splunk>

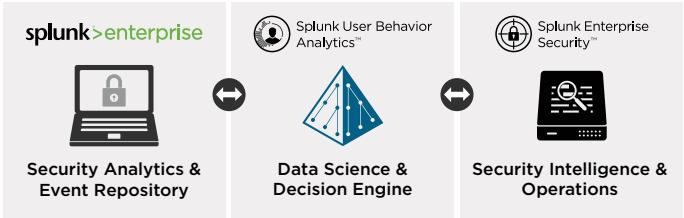
PRODUCT BRIEF

SPLUNK® USER BEHAVIOR ANALYTICS

Erkennen von Cyber-Angriffen und Insider-Bedrohungen

- **Verbesserte Erkennung** bekannter, unbekannter und versteckter Cyber-Angriffe und Insider-Bedrohungen
- **Höhere Produktivität von Sicherheitsanalysten** durch Priorisieren von Bedrohungen und Vermeidung von False Positives (falschen Alarmen)
- **Benutzerfreundlich** für SOC-Analysten, CERT Teams und SIEM-Administratoren

Komplexe Sicherheitsanalyse



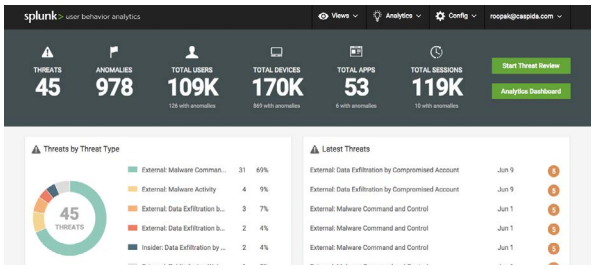
Komplexe Cyber-Angriffe sind oftmals gut versteckt und schwer aufzuspüren, es ist jedoch für den Schutz vertraulicher Daten unabdingbar, solche Bedrohungen anzugehen. IT-Sicherheitsanalysten haben daher die Aufgabe, die in IT-Umgebungen versteckten Bedrohungen unabhängig von Größe und Expertise des Unternehmens zu finden und abzuwehren.

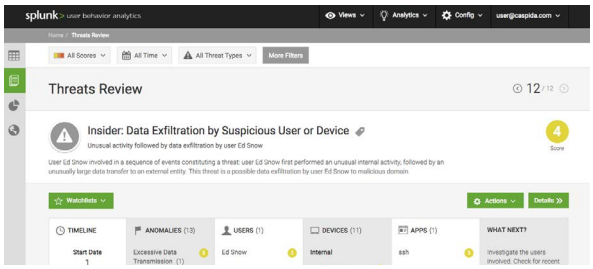
Splunk User Behavior Analytics (Splunk UBA) ist eine Lösung, mit der Unternehmen bekannte, unbekannte und versteckte Bedrohungen mittels Machine Learning, Baselining, Peer-Gruppen-Analysen und komplexer Korrelation aufdecken und versteckte APT-Bedrohungen (Advanced Persistent Threats), Infektionen mit Schadsoftware und Insider-Angriffe aufspüren können. Splunk UBA setzt bei der Unterstützung von Arbeitsabläufen für Sicherheitsanalysten an, erfordert nur minimalen Verwaltungsaufwand und lässt sich in bestehende Infrastrukturen integrieren, um versteckte Bedrohungen zu lokalisieren.

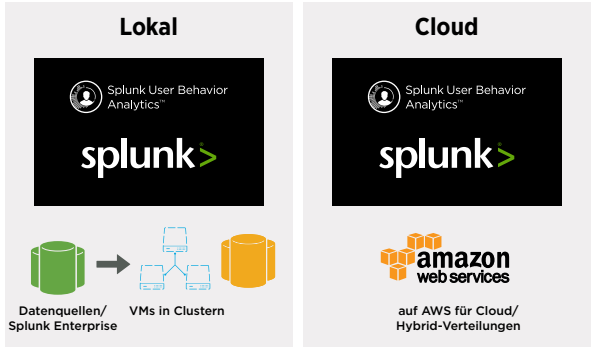
Was ist verhaltensbasierte Bedrohungserkennung? Die verhaltensbasierte Bedrohungserkennung basiert auf Machine Learning-Methodiken, die keine Signaturen oder menschlichen Analysen erfordern und die Erstellung von Profilen zum Verhalten mehrerer Entitäten sowie Peer-Gruppen-Analysen ermöglichen – und zwar für Benutzer, Geräte, Dienstkonten und Anwendungen. Das Ergebnis dieser Auswertungen ist eine automatisierte, exakte Bedrohungs- und Anomalieerkennung.

Der gesamte Lebenszyklus des Sicherheitsprozesses – von Vorbeugung, Erkennung, Reaktion und Abwehr bis hin zum kontinuierlichen Feedback-Austausch – muss durch kontinuierliches Monitoring und leistungsfähige Analysen vereinheitlicht werden, um kontextbezogene Intelligence bereitzustellen. Splunk Enterprise, Splunk Enterprise Security (ES) und Splunk UBA sind aufeinander abgestimmt und bieten:

- Erweiterung der auf Suchen/Mustern/Ausdrücken (Regeln) basierenden Methoden in Splunk Enterprise und Splunk Enterprise Security (Splunk ES) durch Verfahren zur Erkennung von Bedrohungen, damit Bedrohungen mithilfe fortschrittlicher "Kill Chain"-Visualisierungen aufgespürt werden können
- Verfahren für Sicherheitsteams wie Machine Learning, welche die Erstellung statistischer Modelle zur Erkennung von Anomalien erlauben, bei denen die in Splunk Enterprise gespeicherten Daten ohne großen Aufwand genutzt werden können
- Verknüpfung von Machine Learning-Methoden und komplexen Analysemöglichkeiten, damit Unternehmen unabhängig von Größe und technischem Know-how bekannte und unbekannte Bedrohungen überwachen, durch Benachrichtigungen bekanntmachen, analysieren, untersuchen, abwehren und erkennen können







Optimierter Bedrohungs-Workflow

Reduzieren Sie Milliarden von Original-Ereignissen zunächst auf Tausende von Anomalien und dann auf eine Handvoll Bedrohungen, die Sie schnell prüfen und abwehren können. Nutzen Sie für Sicherheitssemantik optimierte Machine Learning-Algorithmen, dynamische Statistikmethoden und Korrelationen, um versteckte Bedrohungen ohne menschliche Analysen zu identifizieren. Durch Hinzufügen von Kontext-, Standort- und weiteren Informationen werden False Positive Werte vermieden.

Bedrohungsprüfung und -untersuchung

Stellen Sie den Ablauf von Bedrohungen visuell dar und identifizieren Sie verdächtiges Verhalten und Auffälligkeiten. Entdecken Sie kritische Bedrohungen mithilfe komplexer, modellübergreifender Korrelationen, bei denen Selbstlernfunktionen und adaptive Algorithmen eingesetzt werden (Machine Learning und Statistik). Untersuchen Sie Bedrohungen und entsprechende Nachweise interaktiv.

Kill Chain-Erkennung und Identifikation des Angriffsvektors

Erkennen Sie auffällige APTs bzw. Sicherheitsverstöße (z. B. Command&Control Server/CnC, laterale Kommunikation) und Kill Chain-Angriffe (etwa Pass-the-Hash-Angriffe). Finden Sie Bewegungsmuster, die Anzeichen für die Verbreitung von Schadsoftware oder böswilliger Insider sind. Reagieren Sie auf Echtzeit-Warnungen zu Aktivitäten (z. B. verdächtige URL oder Land-Speed-Anmeldeverstöße). Erkennen Sie verhaltensbasierte Unregelmäßigkeiten (z. B. Bedrohungsaktivitäten beim VM- oder AWS-Container). Identifizieren Sie Botnet- oder CnC-Aktivitäten (wie Trojaner oder polymorphe Schadsoftware).

Plattformarchitektur und Implementierungsoptionen

Splunk UBA beinhaltet das Hadoop-Ökosystem für skalierbare, kosteneffiziente und offene Datenpersistenz. Das Produkt ist auf Echtzeit-Ereignisanalysen in großem Maßstab ausgelegt und umfasst Zeitreihen- und Diagrammdatenbanken für die Verarbeitung und Darstellung von Sicherheitsverbindungen innerhalb des Netzwerks. RESTful-APIs automatisieren die Datenzufuhr mithilfe von Produkten von Drittanbietern und unterstützen damit Gegen- und Vorbeugemaßnahmen. Splunk UBA skaliert erwiesenermaßen auf Hunderte von Terabyte und Milliarden von Ereignissen und kann als lokale Software, auf einer virtuellen Maschine oder als vom Kunden verwaltete, öffentliche Cloud-Instanz (AWS und vCloud Air) eingesetzt werden.

Laden Sie Splunk Free herunter oder testen Sie die Online-Sandbox. Ob für cloud-basierte oder lokale Umgebungen, große oder kleine Teams – Splunk hat auf jeden Fall ein passendes Verteilungsmodell für Sie. **Erfahren Sie mehr** über Splunk User Behavioral Analytics von **ubainfo@splunk.com**.

splunk> SplunkCe@Splunk.com www.splunk.com

PB-Splunk-UBA-A4-105