splunk>

DATENBLATT

Splunk® App for Enterprise Security

Analysegestützte Sicherheit und ständiges Monitoring auf moderne Sicherheitsbedrohungen

Anpassung an eine dynamische Bedrohungslandschaft

Moderne Unternehmen brauchen Sicherheitstechnologien, die sich an eine dynamische Bedrohungslandschaft, ständig weiterentwickelte Angriffstaktiken, komplexe Bedrohungen und variable Unternehmensanforderungen anpassen können. Um sich diesen neuen Herausforderungen stellen zu können, müssen Sicherheitsanalysten flexibel sein, damit sie schnell auf Bedrohungen reagieren und unternehmensspezifische Entscheidungen treffen können. Angesichts der neuen Anforderungen brauchen Sicherheitsteams komplexe Analysemöglichkeiten, kontextbezogene Reaktionsprozesse und Möglichkeiten, rasch neue Verfahren zur Erkennung von Bedrohungen implementieren zu können.

Eine wichtige Komponente dieser dynamischen Bedrohungslandschaft ist, dass Angreifer die Zeit, die Expertise und die Ressourcen zum Erstellen von Angriffsszenarien haben, die von Punktlösungen für die Sicherheit und nachgeschalteten SIEM-Systemen (Security Information and Event Management) nicht erkannt werden. Ihre Aktionen können sich hinter den Terabyte an Daten verstecken, die durch normale Benutzeraktivitäten generiert werden. Angreifer, die auf persistente Bedrohungen setzen, sind sich bewusst, dass viele Sicherheitsteams keine Chance haben, diese versteckten Bedrohungen zu entdecken: Grund dafür sind organisatorische Datensilos, Probleme bei der Datenerfassung, Skalierbarkeitseinschränkungen und ein Mangel an Analysemöglichkeiten. Sicherheitsteams können diesen Angreifern einen Strich durch die Rechnung machen, indem sie zur Analyse der Bedrohungsaktivitäten Risikokontext auf sicherheitsrelevante Daten anwenden. Wird die Analyse dann noch durch Bedrohungsdaten-Feeds unterstützt, können Analysten zuvor unbekannte Bedrohungen identifizieren und eine proaktive Risikominimierung vorantreiben. Weiterer Kontext kann mittels anderer Datenquellen im Unternehmen (z. B. Zeitwirtschaftssysteme, Personaldatenbanken, Inventardatenbanken) hinzugefügt werden, um Insider-Bedrohungen, einschließlich Betrug und Diebstahl geistigen Eigentums zu erkennen und zu verstehen. Aufgrund der dynamischen Bedrohungslandschaft müssen Sicherheitsteams analysebasierte Sicherheitsverfahren einsetzen, um das Sicherheitsniveau am Gefährdungsgrad des Unternehmens auszurichten.

Die Erkennung komplexer Bedrohungen und die Abschreckung interner Angreifer erfordern ein risikobasiertes Sicherheitskonzept, das sich nur mit Hilfe einer auf Big Data basierenden Security Intelligence-Plattform umsetzen lässt. Diese Plattform muss mit sämtlichen Maschinendaten und verschiedenen Bedrohungsdaten "gefüttert" werden und Funktionen für die Korrelation dieser Informationen mit beliebigen, vom Analysten festgelegten Maschinendaten bieten. Diese Möglichkeiten geben dem Sicherheitsanalysten kreative Freiheit und unterstützten den Einsatz von Visualisierungen sowie die Nutzung statistischer Analysen zur Aufdeckung unbekannter Bedrohungen.

Definition der analysegestützten Sicherheit:

Prozesse zur Erkennung von Beziehungen innerhalb sämtlicher sicherheitsrelevanter Daten, einschließlich Daten aus IT-Infrastrukturen, Punktlösungen für die Sicherheit und allen maschinengenerierten Daten, die eine schnelle Anpassung an die sich schnell ändernde Bedrohungslandschaft ermöglichen.

Die Splunk App for Enterprise Security

Es spielt keine Rolle, ob die Splunk App for Enterprise Security (ES) für kontinuierliches Monitoring, Reaktionprozesse, ein Security Operations Center oder Führungskräfte mit Bedarf an Informationen über die Unternehmensgefährdung eingesetzt wird – die App gibt Ihnen in jedem Fall die Flexibilität, Ansichten an spezifische Anforderungen anzupassen. Zu den Features der Splunk App for Enterprise Security gehören die durch einfache Mausklicks steuerbare Übertragungsdatenerfassung, ein benutzerfreundliches Framework für Bedrohungsdaten und sich selbst anpassende Korrelationen und Schwellenwerte. Alle diese Funktionen erleichtern Ihnen das Monitoring auf bekannte und unbekannte Bedrohungen. Zu den wichtigsten, sofort verwendbaren Inhalten gehören:

Überprüfung und Klassifizierung von Vorfällen: Als Teil einer umfassenden Funktionspalette zur Überprüfung von Vorfällen ermöglicht die Klassifizierung die Massen-Neuzuweisung von Ereignissen sowie Änderungen an Status und Kritikalitätseinstufung, wobei sämtliche Analystenaktionen für Auditing-Zwecke zur Verfügung stehen.

Berichte und Sicherheitsmetriken: Die App bietet zahlreiche Out-of-the-Box-Berichte, -Dashboards und -Metriken; Suchergebnisse können als Grafiken, Dashboards oder Tabellen dargestellt werden, damit unstrukturierte Rohdaten zu Analysen werden; Rohdaten können im PDF- oder CSV-Format exportiert werden.

Risikobasierte Analyse: Ermöglicht die Ausrichtung des Sicherheitsniveaus am Unternehmen, indem Beziehungen festgestellt werden und eine Gefährdungseinstufung der Daten vorgenommen wird, bei der die berücksichtigten Faktoren transparent gemacht werden; schnelle und einfache Zuordnung von KSI/KPI-Werten zu Ereignissen, um mithilfe des Risiko-Frameworks eine Risikoeinstufung zu erstellen.

Framework für Bedrohungsdaten: Dient zur Integration, Deduplizierung und Zuweisung von Gewichtungen zu beliebig vielen offenen, firmeneigenen oder lokalen Bedrohungsdaten-Feeds, durch die Threat Intelligence verständlicher und zu einer Kernkomponente Ihres Sicherheits-Workflows wird.

Universeller Sucheditor: Erleichtert die benutzerfreundliche, konsistente Erstellung von Suchvorgängen (einschließlich geführter Suchen) für KSI- (Key Security Indicator) oder KPI-Korrelationssuchen (Key Performance Indicator) sowie Visualisierungen für Identitäts- und Elementuntersuchungen (siehe Abbildung 1).

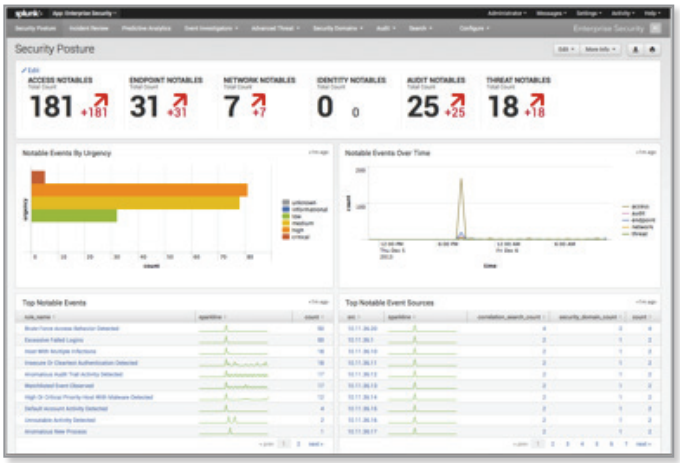

Abbildung 1: Enterprise Security 3.2 – Dashboard "Security Posture"

Statistische Analysen: Vordefinierte Dashboards erleichtern die Erkennung von Anomalien bei Ereignis- und Protokolldaten mithilfe selbstkonfigurierender Schwellen- und Basiswerte.

Flexible Dashboards: Erstellen Sie ein eigenes, auf Ihrer Rolle innerhalb der Organisationsstruktur basierendes Sicherheitsportal (siehe Abbildung 2); organisieren und korrelieren Sie mehrere Datenquellen visuell innerhalb einer Oberfläche, um Beziehungen zu erkennen und Kontext zu erhalten.

Durch die zeitindizierte Datenerfassung ohne vorherige Normalisierung und die Möglichkeit, schon beim Suchen ein Datenschema anwenden zu können, werden Hindernisse beim Erfassen und Anzeigen von Anwendungs- und Betriebsdaten zur Kontextermittlung für Sicherheitsereignisse aus dem Weg geräumt. Die Splunk-Plattform bietet die Möglichkeit, beliebige strukturierte und unstrukturierte Daten aus IT-, Sicherheits- und Produktionssystemen bzw. beliebigen Quellen für Maschinendaten zu erfassen und diese Daten im Zusammenhang mit Änderungs-Management und physischem Zugriff für Sicherheitsprozesse zu beleuchten. Splunk Enterprise und die Splunk App for Enterprise Security bieten eine umfassende, flexible und skalierbare Security Intelligence-Lösung, die weit über herkömmliche SIEM-Technologien hinausgeht.

Splunk App for Enterprise Security – Übersicht

Sicherheitsniveau

Nutzen Sie eine Bibliothek aus vordefinierten Sicherheitsmetriken, die Sie in Dashboards platzieren können, oder erstellen Sie ganz einfach eigene Metriken. Zeigen Sie Sicherheitsereignisse nach Standort, Host, Quelltyp, Inventargruppierung und Geographie an. KPIs ermöglichen das Echtzeit-Trending und -Monitoring Ihres Sicherheitsniveaus.

Überprüfung und Untersuchung von Vorfällen

Die Splunk App for Enterprise Security unterstützt das Drilldown von grafischen Elementen zu Rohdaten sowie die Erfassung von Übertragungsdaten, damit die gesamte Netzwerkkommunikation transparent wird. Spezifische Workflow-Aktionen verbessern die Vorgehensweise bei Sicherheitsuntersuchungen und ermöglichen dem Benutzer, die Pivot-Funktion für eine einzige allgemeine Information oder beliebige Daten auszuführen, um den Bedrohungskontext schnell zu entwickeln.

Zugriffsschutz

Erleichtern Sie Zugriffssteuerungs-Monitoring, Ausnahmeanalyse und Auditing-Prozesse für Anwendungen, Betriebssysteme und Identitätsmanagementsysteme im gesamten Unternehmen. Erfüllen Sie Compliance- und Forensikanforderungen im Zusammenhang mit der Erfassung von Benutzern mit sehr hohen Zugriffsrechten und Systemzugriffsversuchen in unternehmenskritischen Anwendungen.

Endpunktsicherheit

Erhöhen Sie die Wirksamkeit von Endpunktsicherheitsprodukten wie Symantec™ Endpoint Protection, IBM® Proventia Desktop oder McAfee® Endpoint Protection. Priorisieren Sie Bedrohungen und visualisieren Sie langfristige Trends. Die Endpunktsicherheit umfasst Suchvorgänge, Berichte und eine Bibliothek mit Benachrichtigungen zu Schadsoftware, seltenen Aktivitäten, Ressourcennutzung und -verfügbarkeit.

Netzwerksicherheit

Nutzen Sie Monitoring- und Erkennungsfunktionen für die Erfassung von Ereignissen aus Netzwerk- und Sicherheitstechnik im gesamten Unternehmen. Erkennen Sie Anomalien bei Protokolldaten, Firewalls, Routern, DHCP, Wireless Access Points, Load Balancern, Intrusion Detection-Sensoren und Datensicherungstechnik. Nutzen Sie Korrelationen, Suchvorgänge, Berichte und Dashboards für Monitoring- und Benachrichtigungsprozesse im Zusammenhang mit Netzwerkaktivitäten.

Asset Center/Identity Center

Wenn Sie verstehen, wo sich Elemente befinden, wer ihr Eigentümer ist, wie ihre Kritikalität eingestuft wird und, wer auf kritische Informationen in Systemen zugreifen dürfen sollte, dann erleichtert dies die Priorisierung von Sicherheitsereignissen und -untersuchungen. Die App nutzt die von Splunk gebotenen Möglichkeiten, Echtzeit-Lookups von Daten in Inventardatenbanken, Active Directory, Tabellenkalkulations- oder CSV-Dateien durchzuführen und Informationen als Kontext für Sicherheitsereignisse in Berichten und Dashboards zu verwenden.

Risikoanalyse

Ermitteln Sie Quellen, Schweregrade und zu berücksichtigende Faktoren der Risiken in Ihren Umgebung. Nutzen Sie Risikoeinstufungen dazu, ungewöhnliche Aktivitäten aufzuspüren.

Vorfallsüberprüfungs-Auditing

Zur Erleichterung von Kontrolle, Auditing und Manipulationssicherheit bietet die Splunk App for Enterprise Security Berichte zu sämtlichen Splunk-Benutzer- und -Systemaktivitäten für einen lückenlosen Audit Trail. Innerhalb der Splunk-Plattform wird die Datensignierung eingesetzt, um die Chain-of-Custody zu dokumentieren und jegliche Modifikationen an den Originaldaten von Logs und Ereignissen zu entdecken.

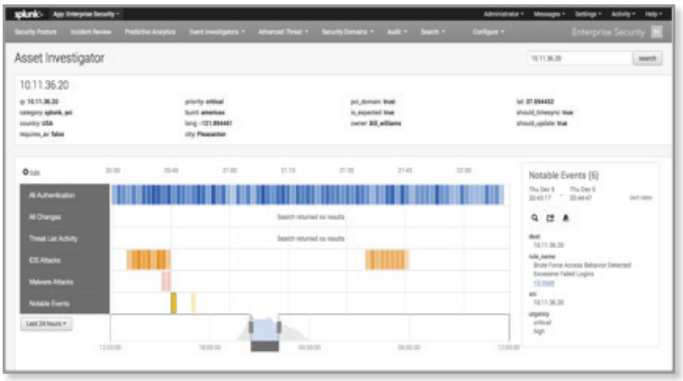

Abbildung 2: Enterprise Security 3.2 – Asset Investigator

Kostenloser Download

Laden Sie Splunk kostenlos herunter. Sie erhalten eine Splunk Enterprise 6-Lizenz für 60 Tage und können bis zu 500 Megabyte an Daten pro Tag indizieren. Während bzw. am Ende des Testzeitraums von 60 Tagen können Sie sich für eine ständige Splunk Free-Lizenz entscheiden oder aber eine Splunk Enterprise-Lizenz erwerben, indem Sie sich an dach_sales@splunk.com wenden.

250 Brannan St., San Francisco, CA 94107 info@splunk.com | dach_sales@splunk.com +49 (0)89 90 405 998 apps.splunk.com

Artikelnummer FS-SPLUNK-AppEntSec-117-A4