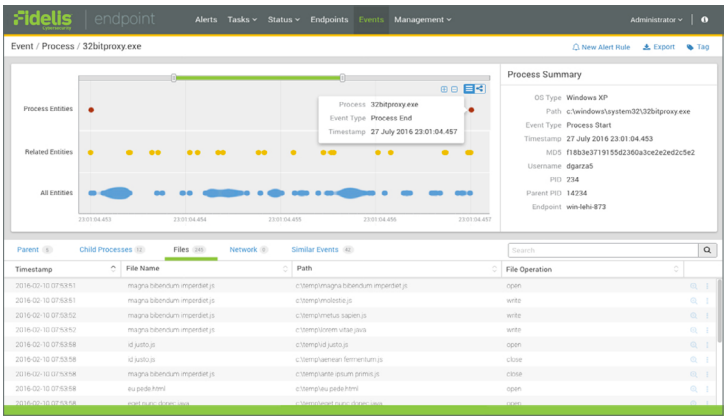
Datenblatt

Fidelis Endpoint™

Bedrohungen in Echtzeit erkennen, Untersuchung und Reaktion automatisieren

Klarer Fokus auf die relevanten Incidents in der Masse der Alerts

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 – die verdächtige Vorfälle prüfen und einstufen sollen – können die enorme Anzahl von Alerts kaum noch bewältigen. Deshalb gelingt es ihnen nicht, rasch festzustellen, ob es sich bei einem verdächtigen Vorfall tatsächlich um einen Angriff oder nur einen False Positive handelt. Zudem fehlen ihnen oft ausreichende Detailinformationen, um die Auswirkungen abzuschätzen.



Mit Fidelis decken Sie Bedrohungen in Echtzeit auf und erhalten kontextuelle Informationen zu Schweregrad und den Folgen.

Produktüberblick

Mit Fidelis Endpoint sind sicherheitsbewusste Unternehmen in der Lage, Sicherheitsverletzungen kompetent aufzuspüren und zu beseitigen – und das in einem Bruchteil der Zeit, die bisher dafür nötig war. Sicherheitsteams erhalten neben dem erforderlichen Überblick und Kontext vor allem Unterstützung bei der Automatisierung der folgenden Aufgaben:

- **Rasche Erkennung und Abwehr gezielter Angriffe:** Sie können Angriffsmuster schnell erkennen, Bedrohungen anhand mehrerer Kriterien bestätigen, die Workflows für Gegenmaßnahmen und Analysen automatisieren und proaktiv nach Bedrohungen suchen.
- **Korrelation mit Daten anderer Sicherheitstools:** Sie können die Warnmeldungen Ihrer vorhandenen netzwerkbasierten Sicherheitsprodukte, SIEM-Programme und anderer Sicherheitslösungen überprüfen, damit Sie sich nur mit echten Bedrohungen befassen müssen und innerhalb weniger Sekunden nach einem Alert handeln können.
- **Schnellere und fundiertere Entscheidungsfindung:** Automatisieren Sie die Abläufe für Notfallreaktionen, wenden Sie Bedrohungsanalysen an und durchleuchten Sie alle schädlichen Aktivitäten in jedem Systembereich.
- **Minimierung des Zeitaufwands für die Behebung von Zwischenfällen:** Automatisieren Sie komplexe und zeitaufwendige manuelle Abläufe und ziehen Sie aktuelle Bedrohungsdaten sowie detaillierte Kontextinformationen zur Auswertung von Warnmeldungen heran, erheben Sie Verlaufs- und Berichtsdaten wie die durchschnittliche Zeit bis zur Bestätigung (MTV) und zur Reaktion (MTR) auf Vorfälle für die Berichterstellung.

Highlights

Transparenz in Echtzeit: Überwacht und erfasst kontinuierlich die wichtigsten Endpunktaktivitäten, einschließlich Dateien, Prozesse und Netzverkehr sowie URLs und DNS.

Alarm bei verdächtigen Aktivitäten am Endgerät: Erkennt automatisch, wenn am Endgerät ein Anhaltspunkt für eine Bedrohung vorliegt (IP-Adresse, DNS, Prozessname, URL, MD5), und löst eine vorkonfigurierte Reaktion aus.

Einbindung vorhandener Sicherheitstools: Arbeitet nahtlos mit Fidelis Network™, SIEM-Lösungen, Next-Gen Firewalls sowie Alarm- und Überwachungstools zusammen, um Warnmeldungen automatisch zu prüfen und ggf. Gegenmaßnahmen einzuleiten.

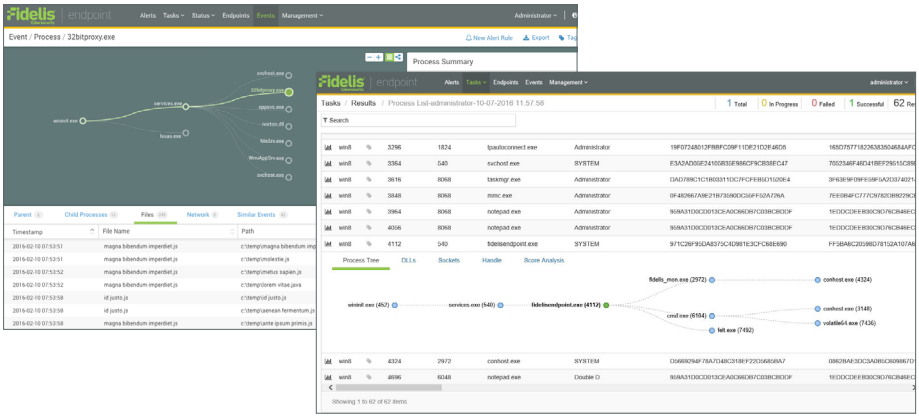
Systemmanagement: Ausführung spezifischer Aufgaben auf Endpunkten, wie rasche Softwareverteilung oder die gezielte Suche nach nicht verwalteten Geräten

Threat Intelligence: Importiert Bedrohungsdaten von Fidelis und anderen kommerziellen Anbietern, aus Open Source und eigenen Quellen, um Bedrohungen auf Endgeräten automatisch zu erkennen und zu bewerten.

Beschleunigen Sie die Erkennung, Einstufung und Bearbeitung von Incidents ohne zeitaufwändige manuelle Schritte und teure und schwer verfügbare Security Experten.

Über Fidelis Endpoint

- **Sofortige Gegenmaßnahmen:** Verknüpfen Sie SIEM-Lösungen, moderne Firewalls und Alarmprogramme mit Endgeräten, um Daten verschiedener Herkunft automatisch miteinander in Beziehung zu bringen, sich einen Überblick über Vorfälle auf allen Infrastrukturebenen zu verschaffen und effizient auf sie zu reagieren.
- **Akute Bedrohungen rasch aufdecken:** Durch die kontinuierliche Auswertung von Ereignisdaten können Sie schädliche Aktivitäten ohne Zeitverlust identifizieren und Warnmeldungen und Gegenmaßnahmen in Echtzeit generieren.
- **Proaktiv nach Bedrohungen suchen:** Anhand einfacher und komplexer Bedrohungsdaten aus dem Netzwerk bzw. von Hosts können Sie gehackte Endgeräte rasch erkennen und automatisch die erforderlichen Gegenmaßnahmen einleiten.
- **Vorfälle schneller beurteilen und priorisieren:** Ohne unterschiedliche Einzelprodukte und ohne Zeitaufwand für Ihre Sicherheitsanalysten können Sie automatisch umfassende Daten zu Endgeräten abrufen und anhand von Threat Reputationsdiensten auf Bedrohungen prüfen. Ebenso können Sie anhand ausgefeilter Daten und Mechanismen zur Erkennung von Bedrohungen feststellen, ob Angreifer in Endgeräte eingedrungen sind.



Mit den Funktionen zur Datenvisualisierung können Sie den primären Angriffspunkt ermitteln und den Verlauf des Angriffs nachvollziehen..

- **Mit „Playback“ nachvollziehen, was passiert ist:** Sie können den Verlauf eines Angriffs auch später lückenlos nachvollziehen und sehen, welche Daten genutzt wurden und wer der Angreifer ist. Dazu werden wichtige Daten zu Dateien, Prozessen, Registry, Netzwerk, DNS und URLs aufgezeichnet und, gemeinsam mit den wichtigsten Warnungen, automatisch in einer Zeitleiste aufbereitet.
- **Betroffene Endgeräte automatisch sichern und Gegenmaßnahmen einleiten:** Sie können den Abfluss von Daten und das weitere laterale Vordringen von betroffenen Endgeräten aus umgehend stoppen, indem Sie das Endgerät isolieren, Prozesse beenden, Dateien löschen und einen Task starten, der eine Virusprüfung oder spezielle Skripte auf diesen Geräten startet.
- **Automatische Abläufe in Notfällen:** Sie können für Ihr Unternehmen ganz einfach individuelle Abläufe für Sicherheitsvorfälle einrichten. Diese starten über definierte Auslöser automatisch Gegenmaßnahmen oder eine umfangreiche Vorgangsanalyse.

„Einer der größten Vorteile von Fidelis Endpoint ist, dass wir jetzt ohne externe Unterstützung auf Zwischenfälle reagieren können. So konnten wir unsere Reaktionszeit bei Sicherheitsvorfällen von zehn Tagen auf fünf Stunden reduzieren.“

– Director of Forensics and eDiscovery bei einer der fünf größten weltweit agierenden Banken

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.

