



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

La scelta **EUROPEA** per la
cybersecurity.



STORMSHIELD

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

Vendor orientato
prevalentemente alla
realizzazione di tecnologie
di sicurezza.



STORMSHIELD

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 superficie 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 esfiltrare 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

Reconnaissance 10 techniques	Resource Development 8 techniques	Initial Access 10 techniques	Execution 14 techniques	Persistence 20 techniques	Privilege Escalation 14 techniques	Defense Evasion 43 techniques	Credential Access 17 techniques	Discovery 32 techniques	Lateral Movement 9 techniques	Collection 17 techniques	Command and Control 17 techniques	Exfiltration 9 techniques	Impact 14 techniques
Active Scanning (5) Gather Victim Host Information (4) Gather Victim Identity Information (3) Gather Victim Network Information (4) Gather Victim Org Information (4) Phishing for Information (4) Search Closed Sources (2) Search Open Technical Databases (3) Search Open Websites/Domains (3) Search Victim-Owned Websites	Acquire Access Acquire Infrastructure (6) Compromise Accounts (2) Compromise Infrastructure (7) Develop Capabilities (4) Establish Accounts (2) Obtain Capabilities (4) Stage Capabilities (4)	Content Injection Drive-by Compromise Exploit Public-Facing Application External Remote Services Hardware Additions Phishing (4) Replication Through Removable Media Supply Chain Compromise (3) Trusted Relationship Valid Accounts (4)	Cloud Administration Command Command and Scripting Interpreter (3) Container Administration Command Deploy Container Exploitation for Client Execution Inter-Process Communication (3) Native API Scheduled Task/Job (3) Serverless Execution Shared Modules Software Deployment Tools System Services (2) User Execution (3)	Account Manipulation (4) BITS Jobs Boot or Logon Autostart Execution (14) Boot or Logon Initialization Scripts (3) Browser Extensions Compromise Client Software Binary Create Account (3) Create or Modify System Process (4) Domain Policy Modification (2) Escape to Host Event Triggered Execution (14) External Remote Services Hijack Execution Flow (12) Implant Internal Image	Abuse Elevation Control Mechanism (3) Access Token Manipulation (3) Account Manipulation (4) Boot or Logon Autostart Execution (14) Boot or Logon Initialization Scripts (3) Create or Modify System Process (4) Domain Policy Modification (2) Execution Guardrails (1) Escape to Host Event Triggered Execution (14) Exploitation for Privilege Escalation Hijack Execution Flow (12)	Abuse Elevation Control Mechanism (3) Access Token Manipulation (3) BITS Jobs Build Image on Host Debugger Evasion Deobfuscate/Decode Files or Information Deploy Container Direct Volume Access Domain Policy Modification (2) Execution Guardrails (1) Exploitation for Defense Evasion File and Directory Permissions Modification (2) Hide Artifacts (11) Hijack Execution Flow (12)	Adversary-in-the-Middle (3) Brute Force (4) Credentials from Password Stores (4) Exploitation for Credential Access Forced Authentication Forge Web Credentials (2) Input Capture (4) Modify Authentication Process (3) Multi-Factor Authentication Interception Multi-Factor Authentication Request Generation Network Sniffing Out Credential	Account Discovery (4) Application Window Discovery Browser Information Discovery Cloud Infrastructure Discovery Cloud Service Dashboard Cloud Service Discovery Cloud Storage Object Discovery Container and Resource Discovery Debugger Evasion Device Driver Discovery Domain Trust Discovery File and Directory Discovery Group Policy Discovery Log Enumeration Network Service Discovery Network Share Discovery	Exploitation of Remote Services Internal Spearphishing Lateral Tool Transfer Remote Service Session Hijacking (2) Remote Services (3) Replication Through Removable Media Software Deployment Tools Taint Shared Content Use Alternate Authentication Material (4)	Adversary-in-the-Middle (3) Archive Collected Data (3) Audio Capture Automated Collection Browser Session Hijacking Clipboard Data Data from Cloud Storage Data from Configuration Repository (2) Data from Information Repositories (3) Data from Local System Data from Network Shared Drive Data from Removable	Application Layer Protocol (4) Communication Through Removable Media Content Injection Data Encoding (2) Data Obfuscation (3) Dynamic Resolution (3) Encrypted Channel (2) Fallback Channels Ingress Tool Transfer Multi-Stage Channels Non-Application Layer Protocol Non-Standard Port Protocol Tunneling Proxy (4)	Automated Exfiltration (1) Data Transfer Size Limits Exfiltration Over Alternative Protocol (3) Exfiltration Over C2 Channel Exfiltration Over Other Network Medium (1) Exfiltration Over Physical Medium (1) Exfiltration Over Web Service (4) Scheduled Transfer Transfer Data to Cloud Account	Account Access Removal Data Destruction Data Encrypted for Impact Data Manipulation (3) Defacement (2) Disk Wipe (2) Endpoint Denial of Service (4) Financial Theft Firmware Corruption Inhibit System Recovery Network Denial of Service (2) Resource Hijacking Service Stop System Shutdown/Reboot

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.

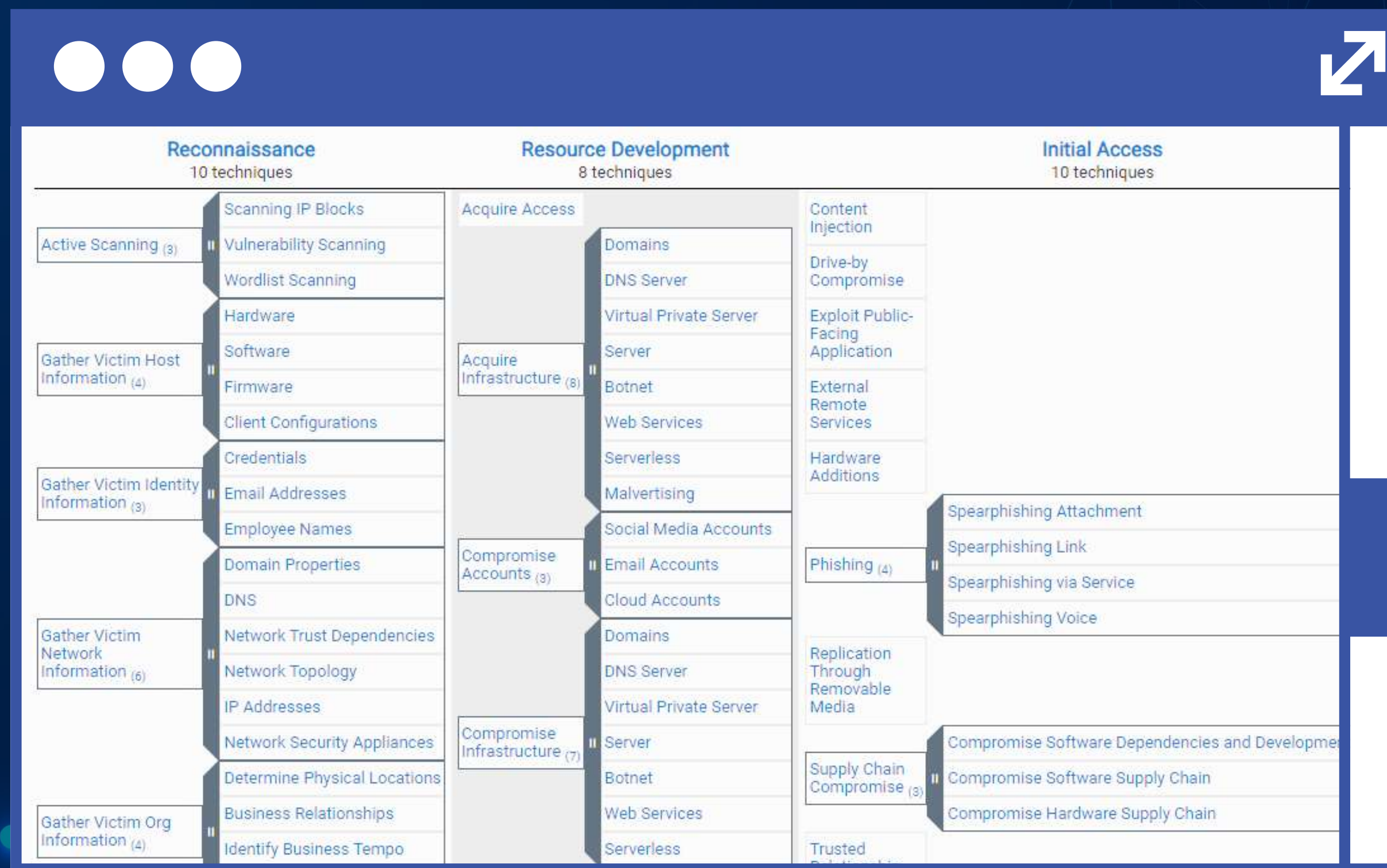


STORMSHIELD



MITRE AT&CK: razionalizzare l'attacco

Contiene:
196 tecniche
411 Sotto tecniche





MITRE AT&CK: razionalizzare l'attacco

Reconnaissance 10 techniques	Resource Development 8 techniques	Initial Access 10 techniques	Execution 14 techniques	Persistence 20 techniques	Privilege Escalation 14 techniques	Defense Evasion 43 techniques	Credential Access 17 techniques	Discovery 32 techniques	Lateral Movement 9 techniques	Collection 17 techniques	Command and Control 17 techniques	Exfiltration 9 techniques	Impact 14 techniques
Active Scanning (2)	Acquire Access	Content Injection	Cloud Administration Command	Account Manipulation (4)	Abuse Elevation Control Mechanism (2)	Abuse Elevation Control Mechanism (2)	Adversary-in-the-Middle (3)	Account Discovery (4)	Exploitation of Remote Services	Adversary-in-the-Middle (3)	Application Layer Protocol (4)	Automated Exfiltration (1)	Account Access Removal
Gather Victim Host Information (4)	Acquire Infrastructure (6)	Drive-by Compromise	Command and Scripting Interpreter (1)	BITS Jobs	Access Token Manipulation (3)	Access Token Manipulation (3)	Brute Force (4)	Application Window Discovery	Internal Spearphishing	Archive Collected Data (3)	Communication Through Removable Media	Data Transfer Size Limits	Data Destruction
Gather Victim Identity Information (3)	Compromise Accounts (2)	Exploit Public-Facing Application	Container Administration Command	Boot or Logon Autostart Execution (14)	Account Manipulation (4)	BITS Jobs	Credentials from Password Stores (4)	Browser Information Discovery	Lateral Tool Transfer	Audio Capture	Content Injection	Exfiltration Over Alternative Protocol (3)	Data Manipulation (3)
Gather Victim Network Information (4)	Compromise Infrastructure (7)	External Remote Services	Deploy Container	Boot or Logon Initialization Scripts (3)	Boot or Logon Autostart Execution (14)	Build Image on Host	Exploitation for Credential Access	Cloud Infrastructure Discovery	Remote Service Session Hijacking (2)	Automated Collection	Data Encoding (2)	Exfiltration Over C2 Channel	Defacement (2)
Gather Victim Org Information (4)	Develop Capabilities (4)	Hardware Additions	Exploitation for Client Execution	Browser Extensions	Boot or Logon Initialization Scripts (3)	Debugger Evasion	Forced Authentication	Cloud Service Dashboard	Remote Services (6)	Browser Session Hijacking	Data Obfuscation (3)	Exfiltration Over Other Network Medium (1)	Disk Wipe (2)
Phishing for Information (4)	Establish Accounts (3)	Phishing (4)	Inter-Process Communication (3)	Compromise Client Software Binary	Create or Modify System Process (4)	Deobfuscate/Decode Files or Information	Forge Web Credentials (2)	Cloud Service Discovery	Replication Through Removable Media	Clipboard Data	Dynamic Resolution (3)	Exfiltration Over Physical Medium (1)	Endpoint Denial of Service (4)
Search Closed Sources (2)	Obtain Capabilities (4)	Replication Through Removable Media	Native API	Create Account (3)	Create or Modify System Process (4)	Deploy Container	Input Capture (4)	Container and Resource Discovery	Software Deployment Tools	Data from Cloud Storage	Encrypted Channel (2)	Exfiltration Over Web Service (4)	Financial Theft
Search Open Technical Databases (3)	Stage Capabilities (4)	Supply Chain Compromise (3)	Scheduled Task/Job (3)	Create or Modify System Process (4)	Domain Policy Modification (2)	Direct Volume Access	Modify Authentication Process (3)	Debugger Evasion	Taint Shared Content	Data from Configuration Repository (2)	Fallback Channels	Ingress Tool Transfer	Firmware Corruption
Search Open Websites/Domains (6)		Trusted Relationship	Serverless Execution	Event Triggered Execution (14)	Escape to Host	Execution Guardrails (1)	Multi-Factor Authentication Interception	Device Driver Discovery	Use Alternate Authentication Material (4)	Data from Information Repositories (3)	Ingress Tool Transfer	Multi-Stage Channels	Inhibit System Recovery
Search Victim-Owned Websites		Valid Accounts (4)	Shared Modules	External Remote Services	Event Triggered Execution (14)	Exploitation for Defense Evasion	Multi-Factor Authentication Request Generation	Domain Trust Discovery		Data from Local System	Multi-Stage Channels	Non-Application Layer Protocol	Network Denial of Service (3)
			Software Deployment Tools	Hijack Execution Flow (12)	Exploitation for Privilege Escalation	File and Directory Permissions Modification (2)	Network Sniffing	File and Directory Discovery		Data from Network Shared Drive	Non-Standard Port	Scheduled Transfer	Resource Hijacking
			System Services (2)	Implant Internal Image	Hijack Execution Flow (12)	Hide Artifacts (11)	Out Credential	Group Policy Discovery		Data from Removable	Protocol Tunneling	Transfer Data to Cloud Account	Service Stop
			User Execution (3)			Hijack Execution Flow (12)		Log Enumeration			Proxy (4)		System Shutdown/Reboot
								Network Service Discovery					
								Network's Shared Resources					

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



STORMSHIELD



MITRE AT&CK: razionalizzare l'attacco

Reconnaissance 10 techniques	Resource Development 8 techniques	Initial Access 10 techniques	Execution 14 techniques	Persistence 20 techniques	Privilege Escalation 14 techniques	Defense Evasion 43 techniques	Credential Access 17 techniques	Discovery 32 techniques	Lateral Movement 9 techniques	Collection 17 techniques	Command and Control 17 techniques	Exfiltration 9 techniques	Impact 14 techniques
Active Scanning (5)	Acquire Access	Content Injection	Cloud Administration Command	Account Manipulation (4)	Abuse Elevation Control Mechanism (2)	Abuse Elevation Control Mechanism (2)	Adversary-in-the-Middle (3)	Account Discovery (4)	Exploitation of Remote Services	Adversary-in-the-Middle (3)	Application Layer Protocol (4)	Automated Exfiltration (1)	Account Access Removal
Gather Victim Host Information (4)	Acquire Infrastructure (6)	Drive-by Compromise	Command and Scripting Interpreter (5)	BITS Jobs	Access Token Manipulation (3)	Access Token Manipulation (3)	Brute Force (4)	Application Window Discovery	Internal Spearphishing	Archive Collected Data (3)	Communication Through Removable Media	Data Transfer Size Limits	Data Destruction
Gather Victim Identity Information (3)	Compromise Accounts (2)	Exploit Public-Facing Application	Container Administration Command	Boot or Logon Autostart Execution (14)	Account Manipulation (4)	BITS Jobs	Credentials from Password Stores (4)	Browser Information Discovery	Lateral Tool Transfer	Audio Capture	Content Injection	Exfiltration Over Alternative Protocol (3)	Data Manipulation (3)
Gather Victim Network Information (4)	Compromise Infrastructure (7)	External Remote Services	Deploy Container	Boot or Logon Initialization Scripts (3)	Boot or Logon Autostart Execution (14)	Build Image on Host	Exploitation for Credential Access	Cloud Infrastructure Discovery	Remote Service Session Hijacking (2)	Automated Collection	Data Encoding (3)	Exfiltration Over C2 Channel	Data Encrypted for Impact
Gather Victim Org Information (4)	Develop Capabilities (4)	Hardware Additions	Exploitation for Client Execution	Browser Extensions	Boot or Logon Initialization Scripts (3)	Debugger Evasion	Forced Authentication	Cloud Service Dashboard	Remote Services (6)	Browser Session Hijacking	Data Obfuscation (3)	Exfiltration Over Other Network Medium (1)	Defacement (2)
Phishing for Information (4)	Establish Accounts (3)	Phishing (4)	Inter-Process Communication (3)	Compromise Client Software Binary	Create or Modify System Process (4)	Deobfuscate/Decode Files or Information	Forge Web Credentials (2)	Cloud Service Discovery	Replication Through Removable Media	Clipboard Data	Dynamic Resolution (3)	Exfiltration Over Physical Medium (1)	Disk Wipe (2)
Search Closed Sources (2)	Obtain Capabilities (4)	Replication Through Removable Media	Native API	Create Account (3)	Create or Modify System Process (4)	Deploy Container	Input Capture (4)	Cloud Storage Object Discovery	Software Deployment Tools	Data from Cloud Storage	Exfiltrated Channel (4)	Exfiltration Over Web Service (4)	Endpoint Denial of Service (4)
Search Open Technical Databases (3)	Stage Capabilities (4)	Supply Chain Compromise (3)	Scheduled Task/Job (3)	Create or Modify System Process (4)	Domain Policy Modification (2)	Direct Volume Access	Weakly Authenticated Process (3)	Debugger Evasion	Taint Shared Content	Data from Configuration Repository (2)	Fallback Channels	Ingress Tool Transfer	Financial Theft
Search Open Websites/Domains (6)		Trusted Relationship	Serverless Execution	Event Triggered Execution (14)	Escape to Host	Execution Guardrails (1)	Multi-Factor Authentication Interception	Device Driver Discovery	Use Alternate Authentication Material (4)	Data from Information Repositories (3)	Multi-Stage Channels	Non-Application Layer Protocol	Firmware Corruption
Search Victim-Owned Websites		Valid Accounts (4)	Shared Modules	External Remote Services	Event Triggered Execution (14)	Exploitation for Defense Evasion	Multi-Factor Authentication Request Generation	Domain Trust Discovery		Data from Local System	Non-Standard Port	Protocol Tunneling	Inhibit System Recovery
			Software Deployment Tools	Hijack Execution Flow (12)	Exploitation for Privilege Escalation	File and Directory Permissions Modification (2)	Network Sniffing	File and Directory Discovery		Data from Network Shared Drive	Proxy (4)	Scheduled Transfer	Network Denial of Service (3)
			System Services (2)	Implant Internal Image	Hijack Execution Flow (12)	Hide Artifacts (11)	Out Credential	Group Policy Discovery		Data from Removable		Transfer Data to Cloud Account	Resource Hijacking
			User Execution (3)			Hijack Execution Flow (12)		Log Enumeration					Service Stop
								Network Service Discovery					System Shutdown/Reboot
								Discovery of Shared Resources					

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!



Competenza

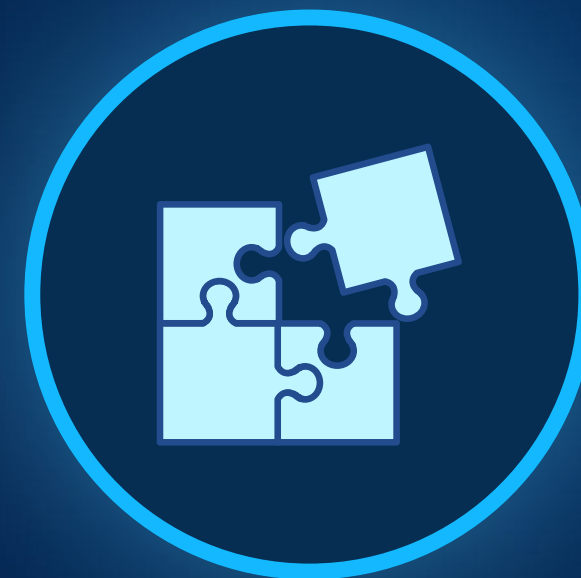
La competenza è alla base della cybersecurity. La vastità di questo dominio impone una preparazione verticale sul tema.

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 modello CID

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.

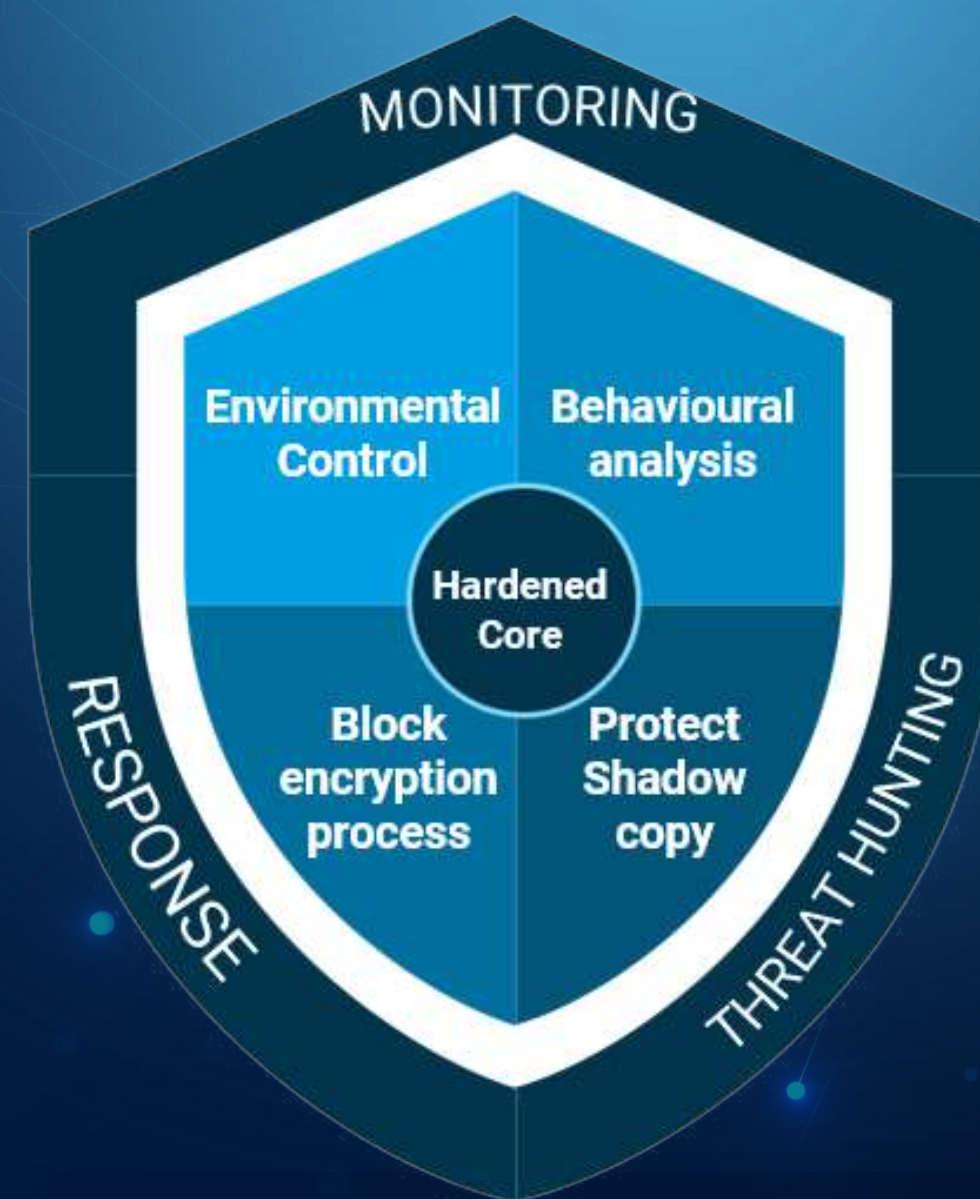
Meccanismo basato su un granulare sistema di regole che permette un controllo estremamente puntuale. Le regole messe a disposizione dallo SCSL sono integrabili con regole di detection e hardening custom create dagli amministratori.

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



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.

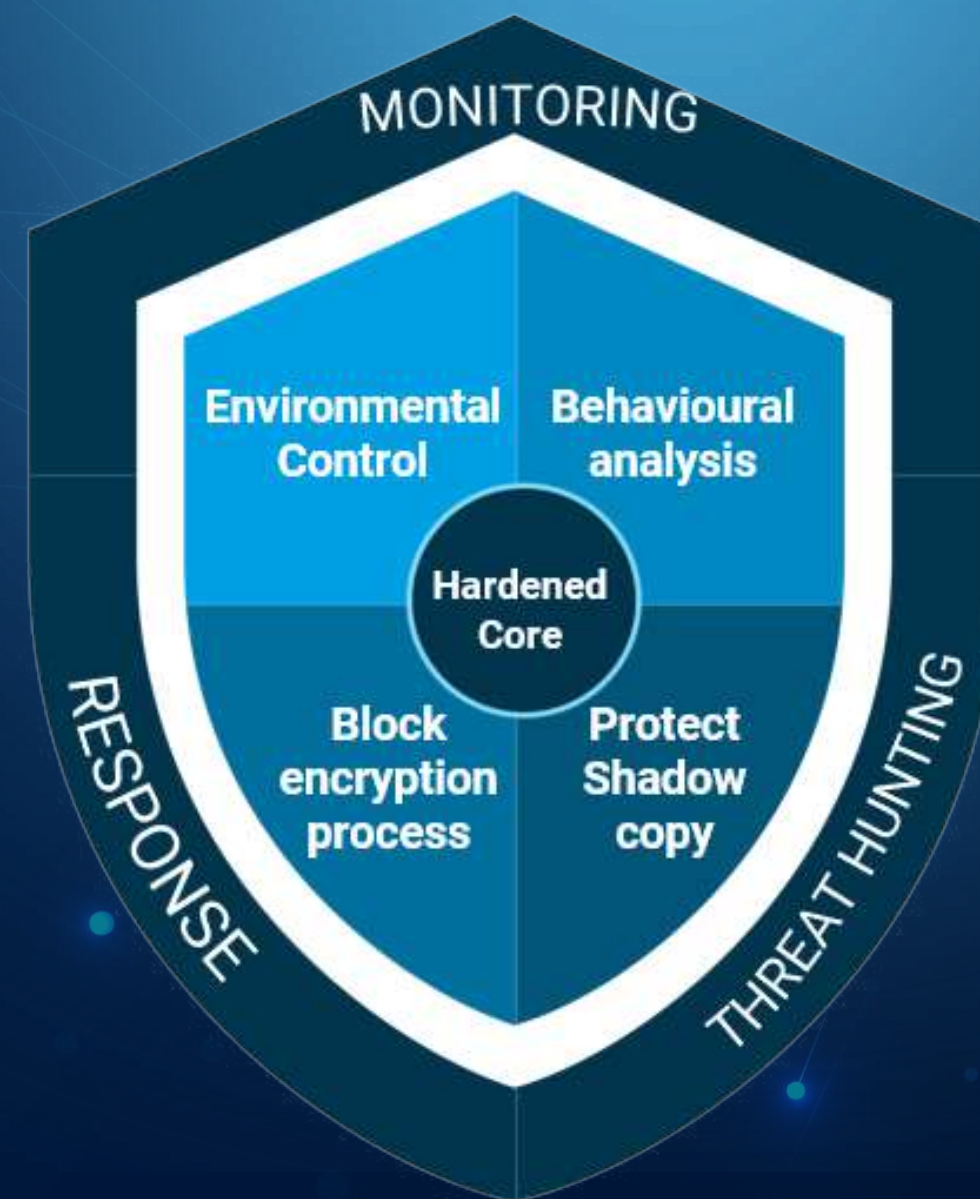


STORMSHIELD

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.



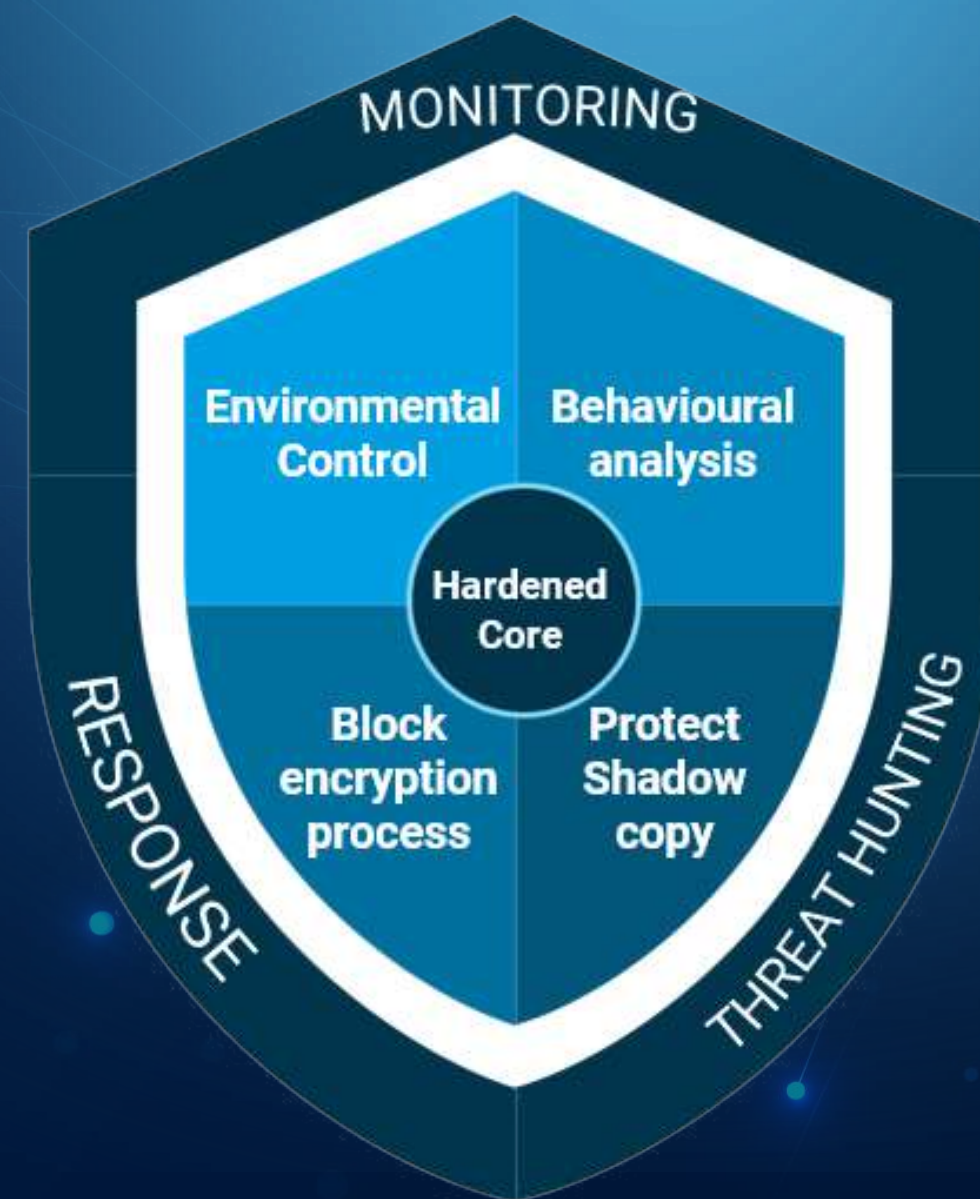
STORMSHIELD

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

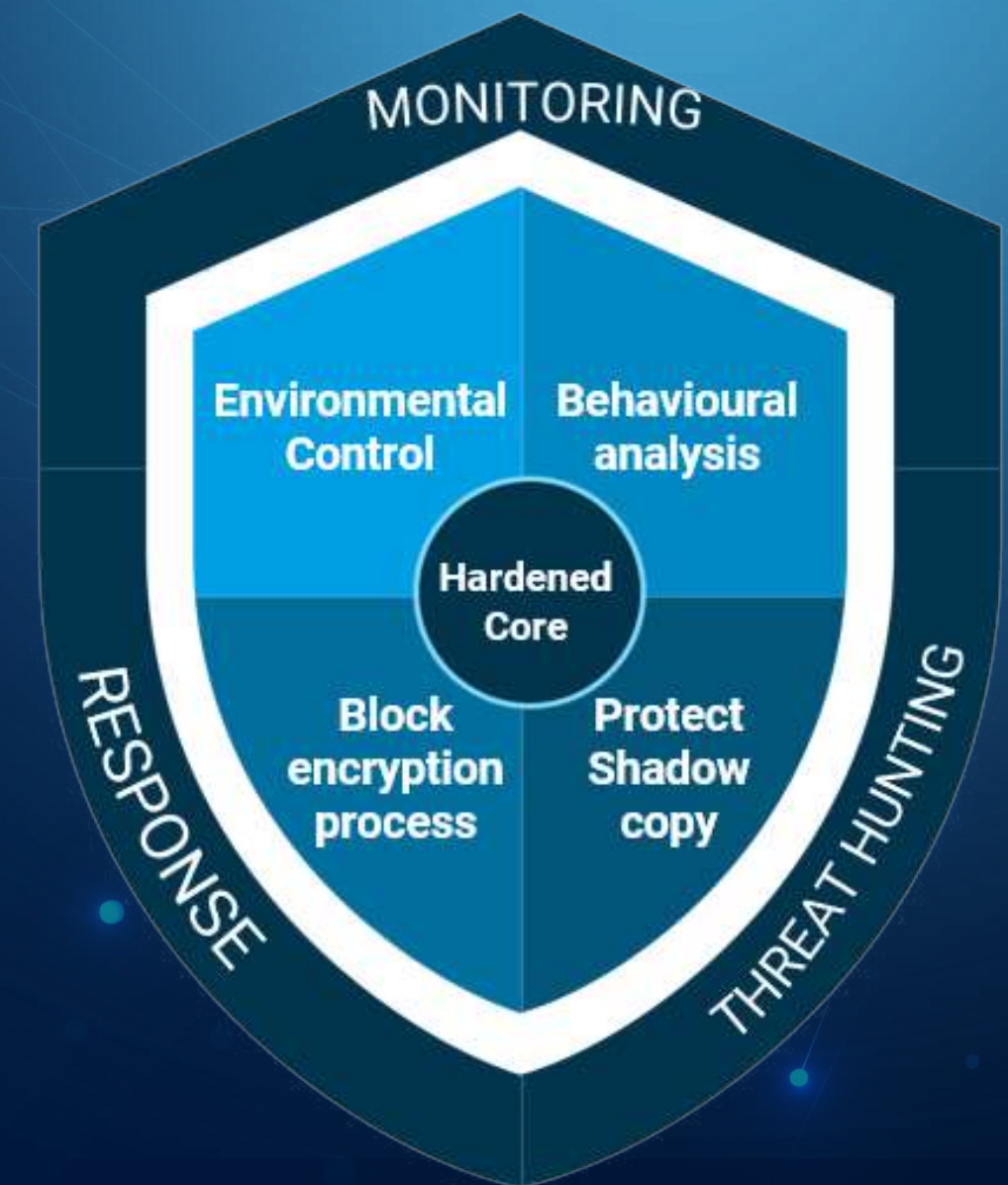
Stormshield Endpoint Security

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

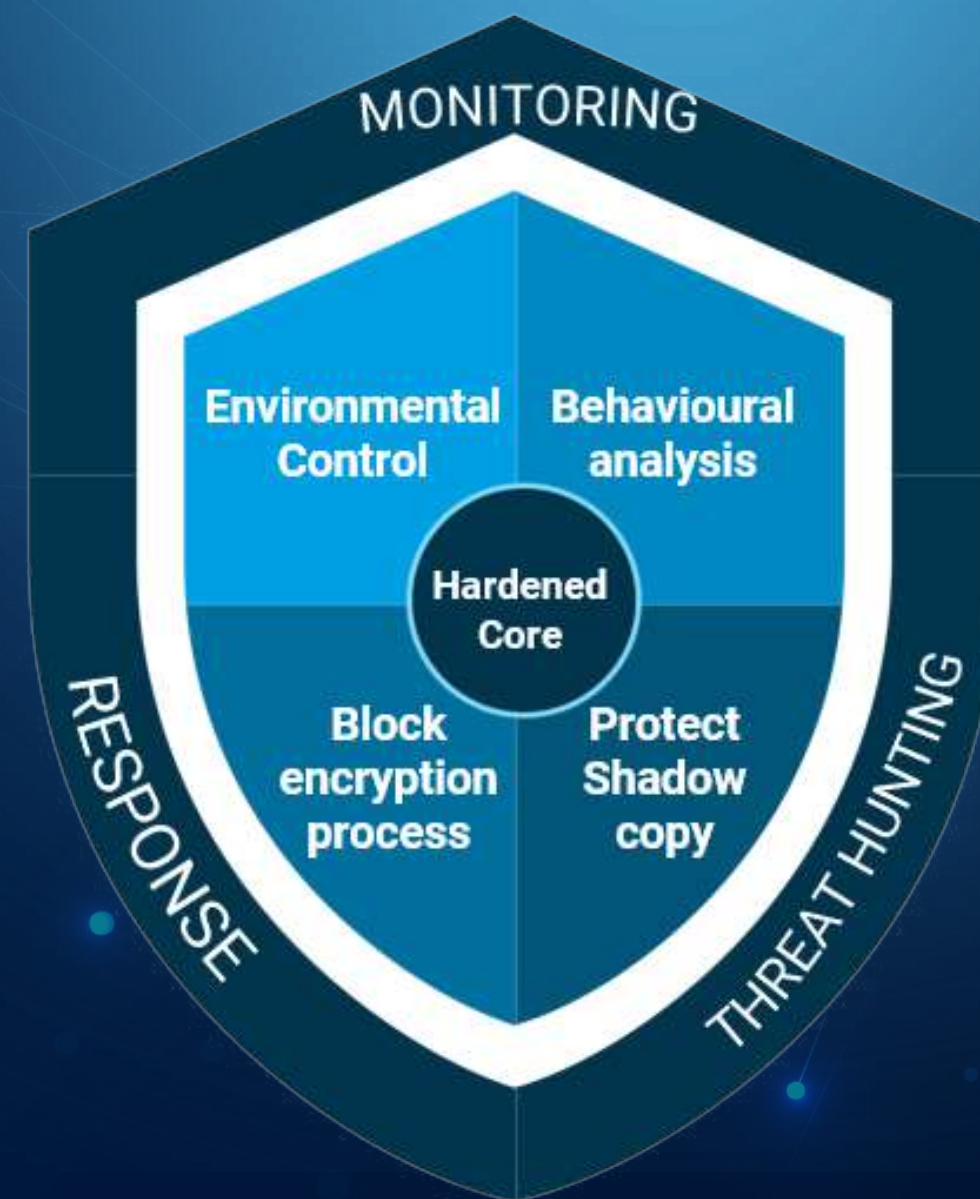
La prima soluzione che consente di costruire la propria, personale, strategia di difesa. Passando dal paradigma della protezione reattiva a quello della protezione proattiva.

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.

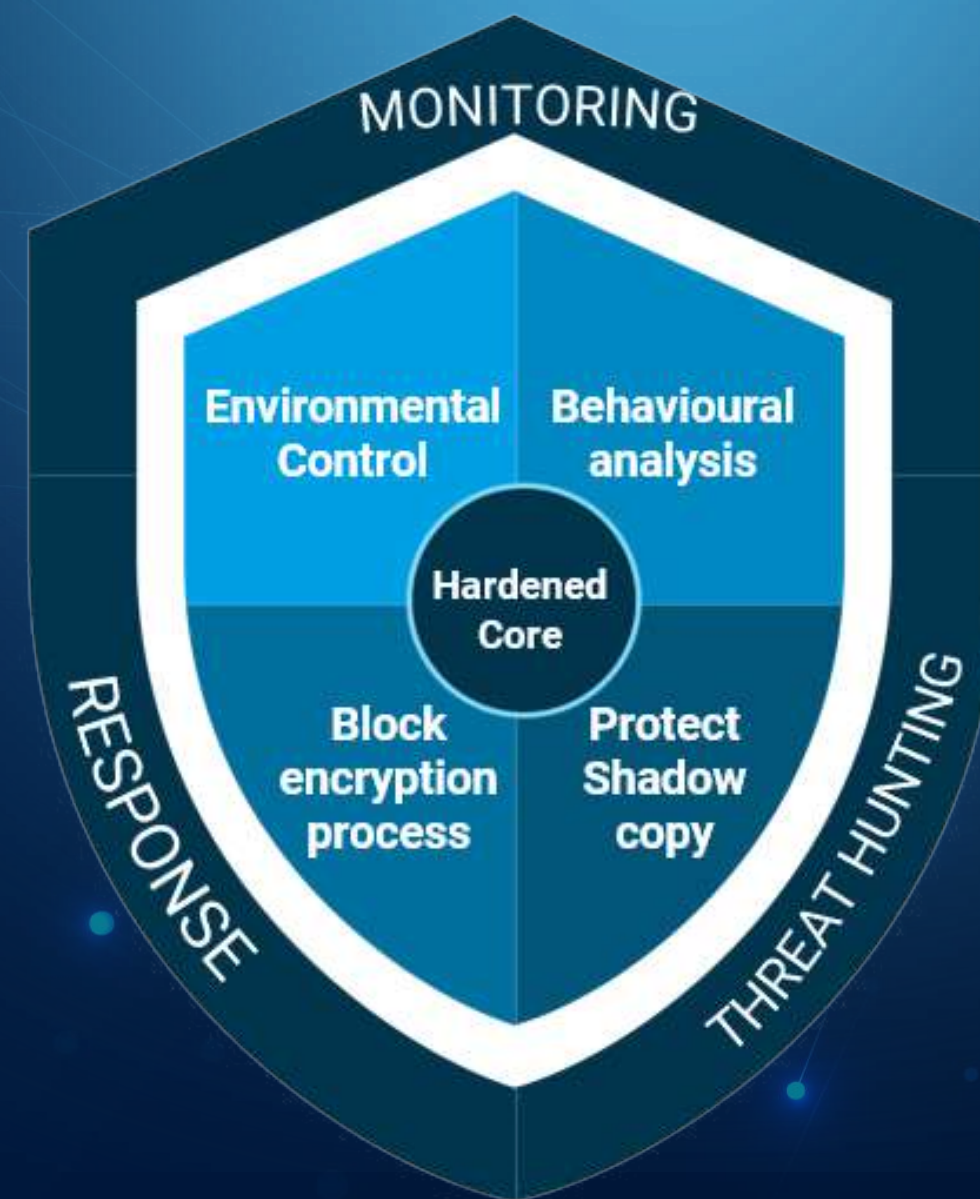
Un prodotto efficace anche nella prevenzione degli attacchi Living Of the Land, grazie all' approccio olistico che valuta il contesto operativo di qualsiasi processo, inclusi quelli dell' OS.

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

