splunk>

PRODUCT BRIEF

SPLUNK® ENTERPRISE SECURITY

Analysegestützte Sicherheit und kontinuierliches Monitoring auf moderne Sicherheitsbedrohungen

- **Optimierung von Sicherheitsprozessen** durch kürzere Reaktionszeiten
- **Verbessern des Sicherheitsniveaus** durch End-to-End-Transparenz innerhalb sämtlicher Maschinendaten
- **Mehr Untersuchungsmöglichkeiten** aufgrund der Feststellung von Anomalien und Bedrohungen mittels der Analyse des Benutzerverhaltens
- **Fundiertere Entscheidungen** aufgrund von Bedrohungsinformationen

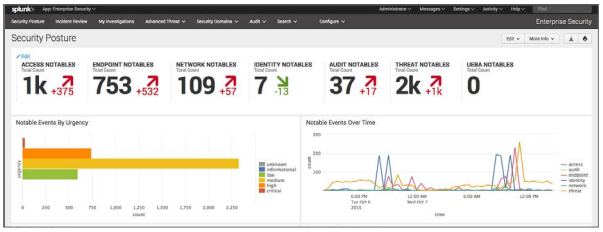
Moderne Unternehmen sind mit Herausforderungen wie eine dynamische Bedrohungslandschaft, ständig weiterentwickelte Angriffstaktiken, komplexe Bedrohungen und variable Unternehmensanforderungen konfrontiert, und die vorhandenen Sicherheitstechnologien können damit nicht Schritt halten. Angesichts dieser neuen Herausforderungen brauchen Sicherheitsteams Analysemöglichkeiten und kontextspezifische Responseprozesse. Zudem müssen sie schnell Verfahren zur Erkennung neuer Bedrohungen implementieren können, um die Reaktionszeit bei Vorfällen zu verkürzen und unternehmensorientierte Entscheidungen zu treffen. Sicherheitsteams können Angriffe schneller erkennen, abwehren und eingrenzen, wenn sämtliche Maschinendaten zentral verwaltet und genutzt werden.

Splunk Enterprise Security (ES) ist eine Premium-Sicherheitslösung, mit der Sicherheitsteams interne und externe Angriffe schnell erkennen und abwehren und somit das Threat Management vereinfachen, Risiken minimieren und Ihr Unternehmen schützen können. Mit Splunk ES können Ihre Sicherheitsteams alle Daten nutzen, um unternehmensweite Transparenz zu erzielen und Security Intelligence zu gewinnen. Es spielt keine Rolle, ob Splunk ES lokal, in einer öffentlichen oder privaten Cloud, als SaaS oder mit einer beliebigen Kombination dieser Modelle verteilt wird – die Lösung kann in jedem Fall für kontinuierliches Monitoring, eine schnelle Reaktion bei Vorfällen, ein SOC (Security Operations Center) oder für Führungskräfte eingesetzt werden, die eine Sicht auf Unternehmensrisiken brauchen. Splunk ES kann als Software zusammen mit Splunk Enterprise oder als Cloud-Service mit Splunk Cloud verteilt werden.

Mit Splunk ES können Sicherheitsteams Sicherheitsprozesse für Unternehmen jeder Größe und Expertise optimieren. Die Lösung bietet Folgendes:

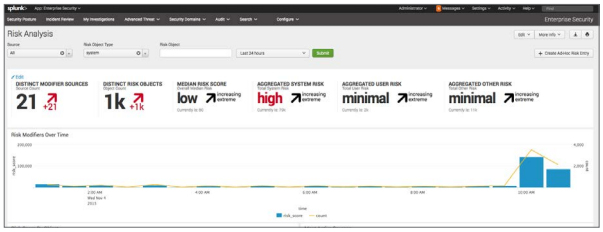
- **Erkenntnisse aus Daten,** die von Sicherheitstechnologien erzeugt werden, wie Angaben über Netzwerke, Endpunkte, Zugriffe, UBA-Anomalien, Schadsoftware, Schwachstellen sowie Identitätsdaten, die mit vordefinierten Regeln oder über Ad-hoc-Suchen korreliert werden
- **Gebrauchsfertige Funktionen für die Verwaltung von Benachrichtigungen** und für dynamische Entdeckungen, kontextbezogene Suchen und die schnelle Erkennung und Analyse komplexer Bedrohungen
- **Flexibilität für die Anpassung** von Korrelationssuchen, Benachrichtigungen, Berichten und Dashboards an spezifische Anforderungen, ganz gleich, ob Splunk ES für kontinuierliches Monitoring, eine schnelle Reaktion bei Vorfällen, ein SOC (Security Operations Center) oder für Führungskräfte eingesetzt wird, die eine Sicht auf Unternehmensrisiken brauchen

Definition analysegestützter Sicherheit **Der Prozess, bei dem Beziehungen zwischen sämtlichen sicherheitsrelevanten Daten aufgedeckt werden, damit eine schnelle Anpassung an neue Entwicklungen in der Bedrohungslandschaft möglich ist. (Zu den sicherheitsrelevanten Daten zählen dabei Daten aus IT-Infrastrukturen und individuellen Sicherheitslösungen sowie sämtliche maschinengenerierten Daten.)**



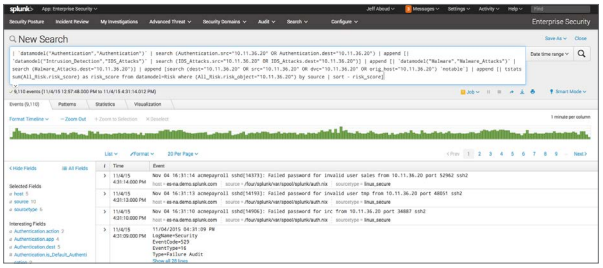
Ständiges Monitoring des Sicherheitsniveaus

Verschaffen Sie sich ein klares, grafisch aufbereitetes Bild vom Sicherheitsniveau des Unternehmens mithilfe zahlreicher, vordefinierter Dashboards, wichtiger Sicherheitsindikatoren (KSIs) und Leistungsmetriken (KPIs), statischer und dynamischer Schwellenwerte sowie Trendindikatoren.



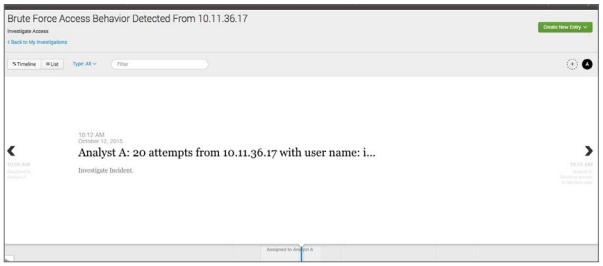
Priorisieren und Handeln bei Vorfällen

Optimieren Sie Vorfallsreaktions-Workflows für einzelne Analysten oder Untersuchungsteams mithilfe zentral verwalteter Logs, Benachrichtigungen und Vorfälle, UBA-Anomalien, vordefinierter Berichte und Korrelationen, Vorfallsreaktions-Workflows und Korrelationen für eine sicherheitsspezifische Sicht.



Schnelle Untersuchung von Bedrohungen

Führen Sie schnelle Untersuchungen mit Ad-hoc-Suchen sowie statischen, dynamischen und visuellen Korrelationen durch, um böswillige Aktivitäten aufzuspüren. Erstellen Sie Untersuchung und Pivots zu beliebigen Datenfeldern, um schnell den Bedrohungskontext und die Angriffsschritte zu ermitteln, damit Sie Hinweise überprüfen, weitere Informationen gewinnen und mit Teammitgliedern zusammenarbeiten können.



Mehrstufige Untersuchungen

Führen Sie Sicherheitsverletzungs- und Untersuchungsanalysen durch, um die Aktivitäten im Zusammenhang mit den kompromittierten Systemen nachzuverfolgen. Wenden Sie die "Kill Chain"-Methodik" an und untersuchen Sie den Lebenszyklus von Angriffen mit Ad-hoc-Suchen, sämtlichen Splunk ES-Funktionen und spezifischen Features wie dem Untersuchungsprotokoll und der Vorfallszeitachse.

Testen Sie Splunk Enterprise Security Überzeugen Sie sich von der Leistungsfähigkeit von Splunk Enterprise Security, ganz ohne Downloads, Hardwareeinrichtung oder Konfiguration. Mit der Splunk Enterprise Security Online-Umgebung mit mehr Untersuchungsmöglichkeiten aufgrund der Feststellung von Anomalien und Bedrohungen mittels der Analyse des Benutzerverhaltens erhalten Sie sieben Tage lang Zugriff auf eine Testumgebung mit bereits vorhandenen Daten in der Cloud, in der Sie Daten durchsuchen, visualisieren und analysieren sowie Vorfälle aus verschiedensten Sicherheitsbereichen eingehend untersuchen können. Sie können auch die schrittweise Anleitung durchgehen, um die mit der Splunk-Software möglichen leistungsfähigen Visualisierungen und Analysen kennen zu lernen. **Erfahren Sie mehr.**

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