Next Generation Intrusion Prevention
We Prevent Intrusions.

Fidelis erkennt Angriffe und verhindert Datendiebstahl in Echtzeit.

Die Herausforderung

Die ursprüngliche Aufgabe eines Intrusion-Prevention-Systems (IPS) war das Erkennen von Angriffen auf bekannte Server-Schwachstellen. Doch die Strategie der Angreifer hat sich mittlerweile geändert. Sie konzentrieren sich nicht mehr ausschließlich auf die Server, sondern greifen auch Endpunkte an. Doch während die Hacker immer neue Wege zu alten Zielen finden, treten herkömmliche IPS auf der Stelle. Mit ihrem größtenteils unveränderten Funktionsumfang erzeugen sie Warnmeldungen mit geringem Wert für die Sicherheitsteams und lassen Angriffe unerkannt passieren.

Fidelis im Vergleich mit traditionellen IPS-Lösungen

	traditionelles IPS	Fidelis
Verwendete Technologie	Deep Packet Inspection	Deep **Session** Inspection™
Erkennungsschwerpunkt	Exploits	Exploits, Verhalten **und** Datendiebstahl
Überwachte Systeme	Server	Server **und** Endpunkte
Erkennungszeitraum	Echtzeit	Echtzeit **und** rückwirkend
Advanced Threat Detection	Sandbox	Regeln, Sandbox **und** Analysen
Überprüfung der Inhalte	Keine	Inbound **und** Outbound
Kontextinformationen	Begrenzt	Detailliert **und** praxistauglich
Aktionen am Endpunkt	Begrenzt	Validierung **und** Behebung

Lösungsansatz

Fidelis nutzt zur Erkennung und Abwehr von Angriffen einen hochmodernen Ansatz, indem es in Echtzeit über alle Ports und Protokolle hinweg die Bestandteile einer Session zusammensetzt und deren Inhalt rekursiv dekodiert. So erkennt es im Inhalt versteckte Exploits, APTs, Spearfishing und andere moderne Angriffe, die traditionelle IPS übersehen.

- **Sessions statt Packets:** Die Session-basierte Herangehensweise ist um einiges effizienter als paketbasierte Signaturen. Fidelis überwacht den gesamten eingehenden und ausgehenden Datenstrom. Das macht es möglich, Angriffe zu erkennen, die paket-basierten IPS entgehen, aber auch Datenabfluss zu erkennen.
- **Bedrohungen statt Schwachstellen:** Durch die Verwendung von dynamischen Yara-Regeln gegenüber statischen Snort-Signaturen müssen diese nicht mehr stetig ergänzt werden, sondern die Bedrohung selber rückt in den Mittelpunkt der Erkennung.
- **Automatisierte Kontextinformationen:** Fidelis bietet Ihnen Alarme mit integrierter Forensik. Damit sehen Sie auf einen Blick, was diesen Alarm erzeugt hat und was davor und danach geschehen ist und können somit schnell und informiert reagieren.
- **Vergangenheit und Gegenwart:** Neue Angriffsvektoren werden automatisiert mit Metadaten aus Netzwerk und Endpunkten abgeglichen, um bereits erfolgte Angriffe aufzudecken und vormals von ihrem IPS unerkannte Bedrohungen zu beseitigen.
- **Netzwerk + Endpunkt:** Fidelis validiert automatisiert Alarme aus dem Netz auf allen Endpunkten, verringert somit False-Positives, zeigt alle betroffenen Endpunkte an und ermöglicht auch remote umgehende Reaktionen auf diesen zur weiteren Eindämmung und Beseitung von Angriffen. Erkennungs- und Behebungszeiten sinken somit massiv.

Vorteile

- **Erkennen von Angriffen, die ein traditionelles IPS übersieht:** Fidelis untersucht als einziger komplette Sessions statt einzelner Pakete. Dadurch werden mehr als nur die Exploits erkannt, die andere traditionelle IPS erkennen können.
- **Angriffe schneller erkennen:** Die automatisiert zur Verfügung gestellten Kontextinformationen sowie die Endpunktvalidierung reduzieren die Zeit, die Analysten zur Erkennung, Auswertung und Einstufung von Alarmmeldungen benötigen von Tagen auf Minuten.
- **Verhaltensbasierte Analysen:** Die automatisierte Verhaltens-analyse macht auch ohne Signaturen noch unbekannte Angriffsmuster sichtbar.
- **Konsolidierung Ihrer Sicherheits-infrastruktur:** Mit Fidelis können Sie verschiedene Tools konsoli-dieren, darunter IPS, modernen Malware-Schutz, Analysetools und Tools zum Schutz vor Datenverlust.
- **Erfüllt Ihre aktuellen Erwartungen:**
  - Mal- und Ransomware stoppen
  - Angriffe in Echtzeit und rückwirkend erkennen
  - Ereignisse verhaltensbasiert analysieren
  - Datendiebstahl verhindern
  - Gefahren automatisiert beseitigen
  - Forensische Details sichern und auswerten

Gartner

„Ein Best-of-Breed Intrusion-Detection- / Intrusion-Prevention-System **kann mit weitaus mehr Bedrohungen aus dem Internet fertig werden als ein altes IPS** mit diversen Verfahren zur Aufdeckung und Prävention."

– Defining Intrusion Detection and Prevention Systems. *Gartner Research, 20. September 2016*

Fidelis erkennt Angriffe, die herkömmliche IPS nicht aufdecken, und ermöglicht Sicherheitsvorfälle umgehend zu bearbeiten, automatisiert zu validieren und dann zu beheben.

Die Lösung im Überblick

Die Produkte von Fidelis wurden konzipiert, um auch komplexe Angriffe von professionellen Gruppen zu erkennen und zu stoppen. Sie werden vor Ort im Kundennetz installiert und können sowohl am Perimeter, am Web-Proxy, als Mail-Gateway oder auch im internen Netz selber eingesetzt werden.

Architektur

- Netzwerksensoren und Endpunktagenten werden in der lokalen Infrastruktur installiert.
- Weitere Komponenten wie ein Speicher für Netzwerk-Metadaten & Endpunkt Ereignis Historie, eine Kommandozentrale sowie die Fidelis-Sandbox werden lokal bereitgestellt.
- Beinhaltet aktuelle Bedrohungsdaten und Regeln von Fidelis und ermöglicht andere Threat Intelligence Quellen frei hinzuzufügen.
- Ein ausgefeiltes Rollenmodell mit voller Mandantenfähigkeit ermöglicht auch den Einsatz durch Externe wie Managed Service Provider.

Fidelis: Next Generation Intrusion Prevention

Schnelle Reaktion im Ernstfall

Durch die Bereitstellung umfangreicher Kontextinformationen bei jedem Alarm verkürzt Fidelis die zur Abwehr von Bedrohungen benötigte Zeit.

Sie erhalten bei jedem Alarm einen vollständigen Rundumblick, der Ihnen zeigt, was vor und nach dem Auslösen des Alarms geschehen ist.

Mit den am Endpunkt validierten und mit relevanten und umfangreichen Informationen angereicherten Warnmeldungen von Fidelis erhalten Sie einen schnellen Überblick über kritische Alarme mit wertvollen forensischen Details und bekommen ohne Zeitverlust sämtliche zugehörigen Spuren, Beweispakete, Sessions und Benutzerdaten. Sie können somit umgehend Maßnahmen ergreifen – alles über eine einzige Benutzeroberfläche.

Eine Auswahl der durch Fidelis bereitgestellten Kontextinformationen

	Fidelis
Schweregrad des Vorfalls	■
Quelle und Ziel	■
Bedrohungsklassifikation	■
Verdächtiges Dateiobjekt	■
Name und Funktionsweise der Malware	■
Alle relevanten forensischen Dateien	■
Dekodierung sämtlicher Sessioninhalte	■
Name und Identität des anvisierten Opfers	■
Alle Sessiondetails und forensischen Daten	■
Community-Bewertung der Warnmeldung	■
Ereignisse vor und nach dem Alarm	■
In der Vergangenheit infiltrierte Endpunkte	■
Alle Netzpunkte mit identischen Ereignissen	■
Andere angegriffene und infiltrierte Endpunkte	■

Demo anfordern: **www.fidelissecurity.com/NextGenIps**

Nehmen Sie Kontakt mit uns auf, wenn Sie mehr über Fidelis erfahren möchten

Fidelis Cybersecurity | +49 30 4081 73 210 | dach@fidelissecurity.com

Fidelis: We Prevent Intrusion. Und das tun wir konsequent und ohne Abstriche. Egal ob Angreifer versuchen, einen Fuß in Ihr Netz zu bekommen oder auf Daten auf Ihren Laptops und Servern zuzugreifen, Fidelis erkennt es umgehend. Dann zeigen wir Ihnen alles, was Sie wissen müssen, um innerhalb von Minuten den Angriff zu beenden (und nicht in Tagen oder gar Wochen). Um mehr über unsere Produkte und Incident-Response-Services zu erfahren, besuchen Sie uns auf www.fidelissecurity.com oder folgen Sie uns per Twitter @FidelisCyber.

 DS_Fidelis_NGIPS_DE_3101