Security Data Warehouse – Next Generation Security Platform

Eine der wesentlichen Herausforderungen der heutigen Bedrohungslandschaft ist, dass Angreifer Zeit, Know-how und Ressourcen haben, um einen Angriff so auszuführen, dass dieser von den Security-Systemen nicht erkannt wird. Die Spuren der Angreifer sind in Terabytes von Daten versteckt und lassen sich nur schwer mit den klassischen Security-Systemen entdecken. Die Security-Analysten im Unternehmen scheitern in der Regel an klassischen Security Monitoring-Lösungen, weil die Daten dort entweder in Datensilos liegen, nicht oder nur teilweise erfasst werden oder notwendige Analysefunktionen nicht verfügbar sind und daher die Suche nach der sprichwörtlichen Nadel im Heuhaufen zur unlösbaren Herausforderung wird.

Um Angriffe schnell erkennen und analysieren zu können, werden neue Big Data-basierte Security Monitoring-Lösungen, sog. Next-Generation-Security-Monitor-Lösungen benötigt, die es ermöglichen, die Daten aller relevanten Systeme und Prozesse zu integrieren und schnell und einfach zu analysieren.

Die Splunk App für Enterprise Security (ES App) setzt auf Splunk Enterprise an und ermöglicht die Erkennung und Analyse potenzieller Bedrohungen mittels Monitoring, Benachrichtigungen und Analysen. Sie bietet die Möglichkeit, neue Daten schnell und ohne Normalisierung oder Connectoren zu integrieren und lässt sich somit dynamisch an jede geänderte Anforderung anpassen.

Funktionsweise

Die Splunk ES App ist eine App für die Splunk Operational Intelligence Plattform und wird auf einem dedizierten Searchhead installiert.

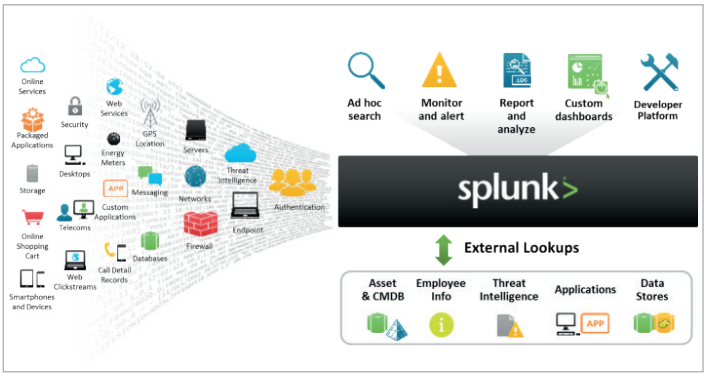

Abbildung 1: Funtkionsweise

Splunk ist eine Plattform für Operational Intelligence mit deren Hilfe sich beliebige Maschinendaten aus fast jeder Datenquelle in Echtzeit sammeln und indizieren lassen. Dies ermöglicht eine schnelle Suche auch in großen Datenmengen. Die Lösung bietet einen einfachen Weg, um Daten zu visualisieren, analysieren und damit besser nutzbar zu machen.

Der Vorteil der Lösung ist, dass für die Indizierung der Daten keinerlei Connectoren oder Parser notwendig sind. Die Normalisierung der Daten in Splunk für die Korrelation erfolgt ausschließlich zur Suchzeit und basiert auf dem CIM (Common Information Model). Sie erfolgt mit Hilfe der sogenannten Technology Add-ons, die mit der ES App mitkommen und für alle gängigen Security-Lösungen schon vordefinierte File-Extraktionen beinhalten.

Die ES App bietet dem Management wie auch den Analysten einen schnellen Überblick über den Sicherheitsstatus ihres Netzwerks und ermöglicht die genaue Analyse von Vorfällen und hilft damit den IT-Security-Spezialisten, schnell auf Vorfälle reagieren zu können. Anpassbare Korrelationssuchen, Schwellwerte und Risikometriken sowie Dashboards erlauben die Anpassung an die spezifischen Unternehmensbedürfnisse und Sicherheitsanforderungen.

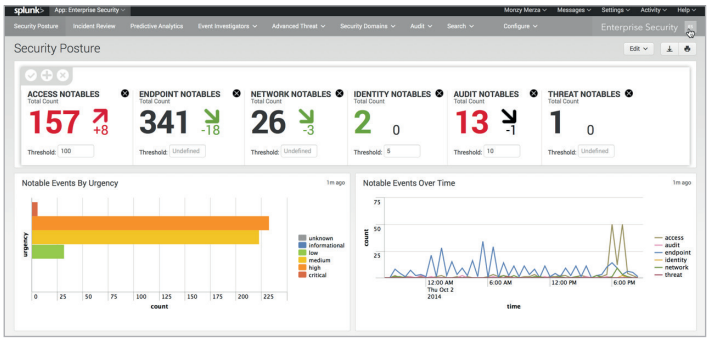

Abbildung 2: Security Posture

Überblick über die ES App

Vordefinierte Korrelationssuchen und KPIs ermöglichen ein kontinuierliches Monitoring von Sicherheitsvorfällen und lassen bereits im Vorfeld Entwicklungstrends erkennen.
Durch die Integration von Asset-Datenbanken und Account-Informationen lassen sich risikobasierte Analysen an die Unternehmensanforderungen und Rahmenbedingungen anpassen.

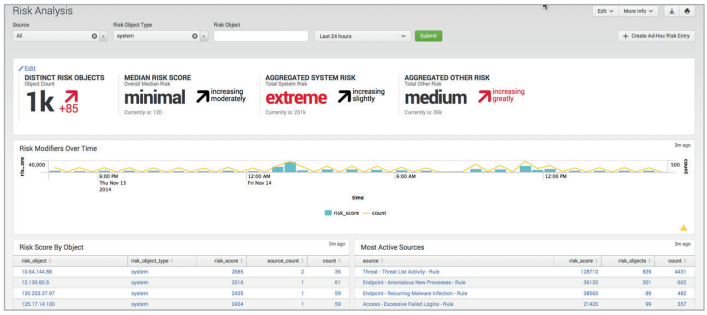

Abbildung 3: Risk Analysis

Das in der ES App integrierte Threat Intelligence Framework erlaubt die Integration von Threat Intelligence Feeds sowie den Austausch von Threat Informationen über Files, Web Feeds und Standards wie OpenIOX oder STIX/TAXII.

Spezielle Incident Review Dashboards und definierbare Workflow-Aktionen erlauben den Anwendern die Analyse von Vorfällen und den Drill Down bis zu den Rohdaten, die zu einem Incident geführt haben.

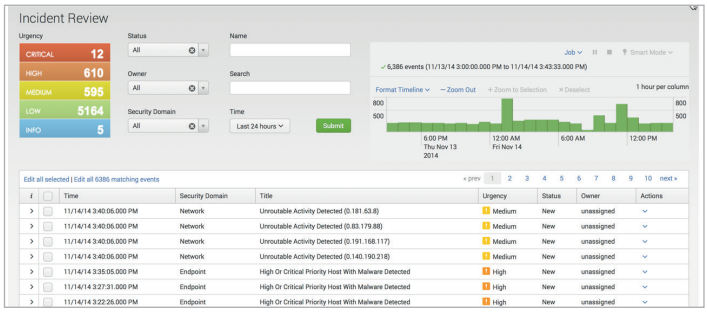

Abbildung 4: Incident Review

Architekturmodell

Die Splunk App für Enterprise Security ist eine Erweiterung (App) von Splunk. Sie wird auf einem dedizierten Searchhead installiert und bringt alle ES App Funktionen mit. Grundsätzlich nutzt die Splunk App für Enterprise Security die Standardfunktionen von Splunk.

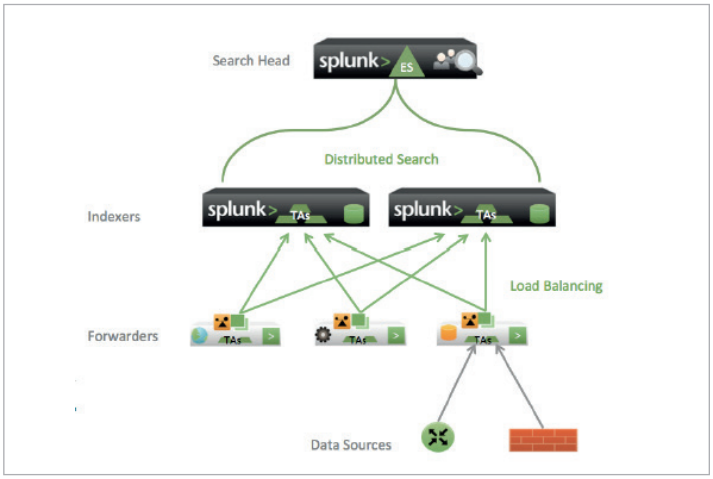

Abbildung 5: Architekturmodell

Preismodell

Die Splunk App für Entprise Security ist eine kostenpflichtige App, die wie Splunk Enterprise nach indizierten Datenvolumen pro Tag lizensiert wird.

Leistungen

iT-CUBE SYSTEMS berät Sie ausführlich darüber, welche Komponenten für Ihr Unternehmen in Betracht kommen und welche Lizenzen für das geplante Log-Aufkommen benötigt werden.

Die anschließende Implementierung erfolgt aus einer Hand Dank der engen Zusammenarbeit mit dem Hersteller, können wir eine hohe Qualität gewährleisten.

Zur Leistung der iT-CUBE gehört zunächst die umfassende Unterstützung bei der Installation und Konfiguration der Splunk ES App und ggf. bei der Implementierung der Splunk Plattform. Anschließend wird die Lösung in Ihr Unternehmensnetzwerk eingebunden und alle wichtigen Log-Quellen an sie angebunden. Egal ob Firewall, IPS, Windows, Malware Protection, o. .Ä., die Experten der iT-CUBE kennen bereits die meisten Systeme, die an die Lösung angebunden werden sollen.Während der Nutzung erstellen wir für Sie Reports und Auswertungen von Netzwerkaktivitäten und entwickeln kundenspezifische Use Cases zur Angriffserkennung oder zur Einhaltung von Compliance Anforderungen. Hier profitieren Sie von unserer umfangreichen Erfahrung aus diversen Log- und SIEM-Projekten. Wir unterziehen die Implementierung einem Health-Check, um den bestmöglichen Schutz zu gewährleisten und die Lösung immer auf dem aktuellsten Stand zu halten. Darüber hinaus bieten wir auch Schulungen für Ihre Mitarbeiter an, damit Sie selbstständig und schnell auf Probleme reagieren können.

Nutzen

Die Splunk ES App ist eine Big Data Security Plattform, welche skalierbar für alle Unternehmensgrößen ist. Sie bietet flexibles Deployment und verfügt über out-of-the-box Use Cases. Die Integration neuer Datenquellen erfolgt einfach, da weder Connectoren noch Parser im Voraus erstellt werden müssen.

Trotz großer Datenmengen ist eine schnelle und effiziente Suche, Analyse und Erstellung von Security Reports über alle Daten garantiert. Die Splunk ES App ermöglicht ein schnelleres Erkennen und Analysieren von Angreifern und Vorfällen und reduziert damit den Schaden durch Cyberangriffe am Unternehmen. Die Bedienung der App ist dank der webbasierten Oberfläche besonders nutzerfreundlich.

In der Splunk ES App lässt sich ein granulares, rollenbasiertes Berechtigungsmodell erstellen. Darüber hinaus lassen sich Threat Intelligence Feeds einfach in ihr integrieren.

iT-CUBE SYSTEMS AG

Paul-Gerhardt-Allee 24
81245 München, Germany

T: +49 89 2000 148 00
F: +49 89 2000 148 29

info@it-cube.de
www.it-cube.de