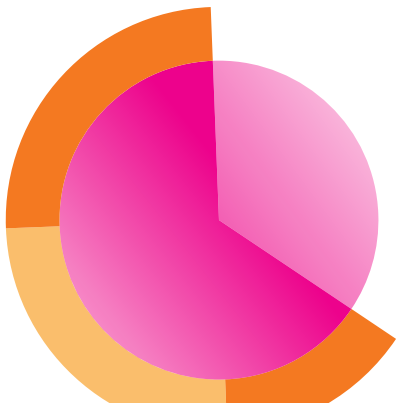
Der Leitfaden für **Sicherheitsdaten**

splunk>

Zeitreihendaten. Streaming-Daten. Dark Data.

Es ist kein Geheimnis, dass Daten in den meisten Unternehmen immer noch unzureichend genutzt, dafür aber um so mehr unterschätzt werden. Obwohl ständig von datengestützten Entscheidungen die Rede ist, schaffen Unternehmen aller Größen es nach wie vor nicht, die täglich anfallenden Datenmengen effektiv zu erfassen und zu verarbeiten. Cyberkriminelle wissen aber sehr wohl, dass Daten „das neue Öl“ sind. Und wie Erdöl können Daten raffiniert und für teures Geld auf dem Markt verkauft werden. Den Security-Teams machen daher nicht nur die zunehmenden Datenmengen und die Zerfaserung der Netzwerkgrenzen zu schaffen, sondern auch immer mehr komplexe Cyberangriffe. Was die Teams jetzt brauchen, sind Transparenz und Erkenntnisse im Zusammenhang, damit sie Security Incidents effektiv untersuchen und klären können, in On-premises-Umgebungen ebenso wie in Hybrid-Cloud- und Multi-Cloud-Architekturen.

Tatsächlich reichern bereits 73 % der Unternehmen ihre Sicherheitsanalysen mit anderen Datenquellen an. In diesen Daten stecken wichtige Erkenntnisse über die IT, die Sicherheit und das Unternehmen insgesamt. Daten sind die Chronik aller Aktivitäten und Verhaltensweisen von Kundschaft und Usern, aller Transaktionen, aller Anwendungen, Server, Netzwerke, mobilen Geräte etc. Entscheidende Informationen über Konfigurationen, APIs, Message Queues, Diagnosen und Sensordaten aus Industriesystemen sowie vieles mehr – es ist alles da. Sie müssen die Daten nur richtig erschließen und nutzbar machen.



Mithilfe des richtigen Ansatzes erleichtern Daten viele Aufgaben, z. B.:

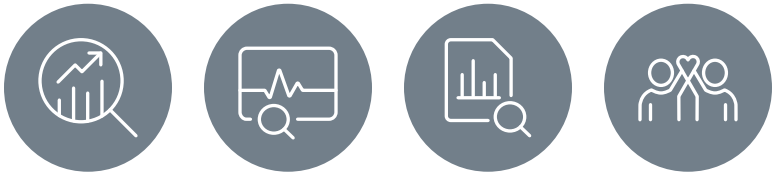
- Fundiertere Entscheidungen in allen Unternehmensbereichen treffen
- Die IT-Operations effizienter gestalten
- User Experience und Customer Experience optimieren
- Betrug erkennen bzw. komplett unterbinden
- Drohendes Unheil bereits im Vorfeld erkennen
- Versteckte Trends identifizieren, die Ihrem Unternehmen zu einem Wettbewerbsvorsprung verhelfen
- Problemlose Audits, verlässliche Reports, belastbare Prognosen und noch vieles mehr.

Die Herausforderung bei der Nutzung der riesigen Datenmengen, die die meisten Unternehmen anhäufen, besteht darin, dass die Daten in einer schwindelerregenden Vielfalt von Formaten vorliegen, mit denen herkömmliche Tools für Monitoring und Datenanalyse nicht umgehen können. Viele Tools sind von den unterschiedlichen Datenstrukturen, Quellen oder Zeitspannen überfordert. Und das geht weit über reine Maschinendaten hinaus. Doch die Vorteile, die sich aus der vollumfänglichen Datennutzung ergeben, sind enorm. Genau hier kommt Splunk ins Spiel.

Mit Splunk können Sie Daten für jede Frage, Entscheidung und Handlung in Ihrem Unternehmen heranziehen, um aussagekräftige Ergebnisse zu erzielen. Im Gegensatz zu allen anderen Plattformen ist Splunk tatsächlich in der Lage, beliebige Daten aus beliebigen Quellen zu verarbeiten, um damit konkrete Maßnahmen anzustoßen, von denen Ihr Unternehmen profitiert. Der Nutzen reicht vom Monitoring der IT-Infrastruktur und IT-Sicherheit bis hin zur Überwachung und Verwaltung der DevOps- und der Anwendungsleistung.

Datenplattform für hybride Welten

Nutzen Sie Daten für diese Zwecke:



Untersuchen **Monitoring** **Analysen** **Maßnahmen**

Die Unternehmen, die am meisten von ihren Daten profitieren, sind diejenigen, die in der Lage sind, unterschiedlichste Datentypen für Analysen heranzuziehen, sie anzureichern und Antworten herauszufiltern. Doch nicht zu wissen, welche Daten verarbeitet werden sollten, kann Unternehmen ausbremsen, ehe sie überhaupt loslegen.

Wenn Sie sich mit allgemeinen Use Cases in den Bereichen Sicherheit, IT-Operations, Business Analytics, DevOps, IoT (Internet of Things) etc. vertraut machen (einschließlich der zugehörigen Datentypen und -quellen), können Sie schnell und einfach den richtigen Lösungsweg einschlagen.

Hier ein Beispiel:

1. Die Bestellung eines Kunden wird nicht bearbeitet.
2. Der Kunde ruft den Support an, um das Problem zu lösen.
3. Der Kunde bleibt allzu lange in der Warteschleife, am Ende gibt er auf und setzt stattdessen einen Tweet ab: eine wütende Beschwerde über das Unternehmen.

Wie sehen Maschinendaten aus?

Abbildung 1: Daten können aus ganz unterschiedlichen Quellen stammen und auf den ersten Blick wie x-beliebiger Text aussehen.

Maschinendaten enthalten wichtige Informationen

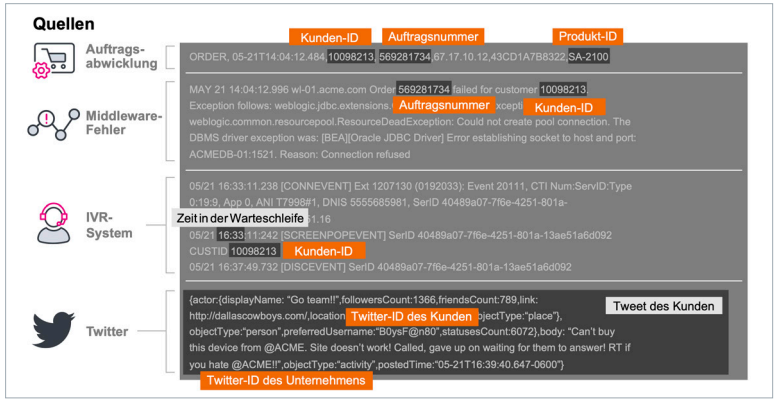


Abbildung 2: Der Mehrwert der Daten ist in diesem scheinbar beliebigen Text verborgen.

Maschinendaten enthalten wichtige Erkenntnisse

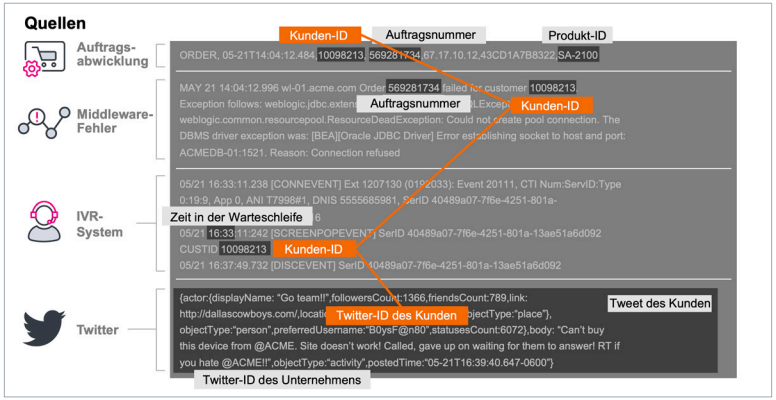


Abbildung 3: Indem verschiedene Datentypen miteinander korreliert werden, können Sie einen wirklichkeitsgetreuen Einblick in die Vorgänge innerhalb Ihrer Infrastruktur erhalten, Sicherheitsbedrohungen erkennen oder die Erkenntnisse sogar für bessere Geschäftsentscheidungen nutzen.

Durch das Erfassen aller am Prozess beteiligten Daten – dies geschieht, indem Informationen aus der Auftragsabwicklung, der Middleware, aus interaktiven Sprachdialogsystemen und Twitter abgerufen werden – kann sich ein Unternehmen einen vollständigen Überblick über die Probleme verschaffen, die die Customer Experience beeinträchtigen.

Sicherheitsdaten

Unternehmen müssen jede verfügbare Ressource nutzen, um Cyberangriffen immer einen Schritt voraus zu sein, denn fortschrittliche Bedrohungen sind nicht zu unterschätzen, und Malware kann problemlos ein ganzes Netzwerk lahmlegen. Außerdem werden die Analysten im SOC (Security Operations Center) mit einer solchen Vielzahl von Warnmeldungen bombardiert, dass sie nicht schnell genug mit den Untersuchungen beginnen können. Darüber hinaus gibt es ohnehin nicht genügend qualifizierte SOC-Analysten.

Diese Herausforderungen werden sich im digitalen Zeitalter noch verschärfen, insbesondere wenn man die zunehmende Komplexität von Cloud-Migrationen, die Netzwerkumstellung von 4G auf 5G, die Anzahl der vernetzten Geräte (die sich mittlerweile auf fast 80 Milliarden beläuft) und die Automatisierung bedenkt, die immer stärker in unser Leben eingreift.

Eine der wichtigsten – und oft vernachlässigten – Ressourcen, die Unternehmen nutzen können, um diese Sicherheitsherausforderungen zu meistern, sind Daten.

Unternehmen, die in der Lage sind, aus dieser Transformation und den dabei entstehenden Daten Kapital zu schlagen, werden effizienter, rentabler, innovativer und letztendlich sicherer sein.

In diesem E-Book werden drei Unternehmen vorgestellt, die Daten nutzen, um sich vor den neuesten Cyberbedrohungen zu schützen, und in vielen Fällen auch, um Herausforderungen in den Bereichen IT-Operations, IoT, DevOps und Business Analytics zu bewältigen.

Security und Compliance

IT-Operations, Anwendungsbereitstellung und DevOps

Inhaltsverzeichnis

Intel erhöht sein Sicherheitsniveau mit innovativer Data Intelligence

Branche

- Technologie

Splunk-Anwendungsfälle

- Security
- Cybersicherheit – Incident Response Management
- Security-Monitoring
- Anwendungsmonitoring

Herausforderungen

- Umstieg auf ein datenzentriertes Geschäftsmodell erhöht den Wert der Daten, gleichzeitig aber auch deren Anfälligkeit
- Bestehendes SIEM war nicht mehr zweckdienlich
- Mehrere abgeschottete Datensilos und Teams lieferten unterschiedliche Datenanalysen

Vorteile für das Unternehmen

- Neuer Ansatz für Kontrolle und Management der Informationssicherheit
- Erkennung hochkomplexer Bedrohungen innerhalb von Minuten oder Stunden statt in Tagen oder Wochen
- Gemeinsamer, einheitlicher Ansatz zur Steuerung der Cybersecurity
- Cyber-Intelligence-Plattform für Intels gesamte InfoSec-Organisation

Splunk-Produkte

- Splunk Enterprise
- Splunk Enterprise Security
- Splunk IT Service Intelligence (ITSI)
- VictorOps
- Splunk Mission Control

„Wir sehen das Potenzial, und weil wir das Potenzial sehen, investieren wir Zeit, Energie und Ressourcen. Wir wollen Splunk zu einem Erfolg machen, weil wir glauben, dass wir damit unsere Mission erfüllen können."

— Brent Conran, Chief Information Security Officer, Intel

Executive Summary

Der Beitrag, den Intel mit seiner Technologie in unserer Gesellschaft leistet, ist nicht zu unterschätzen. Die technische Expertise des Unternehmens trägt dazu bei, Milliarden von Geräten und die Infrastruktur der intelligenten, vernetzten Welt zu sichern, anzutreiben und miteinander zu verbinden. Ebenso wenig zu unterschätzen ist die Bedeutung von sicheren Daten als dem wertvollsten Asset eines Unternehmens.

Mit Splunk und Apache Kafka als Grundlage hat Intels IT-Abteilung eine neue Cyber-Intelligence-Plattform entwickelt, die einen ganz neuen Ansatz für die Informationssicherheit bietet:

- Beschleunigung der Datenanalyse, schnellere Erkennungen und Reaktionen auf komplexe Bedrohungen.
- Förderung einer kollaborativen Organisationsstruktur mit einer gemeinsamen Sprache und Arbeitsoberfläche.
- Bereitstellung von Stream-Processing- und Machine-Learning-Tools, die auch im Zusammenhang mit Sicherheitsprozessen und dem Systemzustand wertschöpfend sind.

Daten sind das A und O

Intel hat sich vom PC- zum Datenunternehmen gewandelt, entwickelt neue Produkte, erschließt neue Märkte und gewinnt auf innovative Weise neue Kunden. „Daten sind das A und O, Daten sind Trumpf. Sie treiben unser Unternehmen an, sie treiben alles an", so Brent Conran, Chief Information Security Officer bei Intel. „Sie transformieren traditionelle Branchen und solche, die in der Cloud zu Hause sind. Die Fähigkeit, Erkenntnisse aus Daten zu gewinnen, unterscheidet erfolgreiche Unternehmen von Unternehmen, die den Anschluss verlieren."

Aufgrund dieser Datenausrichtung musste Intels Abteilung für Informationssicherheit (InfoSec) eine umfassende Defense-in-Depth-Strategie entwickeln. Das Team hat Präventions- und Erkennungstools auf vielen Ebenen automatisiert (Perimeter, Netzwerke, Endpunkte, Anwendungen und Daten) und so 99 % der Bedrohungen in Intels gesamter Umgebung bewältigt.

Jagd nach dem einen Prozent

Komplexe Bedrohungen werden immer zahlreicher und raffinierter. Das Unternehmen mühte sich ab, mit einer Legacy SIEM-Lösung, die mit den aktuellen Anforderungen einfach nicht mehr mithalten konnte. Nur eine Handvoll Experten kannte sich mit der bestehenden SIEM-Lösung aus, die nicht mehr auf die stetig steigende Anzahl neuer Datentypen skalierbar war.

Intel InfoSec brauchte eine Strategie zur Erkennung von hochkomplexen Bedrohungen, die versuchen, in die Unternehmensumgebung einzudringen – intern auch „hunting the one percent" genannt. Diese Strategie war ausschlaggebend für die Entwicklung von Intels Cyber-Intelligence-Plattform (CIP), die auf Spitzentechnologien wie Splunk und Apache Kafka aufbaut. Mit Hochleistungsservern, die auf Intel-Xeon-Platinum-Prozessoren, Intel-3D-NAND-Solid-State-Drives (SSDs) und Intel-Optane-SSDs basieren, erfasst die neue CIP-Plattform ein Datenvolumen von mehr als 12 Terabyte pro Tag und speichert 15 Petabyte. Die Daten fließen aus Hunderten Quellen in einen Kafka Message Bus und dann in die Splunk-Plattform, auf der User mehr als 1,3 Millionen Suchvorgänge pro Woche ausführen.

Mit der einheitlichen Datenplattform von Splunk und Hunderten von Drittanbieter-Tools verfügt Intel InfoSec jetzt über umfassende Transparenz und eine gemeinsame Arbeitsoberfläche, mit der die Effektivität gesteigert werden konnte. Das Team kann nun Bedrohungen innerhalb von Stunden oder Minuten statt in Wochen oder Stunden erkennen und abwehren.

Skalierung der Cyber-Intelligence-Plattform

Die Ergebnisse der CIP führten zu weiteren Datenquellen, neuen Use Cases und vielen weiteren Datenmodellen. Schon bald wurde die Nutzung der CIP auf Bereiche wie Schwachstellenmanagement, Compliance und Enforcement sowie Risikomanagement ausgeweitet, was zusätzliche Anforderungen an die Infrastruktur stellte und noch schnellere Rechen- und Speichervorgänge erforderte. Um die Performance der Plattform zu maximieren, mussten sich Intels Sicherheitsarchitekt sowie die Techniker noch eingehender mit der Splunk-Plattform und den Intel-Technologien auseinandersetzen.

„Wir haben die CIP entwickelt, um zehn und schließlich Hunderte Terabyte Daten pro Tag zu verarbeiten und Hunderte von Usern zu unterstützen, die Ad-hoc-Suchen, geplante Suchen, Datenmodellbeschleunigungen und Machine-Learning-Modelle erstellen. Um diese Leistungsanforderungen zu erfüllen, brauchten wir Server mit den Xeon-Scalable-Prozessoren und SSDs von Intel. Jede Sekunde zählt, wenn wir unsere Mission ‚Make it safe for Intel to go fast' umsetzen wollen."

— Jac Noel, Security Solution Architect, Intel

Gemeinsam entwickelten Splunk und Intel eine Referenzkonfiguration, um die Erweiterung der CIP in den Rechen-, Arbeitsspeicher- und Speicherbereichen mit den neuesten Produkten und Technologien von Intel zu unterstützen. Splunk und Intel lassen nun auch andere an ihrem Erfolg teilhaben, damit sie ihre Splunk- und Apache-Kafka-Implementierungen skalieren können und Rohdaten effektiver in aussagekräftige Informationen zu Betrieb, Business und Sicherheit verwandeln.

Nachhaltige Wertschöpfung

Das InfoSec-Team von Intel ist dabei, die Nutzung von Splunk und Kafka auszuweiten. Die Fachleute für Analyse und Data Science befassen sich mit dem Transformieren, Anreichern, Verknüpfen, Filtern und Bearbeiten von Daten im Datenstrom. Darüber hinaus fügt das Team weitere Machine-Learning-Tools für unterschiedlichste Use Cases hinzu – von Incident Response, Operations und Systemintegrität bis hin zur Workflow-Orchestrierung und zu Warnmeldungen. In Zusammenarbeit mit Splunk setzt Intel nachhaltige Wertschöpfungspotenziale frei.

„Intel Information Security ist viel agiler als früher", so Conran. „Wir haben einen brandneuen Splunk Data Lake integriert und unsere Tools modernisiert. Mit den Daten am richtigen Ort und durch die Schulung unserer Teams konnten wir Kräfte bündeln und einen Multiplikatoreffekt erzielen. Jetzt verwenden wir Machine Learning, um die Tiefe und Geschwindigkeit unserer Cyber-Intelligence signifikant zu steigern."

NewYork-Presbyterian

Das NewYork-Presbyterian-Krankenhaus bekämpft die Opioid-Problematik mit Splunk

Branche

- Gesundheitswesen

Splunk-Anwendungsfälle

- Security

Herausforderungen

- Das Krankenhaus musste Daten aus elektronischen Gesundheitsakten, Plattformen zur elektronischen Verschreibung von Betäubungsmitteln, Apothekensystemen und anderen Quellen nachverfolgen, um herauszufinden, ob Medikamente für möglicherweise illegale Zwecke umgeleitet werden.
- Echtzeitmonitoring des Zugriffs auf elektronische PHI (persönliche Gesundheitsdaten) war nicht möglich, was zu verminderter Sicherheit und mangelndem Schutz der Patientendaten führte.

Vorteile für das Unternehmen

- Schutzmaßnahmen gegen die Entwendung von Opioiden und hochpreisigen Medikamenten wie bestimmten Krebsmedikamenten, die mehrere Zehntausend US-Dollar pro Monat kosten können.
- Monitoring der IT-Sicherheitsprozesse, sodass Betäubungsmittel und andere Medikamente nicht illegal eingesetzt oder verschrieben werden können.
- Möglichkeiten für Peer-Institutionen, in ihren Krankenhäusern dieselben Monitoring-Methoden anzuwenden

Datenquellen

- Audit-Logs
- Anwendungsdaten
- Cerner
- Allscripts
- athenahealth

Splunk-Produkte

- Splunk Enterprise
- Splunk Enterprise Security (ES)

Executive Summary

Das NewYork-Presbyterian Hospital ist in den USA einer der größten Gesundheitsversorger mit Universitätsangliederung und bestrebt, Patienten im Großraum New York, landesweit und auf der ganzen Welt optimale Versorgung zu bieten und das Patientenwohl immer im Blick zu behalten. Das NewYork-Presbyterian gilt als führend in Ausbildung und Forschung und hat sich mit innovativen stationären Versorgungskonzepten, die den Patienten in den Mittelpunkt stellen, einen Namen gemacht.

Mithilfe der leistungsstarken Splunk-Technologie hat das New-York-Presbyterian eine Plattform aufgebaut, die eine genaue Überwachung von Betäubungsmitteln und anderen Medikamenten erlaubt, was letztendlich dem gesamten Gesundheitswesen zugutekommt. Dank Splunk hat das Klinikum nun folgende Möglichkeiten:

- Überprüfung bei Zugriffs auf Patientendaten und kontrollierte Analysefreigabe von Daten für autorisierte User.
- Unterbindung der Entwendung von Betäubungsmitteln.
- Einhaltung der HIPAA-Anforderungen (Health Insurance Portability and Accountability Act) und anderer Informations- und Offenlegungspflichten.
- Schutz der Gesundheitsdaten (PHI) und der Privatsphäre von Patienten.

Schutz von Patientendaten und Privatsphäre

Anfangs nutzte das Krankenhaus Splunk für eine Reihe von Sicherheitsanwendungsfällen, von der Phishing-Abwehr über die Erhöhung der Kontensicherheit bis hin zur Automatisierung wichtiger Workflows. „Schon zwei Monate später haben wir mit dem Aufbau unseres SOCs begonnen“, meint Jennings Aske, Senior Vice President und Chief Information Security Officer bei NewYork-Presbyterian. „Jetzt haben wir ein Team mit sechs Mitarbeitern, die sich den ganzen Tag Dashboards und Visualisierungen anschauen, in die alle Datenquellen integriert sind, die wir für Sicherheitszwecke benötigen.“

Doch das war erst der Anfang. „Beim Aufbau unseres Security Operations Centers ist uns bewusst geworden, dass wir uns auch Gedanken um betriebswirtschaftliche Probleme im Zusammenhang mit dem Patientendatenschutz machen müssen. Insbesondere wollten wir eine Plattform, die dafür sorgt, dass niemand herumspioniert, zu viele Patientendaten ansieht oder auf die falschen Datensätze zugreift“, so Aske weiter. „Also habe ich vorgeschlagen, mit Splunk über die Einrichtung einer Datenschutzplattform für uns und andere Splunk-Kunden zu sprechen, die in klinische Systeme wie EPIC integrierbar ist.“

Gemeinsam haben das NewYork-Presbyterian und Splunk diese Vision verwirklicht und eine Plattform erstellt, die sofortige Untersuchungen ermöglicht, weil bei unbefugtem Zugriff auf Patientendaten eine Warnmeldung an Datenschutzbeauftragte erfolgt. Doch die Verantwortlichen erkannten bald, dass das Potenzial weit über die ursprünglich anvisierte Nutzung hinausging.

Opioid-Missbrauch weltweit bekämpfen

Den Verantwortlichen war klar, dass die Korrelations- und Machine-Learning-Funktionen von Splunk, die für die Patientenplattform von grundlegender Bedeutung waren, auch beim Aufdecken von abgezweigten Opioiden nützlich sein könnten. Diese Umleitungen tagen maßgeblich zur sogenannten Opioidkrise in den Vereinigten Staaten bei, einem bedrohlichen Anstieg des Missbrauchs von Opioid-Schmerzmitteln.

„Krankenhäuser spielen in der Opioidkrise eine große Rolle. Wir haben bei den Mitarbeitern manchmal höhere Abhängigkeitsraten als in der allgemeinen Bevölkerung“, so Aske. „Aus Statistiken der Zentren für die Kontrolle und Prävention von Krankheiten (CDC) wissen wir, dass Krankenhäuser zu bestimmten Zeiten die Hauptquelle für manche Drogen auf der Straße waren. In einem Jahr stammten 25 % des auf der Straße angebotenen OxyContins aus Krankenhäusern. Wir haben eine ethische und moralische Verpflichtung, uns nicht nur auf manuelle Prüfungen zu verlassen, sondern eine Plattform aufzubauen, um mögliche illegale Abzweigungen aufzudecken.“

Mit der Medikationsanalyseplattform kann das NewYork-Presbyterian Daten aus elektronischen Gesundheitsakten, Plattformen zur elektronischen Verschreibung von Betäubungsmitteln, Apothekensystemen und anderen Quellen nachverfolgen und

„Schließlich haben wir uns überlegt, dass diese Plattform problemlos auch von anderen Institutionen im Land genutzt werden kann, wenn wir sie gemeinsam mit Splunk erstellen. Man kann mit Sicherheit sagen, dass Splunk von allen 20 der von U. S. News ernannten Top-20-Krankenhäusern genutzt wird. Diese Zahlen belegen, dass solche Plattformen eine wichtige Rolle bei der Verbesserung der Patientenversorgung und der öffentlichen Gesundheit spielen könnten.“

— Jennings Aske, Senior Vice President and Chief Information Security Officer, NewYork-Presbyterian

Erkenntnisse darüber gewinnen, wie sich die missbräuchliche Entwendung unterbinden lässt. Beispielsweise gibt die Plattform sofort eine Warnmeldung an das NewYork-Presbyterian aus, wenn ein Arzt ein Betäubungsmittelrezept für einen Patienten ausstellt, der sich aktuell gar nicht im Krankenhaus befindet, oder wenn ein Apothekenmitarbeiter einen automatisierten Medikamentenschrank häufiger als andere öffnet.

Vielversprechende Zukunft

Während sich das NewYork-Presbyterian weiterhin leidenschaftlich für das Wohl der Patienten auf der ganzen Welt einsetzt, prüft das Krankenhaus weitere Splunk-Nutzungsmöglichkeiten im Krankenhaussystem. Unter anderem wird die Möglichkeit in Betracht gezogen, Splunk zu nutzen, um Probleme mit der Versicherungscodierung schneller zu erkennen und abgelehnte Erstattungsansprüche besser zu untersuchen. „Splunk ist eine Plattform, deren Funktionen zur Auswertung und Untersuchung von Daten über das Übliche hinausgehen“, so Aske. „Wenn wir Splunk auch für Bereiche wie die Versicherungsabrechnung nutzen, sind für das Krankenhaus möglicherweise Einsparungen von mehreren Millionen Dollar machbar.“

Die Zusammenarbeit von Splunk und dem NewYork-Presbyterian bietet „nahezu unbegrenzte Möglichkeiten zur Nutzung der Krankenhausdaten“, meint Aske. „Wir wollen den Einsatz von Splunk weiter ausbauen und diese Partnerschaft vorantreiben, und zwar nicht nur für uns, sondern für das Gesundheitswesen im ganzen Land.“

Threat Intelligence für Security Playbooks

Warum Kunden von Recorded Future sich für die Splunk-Plattform entschieden haben

Branche

- Technologie

Splunk-Anwendungsfälle

- Security
- Cybersicherheit
- Security Orchestration Automation and Response (SOAR)
- Incident Response Management
- Security-Monitoring
- Anwendungsmonitoring

Herausforderungen

- Kunden führten Prozesse manuell aus.
- Prozesse mussten für individuelle Kundenanforderungen umgestaltet werden.

Vorteile für das Unternehmen

- Kunden können Bedrohungen 10 % schneller erkennen.
- Kunden können um 63 % schneller auf Events reagieren.
- Allgemeine Effizienzsteigerung um 32 %.

Splunk-Produkte

- Splunk SOAR
- Splunk Enterprise Security

„Ohne Automatisierung und Orchestrierung werden Unternehmen nicht in der Lage sein, die aktuellen Herausforderungen zu meistern. Die Flut der Ereignisse überfordert die Unternehmen. Der Mensch kann diese Situation nicht alleine bewältigen.“

— Seth Whitten, VP of Integrations and Strategic Partnerships

Etwa 40.000 Sicherheitsfachleute aus 22 Branchen auf sechs Kontinenten setzen auf die branchenführenden Bedrohungsinformationen von Recorded Future. Das Cybersicherheitsunternehmen erfasst und analysiert enorme Datenmengen und liefert in Echtzeit relevante Erkenntnisse über Cyberbedrohungen. Dank dieser Erkenntnisse können die Kunden Bedrohungen schneller und effizienter erkennen und schneller angemessen reagieren. Und die Sicherheitsteams können schneller fundierte Entscheidungen treffen.

Seth Whitten ist VP Integrations and Strategic Partnerships bei Recorded Future. Wir haben mit ihm über die Partnerschaft von Splunk und Recorded Future sowie über die Auswirkungen der Integration von Splunk SOAR gesprochen. „Unsere umfangreichste Integration ist im Augenblick Splunk Enterprise“, meint er. „Für uns war es ganz selbstverständlich, SOAR zu nutzen. Wir haben viele Kunden, die Events mit ihren SIEM-Tools erkennen und in der Lage sein möchten, besser darauf zu reagieren.“

Warum SOAR?

Vor dem Einsatz von Splunk SOAR haben die Kunden von Recorded Future ihre Prozesse manuell ausgeführt. „Sie mussten auf unsere Plattform gehen, die gesuchten Informationen abfragen und dann bei der Untersuchung oder Sichtung einer Warnmeldung in ihrer Umgebung entscheiden, ob sie fortfahren wollten oder nicht“, erklärt Whitten.

Mit Splunk SOAR haben die Kunden von Recorded Future nun die Möglichkeit, die zuvor manuell ausgeführten monotonen Security-Operations-Aufgaben zu automatisieren. Sicherheitsbenachrichtigungen, deren Bearbeitung zuvor Minuten oder Stunden in Anspruch genommen hat, lassen sich nun dank der Automatisierungsfunktionen von Splunk SOAR in Sekundenschnelle lösen. Folglich konnten die Kunden die Effizienz ihrer Betriebsabläufe steigern und die Reaktionszeit bei Security Events beträchtlich verkürzen.

Whitten begeistern an Splunk SOAR insbesondere die Möglichkeiten, die sein Team beim Strukturieren der Playbooks hat. „Mit Splunk sind Außendiensteinsätze einfacher für uns, weil wir die vordefinierten Playbooks haben, die wir für Kunden viel schneller zum Laufen bringen können, ohne dass wir sie durch einen Redesign-Prozess führen müssten“, erklärt er.

Recorded Future und Splunk SOAR

Splunk-SOAR-Playbooks lassen eine Sequenz von Sicherheitsmaßnahmen in Maschinengeschwindigkeit automatisch ablaufen und ermöglichen den Kunden die Erstellung User-definierter und wiederholbarer Sicherheitsworkflows. Beispielsweise kann ein Splunk-SOAR-Playbook eine Sandbox instruieren, eine Datei zur Detonation zu bringen, oder ein Endpunktsicherheitstool anweisen, ein Gerät in Quarantäne zu nehmen. Mit über 100 vordefinierten, einsatzfertigen Playbooks unterstützt Splunk SOAR Kunden bei der Schaffung wiederholbarer und prüfbarer Prozesse im Security-Operations-Bereich.

„Wir nutzen Natural Language Processing (NLP) und künstliche Intelligenz, um Daten zu korrelieren und für Kunden verfügbar zu machen, die sie zur Problemlösung heranziehen.“

— Seth Whitten, VP of Integrations and Strategic Partnerships

„Unsere Kunden möchten all ihre Warnmeldungen bewältigen können. Sie möchten sie priorisieren. Sie möchten Maßnahmen ergreifen. Sie möchten Ergebnisse erzielen. Splunk SOAR hat sich für die Einspeisung unserer Daten angeboten und unterstützt uns dabei, aktiv auf diese Ergebnisse hinzuarbeiten.“

— Seth Whitten, VP of Integrations and Strategic Partnerships

Durch die Integration in Recorded Future erhalten diese Playbooks Zugriff auf Threat-Intelligence-Daten. Wenn eine Warnmeldung an Splunk SOAR übergeben wird – entweder von Splunk Enterprise Security oder als neues Artefakt – wird ein Playbook aufgerufen, das automatisch mit den Risikobewertungen und dem Kontext von Recorded Future angereichert wird. Die Entscheidungslogik des Playbooks kann bestimmen, ob die Warnmeldung ein Risiko birgt und an menschliche Analysten eskaliert werden muss oder übergangen werden kann. Da Splunk SOAR dabei hilft, falsch positive Warnmeldungen aus dem Flow zu entfernen, kann sich das Fachpersonal verstärkt um die wirklich wichtigen Probleme kümmern.

Die drei wichtigsten Vorteile

- 10 % schnellere Bedrohungserkennung
- 63 % schnellere Reaktion auf Events
- Allgemeine Effizienzsteigerung um 32 %

Authentifizierungs-daten

Use Cases: Security und Compliance, IT-Operations, Anwendungsbereitstellung

Beispiele und Datenquellen: Active Directory, LDAP, Identitätsmanagement, Single Sign-on

Authentifizierungsdaten liefern Erkenntnisse über User- und Identitätsaktivitäten. Zu den gängigen Authentifizierungsdatenquellen gehören:

- **Active Directory:** Ein verteiltes Verzeichnis, in dem Organisationen User- und Gruppenidentitäten, Sicherheitsrichtlinien und Inhaltskontrollen definieren.
- **LDAP:** Ein offener Standard der Internet Engineering Task Force (IETF), der in der Regel für die User-Authentifizierung (Name und Passwort) verwendet wird. Er verfügt über eine flexible Verzeichnisstruktur, die für eine Vielzahl von Informationen verwendet werden kann, z. B. vollständiger Name, Telefonnummern, E-Mail- und physische Adressen, Organisationseinheiten, Arbeitsgruppen und Manager.
- **Identitätsmanagement:** Unter Identitätsmanagement versteht man die Methode, die User digitaler Ressourcen – Menschen, IoT-Geräte, Systeme oder Anwendungen – mit einer überprüfbaren Online-ID zu verknüpfen.
- **Single Sign-on (SSO):** Ein Prozess zur Verwendung von föderiertem Identitätsmanagement, um überprüfbare, bescheinigungsfähige Identitäten aus einer einzigen Quelle für mehrere Systeme bereitzustellen. SSO erhöht die Sicherheit erheblich, indem es die Anmeldeinformationen an eine einzige Quelle bindet. Änderungen an den User-Rechten und am Kontostatus müssen nur einmal vorgenommen werden und werden in jeder Anwendung oder jedem Service berücksichtigt, auf den die User Zugriff haben. SSO ist besonders wichtig für User mit erweiterten Sicherheitsrechten, die Zugriff auf eine große Anzahl von Systemen haben, wie z. B. System- oder Netzwerkadmins.

Use Cases

Security und Compliance: Im Sicherheitsbereich bieten Authentifizierungsdaten eine Fülle von Informationen über User-Aktivitäten, z. B. mehrfache Anmeldefehler oder -erfolge bei mehreren Hosts in einem bestimmten Zeitfenster, Aktivitäten von verschiedenen Standorten innerhalb einer bestimmten Zeitspanne und Brute-Force-Aktivitäten. Im Einzelnen:

- Active-Directory-Domänencontroller-Logs enthalten Informationen zu User-Konten, z. B. Aktivitäten von privilegierten Konten sowie Details zu Remote-Zugriffen, zur Erstellung neuer Konten und zu abgelaufenen Konten.
- LDAP-Protokolle enthalten Aufzeichnungen darüber, welche User sich wann und wo bei einem System anmelden und wie auf Informationen zugegriffen wird.
- Die Daten des Identitätsmanagements beinhalten die Zugriffsrechte nach User, Gruppe und Stellenbezeichnung (z. B. CEO, Vorgesetzte oder normale User). Diese Daten können verwendet werden, um Zugriffsanomalien zu erkennen, die potenzielle Bedrohungen darstellen können. Beispiele sind der CEO-Zugriff auf ein Netzwerkgerät der unteren Ebene oder der Zugriff eines Netzwerkadmins auf das Konto des CEO.

IT-Operations und Anwendungsbereitstellung: Authentifizierungsdaten werden von IT-Operations-Teams zur Fehlerbehebung bei Problemen im Zusammenhang mit der Authentifizierung herangezogen. Zum Beispiel kann der Anwendungssupport mit Anmeldungen verknüpft werden, sodass das IT-Operations-Team erkennen kann, ob User Schwierigkeiten haben, sich bei Anwendungen anzumelden. IT-Operations-Teams, die für den Active-Directory-Support zuständig sind, können Logs zum Troubleshooting und zur Statusbestimmung des Active Directorys verwenden.

Antivirus

Use Cases: Security und Compliance

Beispiele: Kaspersky, McAfee, Norton Security, F-Secure, Avira, Panda, Trend Micro

Das schwächste Glied in der Kette der Unternehmenssicherheit stellen Einzelpersonen dar, und Antiviruslösungen bieten eine Möglichkeit, sie davon abzuhalten, ungewollt Schaden anzurichten. Eine Antivirenlösung kann Schäden verhindern, abmildern oder beheben, die entstehen, wenn User z. B. auf einen nicht vertrauenswürdigen Weblink klicken, Malware herunterladen oder ein präpariertes Dokument öffnen (oftmals gesendet von einem nichts ahnenden Kollegen).

Sogenannte APT-Bedrohungen (Advanced Persistent Threat) dringen häufig über einen einzelnen kompromittierten Rechner ein, der an ein vertrauenswürdiges Netzwerk angeschlossen ist. Antivirensoftware ist zwar nicht perfekt, kann aber gängige Angriffsmethoden erkennen und Angriffe vereiteln, bevor diese weitreichenden Schaden anrichten.

Use Cases

Security und Compliance: Antivirus-Protokolle unterstützen die Analyse von Malware und Schwachstellen von Hosts, Laptops und Servern und können zur Überwachung verdächtiger Dateipfade verwendet werden. Sie können helfen, Folgendes aufzudecken:

- Neu erkannte Binärdateien, Datei-Hash, Dateien im Dateisystem und in Registrys
- Wenn Binärdateien, Hash-Werte oder Registrys mit Bedrohungsinformationen übereinstimmen
- Ungepatchte Betriebssysteme
- Bekannte Malware-Signaturen

Mailserver

Use Cases: Security und Compliance, IT-Operations

Beispiele: Exchange, Office 365

E-Mail ist in den meisten Unternehmen nach wie vor die wichtigste Art der förmlichen Kommunikation. Daher gehören Datenbanken und Logs von E-Mail-Servern zu den wichtigsten geschäftlichen Aufzeichnungen. Aufgrund ihrer Menge und ausufernden Tendenz erfordert die Verwaltung von E-Mail-Daten in der Regel sowohl Datenaufbewahrungs- als auch Archivierungsrichtlinien, sodass nur wichtige Datensätze aufbewahrt werden und inaktive Daten in einen kostengünstigen Speicher verschoben werden.

Use Cases

Security und Compliance: Mail-Server-Daten können helfen, Schadanhänge, böswillige Domain-Links und Weiterleitungen sowie E-Mails von bekanntermaßen böswilligen oder von unbekannten Domains zu erkennen. Sie können auch verwendet werden, um E-Mail-Nachrichten von ungewöhnlicher Größe oder mit ungewöhnlichen Aktivitätszeiten herauszufiltern.

IT-Operations: E-Mail-Nachrichten und Aktivitätsprotokolle können erforderlich sein, um die Prozesse zur Informationssicherheit, Aufbewahrung und Compliance in einem Unternehmen einzuhalten. Transaktions- und Fehlerprotokolle des E-Mail-Servers sind außerdem wichtige Debugging-Werkzeuge für die Problemlösung in der IT und können auch für eine nutzungsabhängige Abrechnung verwendet werden.

Schwachstellenscans

Use Case: Security und Compliance

Beispiele: ncircle IP360, Nessus

Eine wirksame Methode zur Aufdeckung von Sicherheitslücken ist die Untersuchung der Infrastruktur aus dem Blickwinkel eines Angreifers. Mit Schwachstellenscans wird das Netzwerk eines Unternehmens auf bekannte Softwaredefekte getestet, die Eintrittspunkte für externe Angreifer bieten. Diese Scans liefern Daten zu offenen Ports und IP-Adressen, die von Angreifern genutzt werden können, um in ein System oder ein ganzes Netzwerk einzudringen.

Oftmals werden Netzwerkservices standardmäßig weiter ausgeführt, obwohl sie für einen bestimmten Server nicht erforderlich sind. Diese aktiven, nicht überwachten Services werden häufig für externe Angriffe genutzt, da sie eventuell nicht mit den neuesten Sicherheitsupdates des Betriebssystems gepatcht sind. Breit angelegte Schwachstellenscans decken Sicherheitslücken auf, die genutzt werden könnten, um ein ganzes Unternehmensnetzwerk zu infiltrieren.

Use Cases

Security und Compliance: Schwachstellenscans liefern Daten zu offenen Ports und IP-Adressen, die von Angreifern genutzt werden können, um in ein bestimmtes System oder ein ganzes Netzwerk einzudringen. Folgendes lässt sich mit den Daten erkennen:

- Systemfehlkonfigurationen, die Sicherheitsschwachstellen verursachen
- Veraltete Patches
- Unnötige Netzwerkservice-Ports
- Falsch konfigurierte Dateisysteme, User oder Anwendungen
- Änderungen an der Systemkonfiguration
- Änderungen an unterschiedlichen User-, App- oder Dateisystemberechtigungen

Webserver

Use Cases: Security und Compliance, IT-Operations, Anwendungsbereitstellung

Beispiele: Java J2EE, Apache, Anwendungsnutzungsprotokolle, IIS-Logs, nginx

Webserver sind die Backend-Anwendung hinter jeder Website, sie liefern alle Inhalte, die in Browser-Clients angezeigt werden. Webserver greifen auf statische HTML-Seiten zu und führen Skripte in diversen Sprachen aus, die dynamische Inhalte generieren und andere Anwendungen wie die Middleware aufrufen:

- **Java – J2EE:** Java ist eine der gängigsten Programmiersprachen. Über die J2EE-Plattform, die APIs, Protokolle, SDKs und Objektmodule umfasst, wird Java in großem Maßstab für Unternehmensapps einschließlich Web-Applets, Middle-Tier-Geschäftslogiken und grafische Frontends verwendet. Java kommt auch bei nativen, mobilen Android-Apps zum Einsatz.
- **Apache:** Mit Apache laufen Millionen von Unternehmens-, Regierungs- und öffentlichen Websites. Apache zeichnet jede Transaktion detailliert auf: Jedes Mal, wenn ein Browser eine Webseite anfordert, erfasst das Apache-Protokoll Details wie Uhrzeit, Remote-IP-Adresse, Browsertyp und angeforderte Seite. Apache protokolliert auch verschiedene Fehlerzustände, z. B. die Anforderung einer fehlenden Datei, Zugriffsversuche ohne entsprechende Berechtigungen oder Probleme mit einem Apache-Plug-in. Apache-Protokolle sind wichtig für die Fehlersuche und zwar sowohl bei Web-Anwendungen als auch bei Serverproblemen, sie werden aber auch zur Erstellung von Datenverkehrsstatistiken, zum Verfolgen des User-Verhaltens und zur Erkennung von Angriffen verwendet.
- **Anwendungsnutzungsprotokolle:** Ebenso wie Apache-Weblogs können auch Daten zur Anwendungsnutzung wertvolle Informationen liefern. Je nach Detailgrad der Messung kann die Nutzungsprotokollierung den Entwicklungsteams Informationen zu den am häufigsten und am seltensten genutzten Funktionen, zu Funktionen, die Usern Probleme bereiten, sowie zu Bereichen mit Verbesserungspotenzial liefern. Bei kundenseitigen Anwendungen bieten Nutzungsprotokolle den Vertriebs- und Marketing-Teams Erkenntnisse zur Effektivität von Online- bzw. App-Vertriebskanälen und Werbeaktionen, Daten über Sell-Through und Transaktionsabbrüche sowie Informationen für potenzielle Cross-Sale-Promotions.

Use Cases

Security und Compliance: Weblogs zeichnen Fehlerbedingungen auf, z. B. Zugriffsanfragen ohne Berechtigung, und protokollieren User-Aktivitäten, die auf Angriffe hinweisen können. Darüber hinaus können sie beim Erkennen von SQL-Einschleusungen und bei der Korrelation von betrügerischen Transaktionen hilfreich sein.

- Da Java-Anwendungen häufig auf Netzwerkservices und Datenbanken mit sensiblen Daten zugreifen, können Security-Teams anhand von Logdaten die Integrität von J2EE-Anwendungen überprüfen und verdächtiges Anwendungsverhalten sowie Anwendungsschwachstellen identifizieren.
- Apache-Weblogs können vor Angriffen warnen, z. B. vor versuchtem Eindringen, XSS, Pufferüberläufen oder DDoS.
- Ähnlich wie Weblogs können auch generische Anwendungsnutzungsprotokolle Security-Teams vor unbefugtem Zugriff warnen, z. B. wenn jemand mehr Ressourcen als gewöhnlich verbraucht oder Apps zu ungewöhnlichen Zeiten nutzt.

IT-Operations und Anwendungsbereitstellung: Weblogs sind wichtig für die Fehlersuche bei Web-Apps und bei Serverproblemen, werden aber auch zur Erstellung von Traffic-Statistiken herangezogen, die für die Kapazitätsplanung nützlich sind:

- J2EE-Daten können für Operations-Teams hilfreich bei der Diagnose von Problemen mit Three-Tier-Anwendungen sein, die Interaktionen zwischen Web, Middleware und Datenbankservern umfassen.
- Als Ganzes können Apache-Weblogs die Aktivität eines Webservices zeigen. Durch einen Blick auf die Details lassen sich Infrastrukturengpässe ausmachen und nachgelagerte Probleme aufzeigen.
- Anwendungsnutzungsprotokolle können IT-Operations-Teams durch die Bereitstellung detaillierter Aufzeichnungen zum Ressourcenverbrauch bei der Infrastrukturkapazitätsplanung, beim Lastenausgleich und bei der nutzungsbasierten Abrechnung unterstützen.

Firewall

Use Cases: Security und Compliance, IT-Operations

Beispiele: Palo Alto, Cisco, Check Point

Firewalls grenzen Zonen mit unterschiedlichen Sicherheitsrichtlinien ab. Sie kontrollieren den Fluss des Netzwerkverkehrs und übernehmen damit gewissermaßen die Rolle des Gatekeepers. Sie sammeln wertvolle Daten, die aufgrund der einzigartigen Position der Firewall als Gatekeeper des Netzwerkverkehrs nur an dieser Stelle erfasst werden können. Außerdem setzen Firewalls Sicherheitsrichtlinien um und können daher Anwendungen unterbrechen, die ungewöhnliche oder nicht autorisierte Netzwerkprotokolle verwenden.

Use Cases

Security und Compliance: Firewall-Logs bieten detaillierte Aufzeichnungen des Datenverkehrs zwischen Netzwerksegmenten, darunter Quell- und Ziel-IP-Adressen, Ports und Protokolle – alles Informationen, die bei der Untersuchung von Security-Incidents eine wichtige Rolle spielen. Anhand der Daten können auch Lücken in der Sicherheitsrichtlinie ermittelt werden, die sich mit engmaschigeren Firewall-Regeln schließen lassen. Firewall-Daten können bei der Erkennung folgender Elemente helfen:

- Seitwärtsbewegung
- Command-and-Control-Datenverkehr
- DDoS-Datenverkehr
- Datenverkehr von Schaddomains
- Datenverkehr von unbekannten Domains
- Datenverkehr von unbekannten Standorten

IT-Operations: Kommunikationsprobleme von Netzwerkanwendungen können auf die Sicherheitsrichtlinien des Netzwerks zurückzuführen sein. Firewall-Daten können Aufschluss darüber geben, welcher Datenverkehr blockiert ist und welcher ungehindert passieren kann. So können Sie feststellen, ob ein App- oder Netzwerkproblem vorliegt.

Intrusion Detection, Intrusion Prevention

Use Case: Security und Compliance

Beispiele: Tipping Point, Juniper IDP, Netscreen Firewall, Juniper NSM IDP, Juniper NSM, Snort, McAfee IDS

IDS (Intrusion Detection System) und IPS (Intrusion Prevention System) sind komplementäre, parallele Sicherheitssysteme, die Firewalls ergänzen. Ein IDS deckt erfolgreiche Angriffe auf Netzwerke oder Server auf, bei denen die Angreifer die Firewall durchdrungen haben. Ein IPS bietet fortschrittliche Abwehrmechanismen gegen komplexe Angriffe. Ein IDS wird in der Regel am Netzwerkrand platziert, direkt innerhalb einer Perimeter-Firewall, wobei einige Unternehmen auch ein System außerhalb der Firewall einsetzen, um mehr Informationen über alle Angriffe zu erhalten. Analog dazu wird ein IPS in der Regel am Netzwerkperimeter platziert, wobei es auch in Schichten an anderen Punkten innerhalb des Netzwerks oder auf einzelnen Servern eingesetzt werden kann. Ein IPS verhindert in der Regel die Auslieferung von Paketen, setzt Netzwerkverbindungen zurück oder setzt bestimmte IP-Adressen oder Adressbereiche auf die Blacklist.

Use Cases

Security und Compliance: IDS-Logs bieten Security-Teams detaillierte Aufzeichnungen von Angriffen unter Angabe des Typs, der Quelle, des Ziels und der verwendeten Ports und damit eine allgemeine Angriffssignatur. Bestimmte Signaturen können Warnmeldungen oder andere Entschärfungsmaßnahmen auslösen. Ein IPS liefert den gleichen Satz von Angriffssignaturdaten, kann jedoch darüber hinaus auch eine Bedrohungsanalyse von fehlerhaften Netzwerkpaketen und die Erkennung von Seitwärtsbewegungen (Lateral Movement) enthalten. Über diese Logs ist auch die Erkennung von Command-and-Control-Datenverkehr, DDoS-Datenverkehr sowie Datenverkehr von böswilligen oder unbekannten Domains möglich.

Network Access Control (NAC)

Use Case: Security und Compliance

Beispiele: Aruba ClearPass, Cisco ACS

Die Netzwerkzugriffsteuerung ist eine Form der Client-/Endpunktsicherheit, bei der ein lokal installierter Software-Agent verwendet wird, um Verbindungen zu einem geschützten Netzwerk vorab zu autorisieren. Die NAC überprüft Client-Geräte auf Kontamination durch bekannte Malware und auf die Einhaltung von Sicherheitsrichtlinien wie die Nutzung eines zugelassenen Betriebssystems mit den neuesten Patches. Clients, die bei der NAC-Überprüfung durchfallen, werden in ein abgeschottetes Quarantänenetzwerk umgeleitet, bis alle erkannten Probleme behoben sind.

Use Cases

Security und Compliance: NAC-Software sammelt Daten über die sich verbindenden Clients. Diese Daten umfassen eine Bestandsaufnahme der installierten Client-Software, die Einhaltung der Sicherheitsrichtlinien, Versionen von Betriebssystem und Anwendungspatches, Erreichbarkeit für Clients mit Remote-Zugriff sowie User-Zugriff auf geschützte Netzwerke. NAC-Logs bieten Security-Teams ein detailliertes Profil vom Status und von den Aktivitäten eines Clients. Sie können Details zu nicht autorisierten Geräteverbindungen enthalten und verwendet werden, um User/IPs mit einem physischen Netzwerkstandort zu korrelieren.

Netzwerk-Switches

Use Cases: Security und Compliance, IT-Operations

Beispiele: Ethernet-Switches, virtuelle Switches

Switches sind Netzwerkknotenpunkte, an denen Pakete von einem Netzwerksegment in ein anderes übergehen. In ihrer reinsten Form arbeiten Switches innerhalb eines bestimmten IP-Subnetzes und können keine Layer-3-Pakete an ein anderes Netzwerk weiterleiten. In modernen Rechenzentren kommt in der Regel eine zweistufige Switch-Hierarchie zum Tragen: Top-of-Rack-Switches, die Server und Speicher-Arrays am Edge verbinden, und Aggregation- oder Spine-Switches, die mit dem Netzwerkkern verbunden sind. Ethernet-Switches sind zwar weitaus verbreiteter, einige Unternehmen verwenden jedoch auch Fiber Channels oder Infiniband für Storage Area Networks oder HPC-Verbindungen, die jeweils ihren eigenen Switch-Typ haben.

Use Cases

Security und Compliance: Switch-Daten, die oft als NetFlow-Datensätze erfasst werden, sind eine wichtige Quelle für die Erkennung komplexer, hartnäckiger Bedrohungen, die Analyse von Datenverkehrsflüssen mit Blick auf ungewöhnliche Aktivitäten und die Aufdeckung potenzieller Datenexfiltration. Switch-Statistiken sind eine Wire-Level-Datenquelle, somit fast unmöglich zu fälschen und daher wichtig für alle Security-Analysen. Diese Daten können auch genutzt werden, um User oder IP-Adressen mit einem physischen Netzwerkstandort zu korrelieren.

IT-Operations: Operations-Teams nutzen Switch-Logs, um sich einen Überblick über den Status des Datenverkehrsflusses zu verschaffen und Informationen wie Quelle und Ziel, Serviceklasse und Ursachen von Engpässen abzurufen. Logs können auch aggregierte Statistiken zum Datenverkehr nach Port oder Client enthalten und Informationen dazu, ob bestimmte Ports überlastet, fehlerhaft oder ausgefallen sind.

Proxys

Use Cases: Security und Compliance, IT-Operations

Beispiele: Blue Coat, Fortinet, Juniper IDP, Netscreen Firewall, Palo Alto Networks, Palo Alto Networks Config, Palo Alto Networks System, Palo Alto Networks Threat, Palo Alto Networks Traffic, nginx

Netzwerk-Proxys werden unterschiedlich eingesetzt: als Web-Anwendungsbeschleuniger und für die intelligente Traffic-Lenkung, als Firewalls auf Anwendungsebene sowie als Content-Filter. Proxys agieren als transparente „Bump-in-the Wire"-Vermittler. Sie erhöhen die Latenz nur geringfügig, überblicken jedoch die gesamten Layer-7-Netzwerkprotokoll-Stacks (Anwendungsschicht) und können daher anwendungsspezifisches Traffic-Management und Sicherheitsrichtlinien implementieren.

Use Cases

Security und Compliance: Für Security-Teams sind Proxys als Firewalls auf Anwendungsebene von Bedeutung. Proxy-Aufzeichnungen enthalten Details zu bestimmten Inhalten, die Netzwerkkontrollpunkte durchlaufen, darunter Dateinamen, Typen, Quelle und Ziel sowie Metadaten über den anfordernden Client wie Betriebssystemsignatur, Anwendung und User-Name/ID (je nach Proxy-Implementierung). Diese Daten sind auch hilfreich zur Erkennung von Command & Control-Datenverkehr sowie von Datenverkehr von böswilligen oder unbekannten Domains.

Web-Proxys und einige Firewalls der nächsten Generation können in einem transparenten oder expliziten Modus im Namen eines Clients mit HTTP(S)-Servern kommunizieren. Mithilfe einer Reihe von verwandten Technologien können Anforderung und Antwort geprüft und auf der Grundlage der User-Rolle, der Website- oder Ressourcenkategorie oder des Angriffsindikators zugelassen oder blockiert werden. Die in den Events protokollierten Daten können möglicherweise zur Korrelation in der Bedrohungserkennung genutzt werden.

IT-Operations: Operations-Teams verwenden häufig Proxys, die in einen Application Delivery Controller (ADC) eingebettet sind, eine modernere, Layer-7-fähige Version eines Load Balancers. In diesem Zusammenhang können Proxy-Logs Informationen über eingehende Anforderungen und die Verteilung des Datenverkehrs auf die verfügbaren Ressourcen bereitstellen.

Systemprotokolle

Use Cases: Security und Compliance, IT-Operations, Anwendungsbereitstellung

Beispiele: Unix, Windows, Mac OS, Linux

Jedes Betriebssystem zeichnet Details zu seinen Betriebsbedingungen und Fehlern auf, und diese mit Zeitstempeln versehenen Logs sind die grundlegende und maßgebliche Quelle der Systemtelemetrie. Je nach Betriebssystem kann es separate Protokolle für verschiedene Event-Klassen geben, z. B. routinemäßige Informationsaktualisierungen, Systemfehler, Bootloader-Aufzeichnungen, Anmeldeversuche und Debug-Output. In Fehlerprotokollen werden oftmals Datensätze von mehreren Subsystemen und Betriebssystemdiensten oder Daemons zusammengefasst. Daher sind sie eine maßgebliche Quelle für Informationen zum Troubleshooting.

Use Cases

Security und Compliance: Systemprotokolle beinhalten eine Vielzahl von Sicherheitsinformationen, z. B. Anmeldeversuche, Dateizugriffe und Aktivitäten der System-Firewall. Diese Einträge können Security-Teams auf Netzwerkangriffe, eine Sicherheitsverletzung oder kompromittierte Software hinweisen. Darüber hinaus sind sie eine wertvolle Informationsquelle bei der forensischen Analyse eines Security-Incidents. Die Daten können z. B. herangezogen werden, um Änderungen in Systemkonfigurationen und Befehle zu erkennen, die von Usern oder privilegierten Usern ausgeführt werden.

IT-Operations und Anwendungsbereitstellung: Systemprotokolle sind beim Troubleshooting von Systemproblemen oftmals die erste Anlaufstelle für Operations-Teams, dazu zählen Probleme mit dem Betriebssystem, der Hardware oder verschiedenen E/A-Schnittstellen. Da sich ein bestimmtes Problem oftmals durch Fehler in mehreren Subsystemen manifestiert, ist die Korrelation von Protokolleinträgen eine der besten Möglichkeiten, die Kernursache eines subtilen Systemfehlers ausfindig zu machen.

Server-Logs

Use Cases: Security und Compliance, IT-Operations, Anwendungsbereitstellung

Serverbetriebssysteme zeichnen routinemäßig eine Vielzahl von Betriebs-, Sicherheits-, Fehler- und Debugging-Daten auf, wie z. B. beim Systemstart geladene Systembibliotheken, offene Anwendungsprozesse, Netzwerkverbindungen, eingebundene Dateisysteme und die Auslastung des Systemspeichers. Der Detailgrad kann vom Systemadministrator konfiguriert werden. Es gibt jedoch genügend Optionen, um sich ein vollständiges Bild der Systemaktivität während der gesamten Lebensdauer zu verschaffen. Je nach Subsystem sind Server-Logs für System-, Netzwerk-, Speicher- und Security-Teams hilfreich.

Use Cases

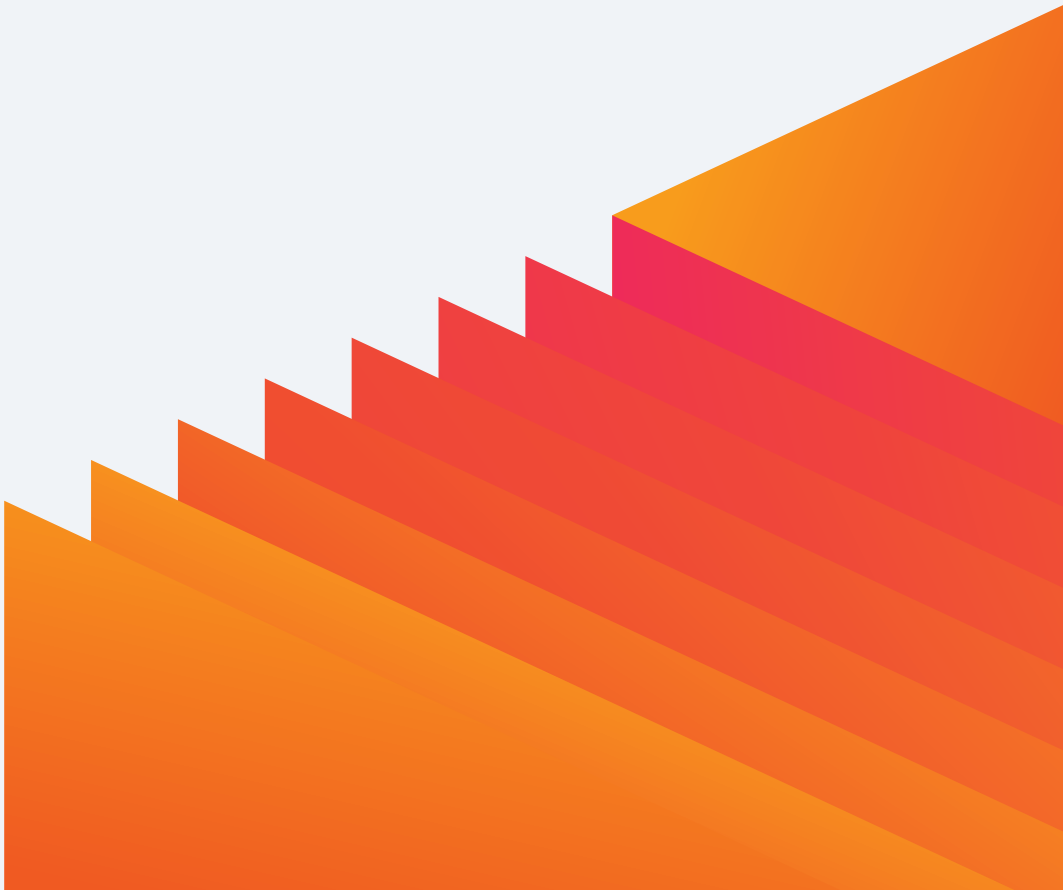
Security und Compliance: Server-Logs enthalten Daten von Sicherheitssubsystemen wie der lokalen Firewall, von Anmeldeversuchen und von Dateizugriffsfehlern, die Security-Teams zur Identifizierung von Angriffsversuchen, zur Nachverfolgung erfolgreicher Eindringversuche in das System und zum Schließen von Schwachstellen verwenden können. Das Monitoring von Server-Logs in Bezug auf Dateizugriff, Authentifizierung und Anwendungsnutzung kann zur Absicherung von Infrastrukturkomponenten beitragen.

IT-Operations und Anwendungsbereitstellung: Server-Logs liefern detaillierte Aufzeichnungen zur allgemeinen Integrität des Systems sowie forensische Informationen zum genauen Zeitpunkt von Fehlern und anomalen Bedingungen, die bei der Suche nach der Ursache von Systemproblemen von unschätzbarem Wert sind.

Über **Splunk.**

Holen Sie mehr aus Ihren Daten – mit Splunk, der Plattform für einheitliche Sicherheit und Observability und einer Technologie, die darauf ausgelegt ist, dass Sie Daten in beliebigem Umfang untersuchen, überwachen und analysieren können – und auf dieser Grundlage Maßnahmen ergreifen. Probieren Sie selbst aus, wie Splunk Ihr Unternehmen sicherer macht.

Kostenlose Testversion



splunk>

24-122987-Splunk-theessentialguidetosecuritydata-101_GER