STORMSHIELD

XDR

Steigern Sie die Cyber-Betriebseffizienz Ihrer Infrastruktur

Angesichts der Professionalität von Cyberkriminellen und ihres *Modus Operandi* setzen Unternehmen immer mehr Sicherheitsprodukte ein. Doch die immer wiederkehrende Feststellung, dass Angriffe erfolgreich verlaufen, zeigt, wie wenig effektiv dieser Ansatz ist. Die Vielzahl an zu schützenden Netzwerkpunkten und Endgeräten sowie eine uneinheitliche Sicherheitspolitik führen dazu, dass Unternehmen schlechter auf Angriffe reagieren können.

Die vielen Lösungen zur Erkennung von Angriffen erfordern immer komplexere Konfigurationen. Außerdem melden sie mehrere und zahlreiche Ereignisse mit Verhaltensweisen, die für Administratoren schwierig zu interpretieren und miteinander zu verknüpfen sind. Diese mangelnde Übersichtlichkeit schränkt die Reaktionsfähigkeit ein, was sich in der Praxis in einem niedrigeren Schutzniveau niederschlägt.

XDR **von Stormshield**

Als anerkannter, vertrauenswürdiger Anbieter im Bereich Cybersicherheit bietet Stormshield ein neues Produkt, um:

- Risiken zu senken und die Cyber-Betriebseffizienz zu steigern,
- die Lücken zu schließen, die mit der Integration heterogener Sicherheitslösungen einhergehen,
- eine umfassende Lösung für die Sicherheit Ihrer Infrastruktur bereitzustellen,
- Ereignisse zu korrelieren, die durch den Netzwerkschutz (SNS) und den Geräteschutz (SES) gemeldet wurden,
- in Echtzeit Alarm zu schlagen,
- aktiv auf Ereignisse zu reagieren und Abhilfemaßnahmen zu ergreifen.

Kontrolle aller XDR-Elemente

Zentrale Verwaltung von Sicherheitsvorfällen

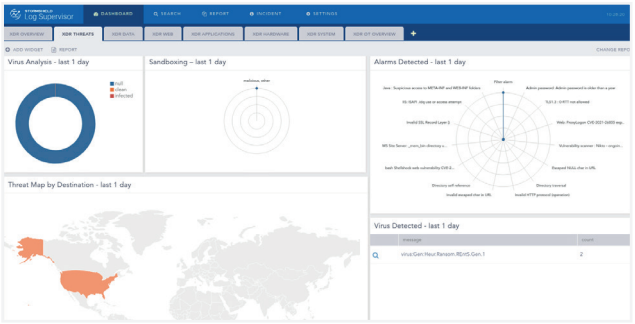
Steigerung der Produktivität und der Cyber-Betriebseffizienz

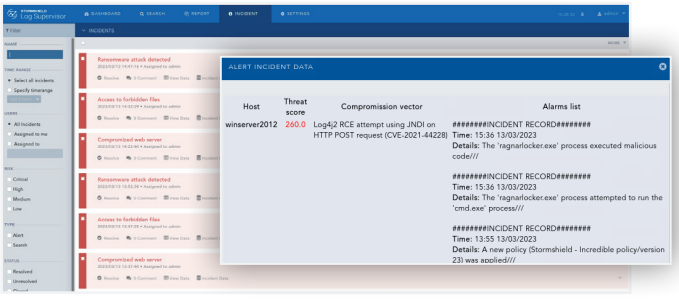
Ein vollständig integriertes und kontrolliertes XDR-Angebot

Die ideale Kombination aus Stormshield Network Security zum **Schutz Ihres Netzwerks** und Stormshield Endpoint Security für die **Sicherheit Ihrer Endgeräte**, verstärkt durch Stormshields Expertise hinsichtlich Threat Intelligence zur **Antizipation von Bedrohungen**.

Das Ganze wird vom Stormshield Log Supervisor orchestriert, um Sie **in Echtzeit zu alarmieren** und **eine schnelle und nachhaltige Reaktion** sowohl im Netzwerk als auch auf Endgeräten zu steuern.

Kurz gesagt: eine Schutzlösung, die 100% europäisch, 100% vertrauenswürdig ist.





Stormshield

XDR

KONTROLLE • PRODUKTIVITÄT • KOHÄRENZ

#01
BÖSARTIGE DATEI

Angriff

- Öffnen der per E-Mail eingegangenen bösartigen Datei
- Ausführen eines Injektors (Dropper)
- Aufbau der Viruslast und Auslösen des Angriffs

Reaktion

- Behebung durch Netzisolierung der Workstation
- Stoppen von bösartigen Prozessen auf dem Terminal

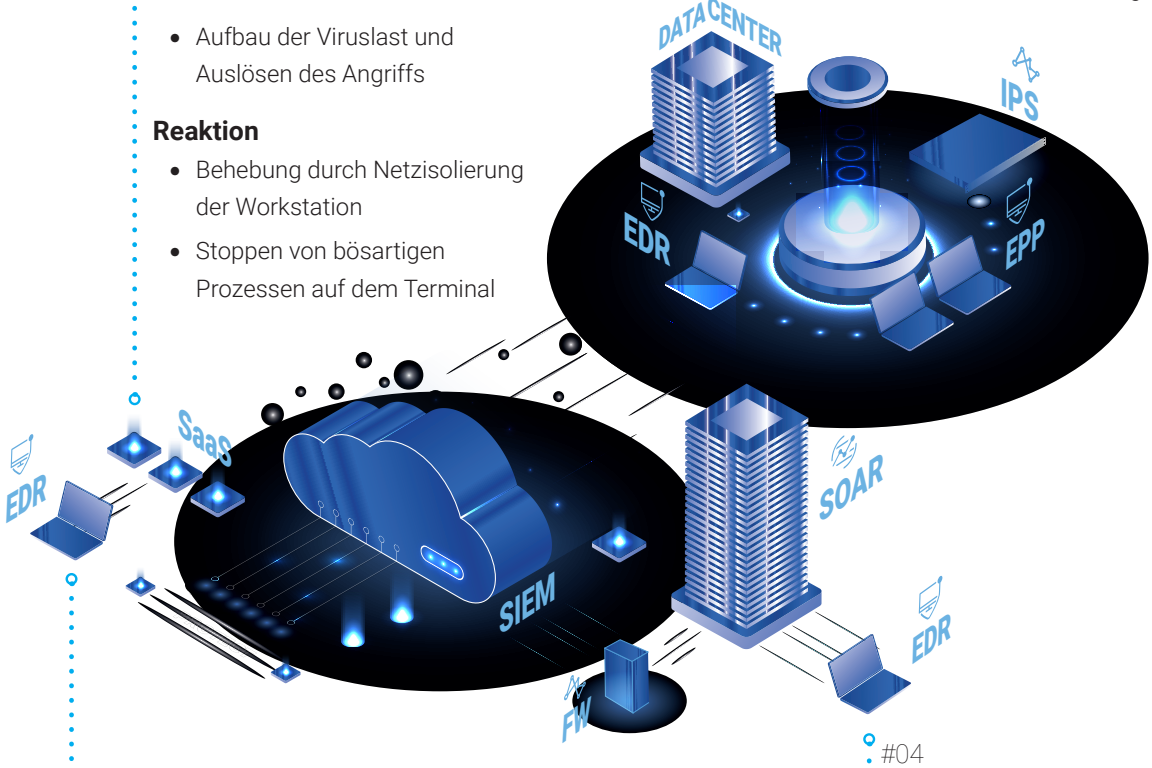
#02
WEB-SERVER, DER EINEM DDoS-ANGRIFF AUSGESETZT IST

Angriff

- Senden einer Vielzahl von Verbindungsanfragen, die den Server überlasten

Reaktion

- Beschränkung auf vertrauenswürdige Verbindungen
- Aktivieren der Verbindungsbeschränkung auf dem Server zum Schutz seiner Integrität



#03
BÖSARTIGER USB-STICK

Angriff

- Hinterlegung eines Injektors (Dropper) auf dem PC
- Verbindung zu einem Command & Control-Server (C2)
- Aufbau der Virenlast durch den Server
- Versuch, den Rechner zu kompromittieren und Beginn der lateralen Ausbreitung des Angriffs

Reaktion

- Stoppen von bösartigen Prozessen auf dem Terminal
- Behebung durch Netzisolierung der Workstation
- Blockieren des USB-Sticks an anderen Workstations
- Blockieren der IP des C2-Servers in der Netzwerksicherheitslösung

#04
ANALYSE DES INTERNEN NETZWERKS DURCH ANGREIFER

Angriff

- Scannen des internen Netzwerks
- Analyse des Netzwerks und seiner Schwachstellen
- Testen von bekannten Exploits auf wichtigen Servern (AD oder Exchange)
- Versuch, die Kontrolle über kritische Ressourcen zu übernehmen

Reaktion

- Isolierung der kompromittierten Workstation
- Aktivierung von IPS bei kritischen Verbindungen

Eigenständige Lösung

Als französischer Anbieter für Cybersicherheit bieten wir Lösungen an, die den europäischen gesetzlichen Anforderungen entsprechen.

Zertifizierungen

Unsere auf höchster europäischer Ebene zertifizierten Technologien garantieren einen angemessenen Schutz für die strategischen oder vertraulichen Informationen Ihrer Organisation.

Ökosystem

Wir arbeiten mit anderen Unternehmen zusammen, um gemeinsame Lösungen zu entwickeln, Informationen über Bedrohungen auszutauschen und gemeinsam den Schutz unserer Kunden zu verbessern.

www.stormshield.com

Stormshield – Lernen Sie unsere Produkte kennen:

Cybersicherheit für IT-Netzwerke und -Infrastrukturen

Dank ihren Kernfunktionen bieten die Lösungen von Stormshield Network Security umfassende Sicherheit sowie eine hohe Leistung beim Schutz von Netzwerken. **Entscheiden Sie sich für leistungsfähige und skalierbare Sicherheit**.

Cybersicherheit für Workstations

Stormshield Endpoint Security kann **ihre Sicherheitsmaßnahmen dynamisch an die Umgebung** anpassen und gleichzeitig den Zugriff auf Anwendungen und Ressourcen des Unternehmens gemäß dem Standort der Workstation analysieren.

Cybersicherheit für sensible Daten

Unsere Lösung Stormshield Data Security nutzt eine End-to-End-Datenverschlüsselung und bildet ein umfassendes Angebot zur **Überwachung sensibler Daten innerhalb Ihrer Organisation und zum Schutz der Vertraulichkeit** von E-Mails.