Fidelis Cybersecurity

Datenblatt

Fidelis Network™

Angriffe in jeder Phase aufdecken, analysieren und stoppen

Damit Ihnen kein gefährlicher Angriff verborgen bleibt

Unternehmen investieren Millionen in den Aufbau sicherer Infrastrukturen, die auch die ambitioniertesten Angreifer abwehren sollen. Dennoch gelingt es entschlossenen Angreifern immer wieder, in scheinbar sichere Unternehmensnetzwerke einzudringen und Geschäftsgeheimnisse, vertrauliche Daten und Finanzinformationen zu stehlen. Die in Security Operation Centers tätigen Analysten können die enorme Anzahl von Fällen mittlerweile kaum noch bewältigen. Das führt dazu, dass sie gefährliche Angriffe oft nicht oder erst nach dem Diebstahl geschäftskritischer Daten bemerken.

Erkennen Sie Angriffe, indem Sie den Datenverkehr bis in die Tiefen analysieren, in denen sich die Angreifer verbergen. Decken Sie ihre Tools, Taktiken und Aktivitäten auf, um Datendiebstahl schnell zu untersuchen oder ihm sogar vorzubeugen.

Produktüberblick

Mit Fidelis Network™ sind sicherheitsbewusste Unternehmen in der Lage, komplexe Angriffe in jeder Angriffsphase zuverlässig zu erkennen, analysieren und stoppen. Das Programm analysiert den Netzwerkverkehr des gesamten Unternehmens, selbst bei mehreren Gigabit pro Sekunde, und erkennt die Tools und Tricks, mit denen versierte Angreifer die Sicherheitssysteme anderer Netzwerke umgehen. Mit Fidelis haben Sie die Transparenz, den Kontext und die Geschwindigkeit, um Bedrohungen zu erkennen und Ihr Unternehmen vor Datendiebstahl zu schützen.

- **Erkennt Angriffe, die andere Lösungen übersehen:** Fidelis erkennt nicht nur komplexe Malware, Exploits und C&C-Fernsteuerung, sondern auch das Verhalten von Angreifern, wenn sie ihr Netzwerk ausspionieren und Daten zum Ausschleusen vorbereiten.
- **Gezielte Angriffe früh erkennen und stoppen:** Sie können verdächtiges Verhalten, wie Änderungen von Netzwerk-Metadaten, Fernsteuerbefehle und das Vordringen von Angreifern im Netzwerk, schnell erkennen und Datenverluste rechtzeitig verhindern.
- **Scheinbar unzusammenhängende Aktivitäten richtig interpretieren:** Warnungen und in Netzwerksitzungen erfasste Metadaten werden von automatischen Such- und Analysefunktionen überprüft, um auch Netzwerkaktivitäten, die scheinbar nichts miteinander zu tun haben, miteinander in Verbindung zu setzen und ggf. als Komponenten desselben Angriffs zu erkennen.
- **Vorfälle schneller erkennen und aufklären:** Über eine einzige Benutzeroberfläche erhalten Sie rasch wichtige Informationen, untersuchen Netzwerkdaten anhand von Informationen über aktuelle Bedrohungen und versetzen Sicherheitsanalysen in die Lage, innerhalb von Sekunden nach der Benachrichtigung mit der Untersuchung zu beginnen.

Highlights

Das Verborgene aufdecken: Die zum Patent angemeldeten Funktionen für die Erfassung, Speicherung und automatische Analyse von Metadaten von Fidelis erkennen und analysieren auch gezielte Angriffe, etwa durch komplexe oder speziell auf Ihr Unternehmen zugeschnittene Malware, Exploits und ferngesteuerte Angriffe.

Echtzeit- und Verlaufsanalysen in einer Oberfläche: Verbinden Sie die tiefgehende Analyse von Inhalten mit der Analyse von Verlaufsdaten, untersuchen Sie zurückliegende Ereignisse mit eigens vom Fidelis-Team für Bedrohungsforschung geschriebenen Regeln. So erkennen Sie Bedrohungen in Ihrem System ohne Verzögerung.

Kontext und Inhalt: Unsere Engine für Deep Session Inspection® generiert Metadaten auf Protokoll-, Anwendungs- und Inhaltsebene. Das liefert umfangreichen Kontext, wie ihn andere Lösungen nicht bieten können. Sie können an mehreren Ebenen der Inhaltsstruktur ansetzen und so die Erkennungsmöglichkeiten erweitern.

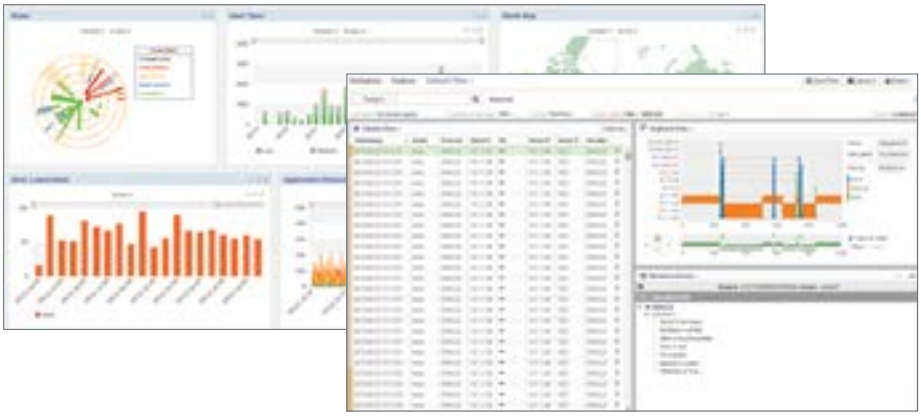
Eine Lösung für das gesamte Netzwerk: Fidelis bietet eng aufeinander abgestimmte Funktionen zur Malware-Analyse, Erkennung von Bedrohungen, Netzwerkforensik, Schutz vor Datendiebstahl und Sicherheitsanalysen.

Geschwindigkeit und Skalierbarkeit: Die Untersuchung von Netzwerksitzungen mit einem Datendurchsatz von mehreren Gigabit pro Sekunde liefert innerhalb von Sekunden aussagekräftige Informationen, so dass Sie aktive Bedrohungen in Systemen jeder Größe erkennen können.

Erkennen Sie mit unserer Engine für „Deep Session Inspection“ und dem Überblick über alle Ports und Protokolle Angriffe, die anderen Lösungen entgehen.

Funktionen

- **Schnellere Untersuchungsergebnisse:** Vereinfachen Sie die bislang zeitraubendste Komponente von Untersuchungen – die Datenerfassung. Damit erkennen Sie viel leichter, was gerade geschieht, und Ihre Fachleute können sich auf die wirklich wichtigen Schritte konzentrieren.
- **Angriffe in jeder Angriffsphase erkennen:** Sie können Angreifer in jeder Phase eines Angriffs erkennen, auch beim Vordringen durch das Netzwerk, beim Installieren von Tools für die Kommunikation mit ihrem Command-and-Control-Server und bei der Vorbereitung des Datendiebstahls.
- **Überblick über alle Ports und Protokolle:** Sie gewinnen den Überblick über den Netzwerkverkehr an allen Ports und mit allen Protokollen und bemerken so die missbräuchliche Nutzung von Protokollen und Diensten auf weniger gängigen Ports. Da die Metadaten aller von Fidelis untersuchten Netzwerksitzungen gespeichert werden, können Sie das Vorgehen der Angreifer auch rückwirkend nachvollziehen.
- **Deep Session Inspection®:** Sie decodieren und analysieren Inhalte in Echtzeit, ganz gleich, wie tief sie eingebettet sind. Unserer „Deep Session Inspection“-Engine entgeht kein einziges Datenpaket im Netzwerk. Sie setzt sie im Arbeitsspeicher zu gepufferten Sitzungen zusammen und decodiert und analysiert darin die Protokolle, Anwendungen und Inhaltsobjekte in Echtzeit – während die Sitzungen noch laufen. So kann Fidelis Anwendungen und gerade auch den Inhalten, die im Netzwerk unterwegs sind, wirklich auf den Grund gehen.
- **Rückwirkende Erkennung und Untersuchung:** Sie können untersuchen, was bei früheren Angriffen geschehen ist. Da Fidelis auf Inhaltsebene umfassende Metadaten von Netzwerk und Endgeräten sammelt, haben Sie eine schlankere, schnellere und kostengünstigere Möglichkeit, Verlaufsdaten zu analysieren.
- **Angreifer im Netzwerk stoppen:** Sie können ohne Proxys von Fremdherstellern einen Angreifer oder eine interne Bedrohung im Netzwerk erkennen und unautorisierte Datenübertragungen in Echtzeit einseitig blockieren – auf allen Ports und für alle Protokolle.
- **Kontinuierliche Suche nach E-Mail-basierten Bedrohungen:** Sensoren in Fidelis Mail verfolgen alle in E-Mails enthaltenen URLs zurück und unterziehen mit ihnen verbundene Folgeaktivitäten im Unternehmen oder in der Cloud einer besonders genauen Überprüfung.



Sie können in derselben Lösung direkt von der Echtzeit-Erkennung zur Untersuchung und zum Einleiten von Gegenmaßnahmen übergehen.

„Mit Playback nachvollziehen, was passiert ist: Sie können den Verlauf eines Angriffs auch später lückenlos nachvollziehen und sehen, welche Daten gestohlen wurden und wer der Angreifer ist. Dazu werden wichtige Daten zu Dateien, Prozessen, Registry, Netzwerk, DNS und URL aufgezeichnet und, gemeinsam mit den wichtigsten Warnungen, automatisch in einer Zeitleiste aufbereitet.“

– IDC, Combined Endpoint and Network Visibility Vital to Combating Advanced Threats, August 2015

Vorteile

- **Besserer Schutz vor Diebstahl von Daten und geistigem Eigentum**
- **Niedrigere Gesamtkosten für die Reaktion auf Sicherheitsvorfälle**
- **Weniger Betriebsstörungen**
- **Geringeres Risiko der Rufschädigung oder Integritätsverletzung**

Wenn Sie mehr über Fidelis erfahren möchten, stehen wir gern zu Ihrer Verfügung.

Fidelis Cybersecurity | + 49 30 408 173 210 | emea@fidelissecurity.com

Fidelis Cybersecurity schützt die sensibelsten Daten weltweit. Wir reduzieren den Zeitaufwand für die Erkennung und Behebung von Sicherheitsvorfällen. Mit Fidelis erkennen Sie Angriffe sofort, können die Aktionen der Angreifer zurückverfolgen und den Diebstahl von Daten vereiteln.