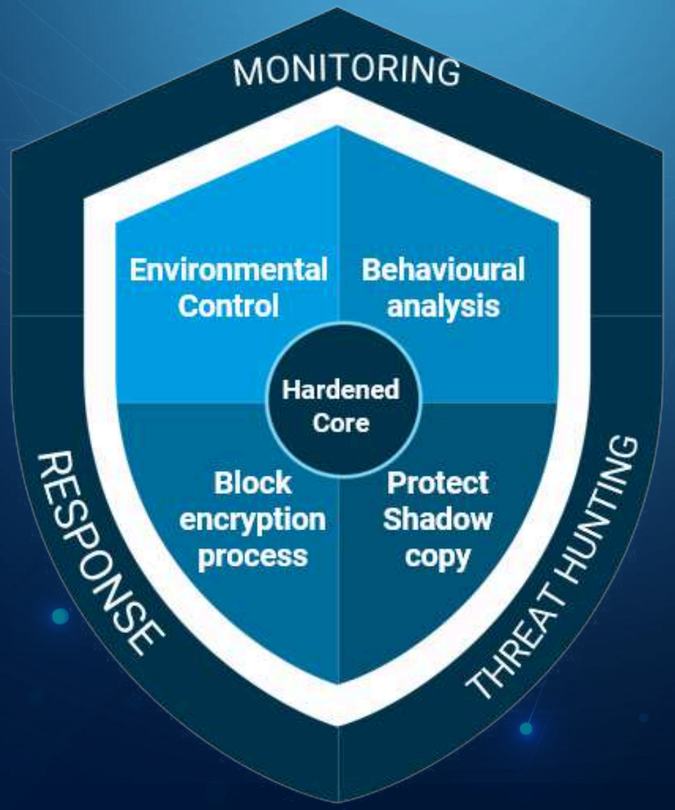
Un prodotto efficace anche nella prevenzione degli attacchi Living Of the Land, grazie all' approccio olistico che valuta il contesto operativo di qualsiasi processo, inclusi quelli dell' OS.

Un'efficace strumento che unisce alle tecniche di hardening, tipiche di un EPP, le funzionalità di detection e reaction caratteristiche degli EDR, garantendo protezione e visibilità.

Agent resiliente. Un meccanismo di verifica, operato in modo vicendevole dai singoli componenti dell' agent, permette di rilevare prontamente qualsiasi situazione di malfunzionamento o compromissione.

Agent autonomo in grado di garantire la protezione in qualsiasi condizione, inclusi contesti dove è assente la comunicazione con internet o con il backend.

Il supporto alle YARA rules ed ad IoC custom, insieme alla possibilità di eseguire script custom, rende SES un'efficace strumento nelle attività di threat hunting.



STORMSHIELD

Thank You

STORMSHIELD

CYBER ACT FORUM 2024