STORMSHIELD

ENDPOINT SECURITY

STORMSHIELD **EVOLUTION**

Erhöhen Sie den Schutz Ihrer Workstations durch eine proaktiv arbeitende EDR-Lösung

Deployment

LOKAL UND SAAS

API REST

INTEGRATION ECOSYSTEM

Detailliert konfigurierbar

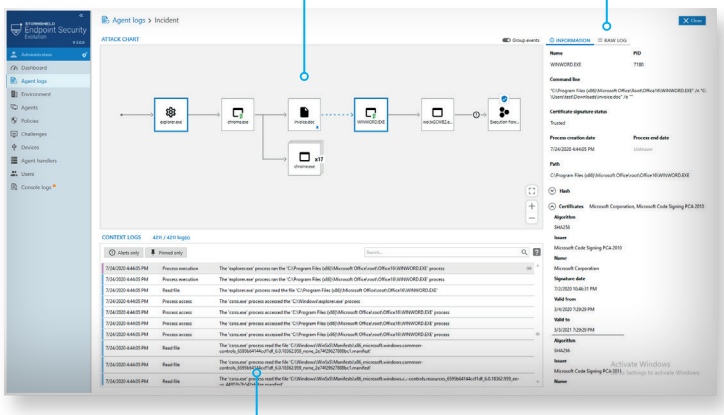
ANPASSBARE SICHERHEITSPARAMETER

Standalone

SCHUTZ VON GETRENNTEN UMGEBUNGEN

ANGRIFFSVERLAUF-SCHAUBILD

DETAILANSICHT



EREIGNISLISTE

Optimaler Schutz durch unsere EDR Lösung

Stormshield Endpoint Security Evolution ist der Endpunkt- und Server Schutz der nächsten Generation. Durch signaturlose Analysetechnologie erkennt der Wächter Angriffe und Bedrohungen und reagiert entsprechend.

Proaktive Sicherheit

- Angriffe in Echtzeit stoppen
- Vordefinierte und anpassbare Analysen und Lösungsmaßnahmen
- Angriffsverlauf-Schaubild und Ursachenforschung (IoC, Yara, etc.)

Verhaltensanalysen

- Signaturloser Schutz gegen Zero-day Angriffe
- Bekämpfung von Exploit-Techniken
- Ransomware-Schutz

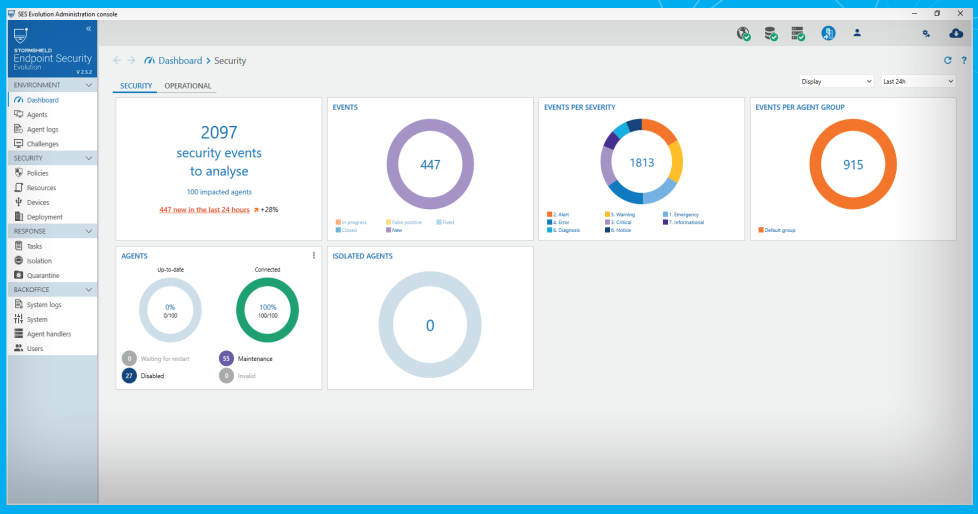
Kontextueller Schutz

- Sicherheitsrichtlinien passen sich automatisch der Umgebung an, sogar im Offline-Betrieb
- Richtlinien anpassbar nach Nutzergruppen
- Standard Sicherheitsrichtlinien und Updates direkt vom Stormshield Customer Security Lab Team

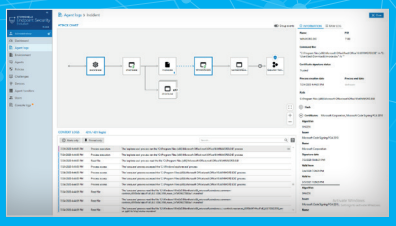
NEXT GENERATION ENDPOINT PROTECTION

MITTLERE UND GROSSE UNTERNEHMEN

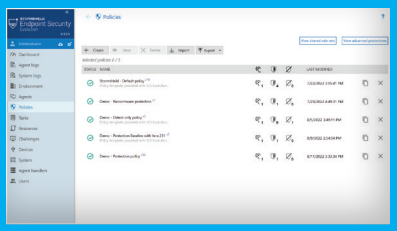
WWW.STORMSHIELD.COM



Dashboard



Detaillierte Ansicht eines Vorfalls



Ansicht der Sicherheitsrichtlinien

FUNKTIONEN

Schutz ohne Signatur

Zero-Day-Schutz gegen bekannte und unbekannte Bedrohungen

Techniken Verhaltensanalyse

- Speicherkorruption (buffer overflow, heap spray)
- Privilegienerweiterung (token stealing)
- Diebstahl sensibler Informationen (keylogging, process access)
- Process Hollowing und seine Varianten
- Code-Injektion (application hooking)

Ransomware-Schutz

- Bösartiger Verschlüsselungsprozess
- Windows Shadow Copy
- Backup-Richtlinie

Personalisierte Abhilfemaßnahmen

- Einen Prozess beenden
- Löschen einer Datei
- Löschen oder Ändern eines Registry-Schlüssels oder seines Wertes
- Wiederherstellen von Dateien, die durch Ransomware verschlüsselt wurden
- Automatische Malware-Quarantäne
- Isolierung kompromittierter Workstations
- Ausführen von PowerShell-Skripten für benutzerdefinierte Aktionen (Stoppen und Entfernen eines Dienstes usw.)

Identifizierung von Indikatoren für Kompromisse (IoC)

- Verdächtiger Text (Dateiname, Hostname, Objektname, usw.)
- Netzwerkinformationen (IP-Adressen, verdächtige URLs, DNS)
- Hash SHA1, SHA256, MD5 und SSDEEP
- Sofortige, geplante oder ereignisbasierte Suche nach Hinweisen auf eine Kompromittierung.
- Schutz vor Umgehung von EDR Erkennungsmechanismen

Sofortige, geplante oder On-Detection-Suche nach Indikatoren für eine Gefährdung

Kontrolle der Peripheriegeräte

- WLAN-Netzwerke • USB-Stick • Bluetooth • Zugriff auf Datenträger • Netzwerkverbindungen • Ausführungskontrolle

Erkennung von Eindringlingen

- Angriffsgraph (Threat Hunting)
- Incident management
- Ereignisweiterleitung (Windows Ereignisse und OSSEC-Regeln)

Optimierter Agent

- Speicherverbrauch
- CPU-Last

Sicherheitsrichtlinien

- Dynamische, kontextabhängige Anpassung
- Verhaltensanalyse und Regelsätze zur Gerätekontrolle, die von Stormshield bereitgestellt und gepflegt werden
- Vorgegebene Modelle
- Unterstützung der Yara-Regeln

Zentrale Verwaltung

- Richtlinienverwaltung durch Agentengruppen
- Rollen-basierte Administratorenverwaltung
- Aktivierung/Deaktivierung von Modulen durch Agentengruppen
  API REST zur nahtlosen Integration mit weiterer Software
  Aktivitätsbericht mit MCS und MCO Indikatoren im HTML-Format
- Automatische E-Mail Benachrichtigung bei Sicherheitsvorfällen

KOMPATIBILITÄT DES AGENTS

AGENT

Systemelemente

CPU:
Mindestens 1 Kern mit 1 GHz - empfohlen 2 Kerne mit 2 GHz

RAM:
Mindestens 1 GB - empfohlen 2 GB

Festplattenspeicher:
100 MB (Installation) - 200 MB (Daten)

Betriebssystem

Client:
Windows 7, 8.1, 10 und 11

Server:
Windows Server 2012 R2, 2016, 2019 und 2022 (auch in der Core-Version) und 2008 R2

VERWALTUNG

Möglichkeit der SaaS- oder Vor-Ort-Verwaltung

FÜR DAS ON-PREMISE-MANAGEMENT

Back-End

CPU:
Mindestens 1 Kern mit 1 GHz - empfohlen 2 Kerne mit 2 GHz

RAM:
Mindestens 1 GB - empfohlen 2 GB

Festplattenspeicher:
100 MB (Installation) - 200 MB (Daten)Windows Server 2012 R2, 2016, 2019 und 2022 (außer Core-Version)

Agenten-Handler

CPU:
Mindestens 2 Kerne mit 2 GHz

RAM:
Mindestens 2 GB

Festplattenspeicher:
200 MB (Installation) - 1 GB (Daten - mindestens)

Client:
Windows 7, 8.1, 10 und 11

Server:
Windows Server 2012 R2, 2016, 2019 und 2022 (auch in der Core-Version) und 2008 R2

Datenbank:
SQL Server 2017 und höher