Die fünf wichtigsten Use Cases für Splunk

Security Analytics

splunk>

turn data into doing™

Es ist nicht leicht, Sicherheitsvorfälle schnell zu erkennen und darauf zu reagieren. Sicherheitsanalysten brauchen einige Minuten (manchmal auch Stunden) für die Bearbeitung eines Warnhinweises. Multipliziert man das mit den Hunderten von Sicherheitswarnungen, die täglich eingehen, so bleiben unterm Strich zu viele Tickets und zu wenige Analysten. Dies ist die Ausgangslage.

Wir müssen den Sicherheitsteams dabei helfen, ihre Reaktionszeiten zu verkürzen, und wir müssen gleichzeitig die Anzahl der Warnhinweise reduzieren. Wir können als Erstes die Transparenz ihrer Umgebungen verbessern, sodass die Teams Bedrohungen schneller erkennen und schneller darauf reagieren. Besser noch: Automatisierte Reaktionen je nach Warnpriorisierung können Minuten auf Sekunden verkürzen und Stunden zu Minuten. Das klingt doch schon ganz gut.

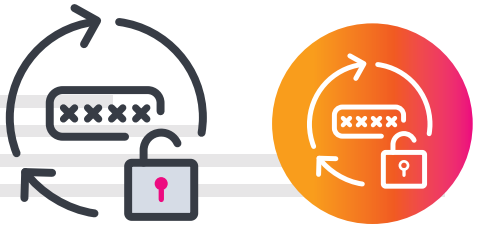
Dann haben heimtückische Bedrohungen wie Malware, die normalerweise schwer zu entdecken sind, weniger Möglichkeiten, sich zu verstecken und zu verbreiten. Und der Schaden, den sie anrichten können, hält sich in Grenzen. Und überarbeitete Sicherheitsanalysten gewinnen wieder Luft für konzentriertes Arbeiten.

Trotzdem ist das Leben in einer sich schnell wandelnden Security-Landschaft nicht immer so einfach. Die meisten Sicherheitsteams müssen erst noch herausfinden, wohin ihre Reise gehen soll. Nachdem aber klar ist, dass potenziell jeder Teil des Unternehmens anfällig ist und es an ihnen liegt, Sicherheitslücken rechtzeitig zu erkennen, wird das Ganze schnell zu einer Aufgabe, die selbst die Besten der Branche wenn nicht überfordert, so doch vor ernsthafte Probleme stellt.

Die gute Nachricht: Wir bei Splunk arbeiten mit unseren Kunden schon seit Jahren daran, genau dieses Problem zu lösen. Wir haben schon bei den schwierigsten Sicherheitsfragen geholfen – einfach dadurch, dass Splunk die Antworten aufzeigt, die in den Daten der Kunden verborgen liegen.

Die Erfahrungen mit unseren Kunden haben wir hier in einem kompakten Leitfaden zusammengefasst, der die wichtigsten Use Cases und die ersten Schritte beschreibt. Es geht um die Sicherheitsprobleme, zu denen wir am häufigsten gefragt werden; dazu gibt es Best Practices für die Umsetzung sowie praktische Vorschläge, damit die Sicherheitsteams sofort loslegen können, wenn sie Splunk Enterprise Security (ES) implementieren oder anpassen.

01



Kompromittierte Anmeldedaten

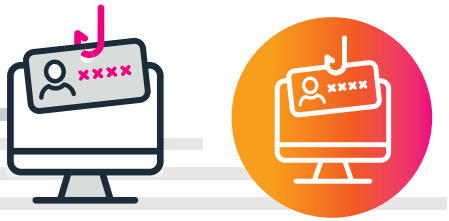
Was sind kompromittierte Anmeldedaten?

Wenn Angreifer die zur Anmeldung erforderlichen Daten von Mitarbeitern erlangen, meist durch gängige Methoden wie Phishing oder CEO Fraud, dann gelten diese Log-in-Daten als kompromittiert. Sind die Schadakteure erst einmal mit den an sich legitimen Anmeldedaten in eine Umgebung gelangt, halten sie nach Schwachstellen Ausschau, durch die sie ihre Ziele erreichen können. Ein Albtraum für Sicherheitsverantwortliche. Das Fatale ist, dass sich die Bedrohungsakteure mit gültigen Log-in-Daten anmelden und somit den Anschein erwecken, dass sie vollkommen rechtmäßige Anwender sind. Das macht die Erkennung dieser Art von Bedrohung so enorm schwer.

Wie geht Splunk mit kompromittierten Anmeldedaten um?

Splunk Security Analytics (SSA) kann herausfinden, ob Anmeldedaten kompromittiert und von einer anderen als der autorisierten Person oder Anwendung verwendet werden. SSA kommt dabei auch mit Gemeinschaftskonten (Shared Accounts) und generischen Accounts klar. Die SSA-Verhaltensmodellierung benachrichtigt die Analysten, wenn ein User Aktivitäten zeigt, die insofern ungewöhnlich sind, als sie von seinem als normal definierten Verhalten abweichen. Die Erkennung umfasst die Identifizierung ungewöhnlicher oder schädlicher Active-Directory-Aktivitäten, wie z. B. selbstbezügliche Operationen oder solche, die mit gelöschten Benutzern, deaktivierten Konten und der Kontowiederherstellung zu tun haben.

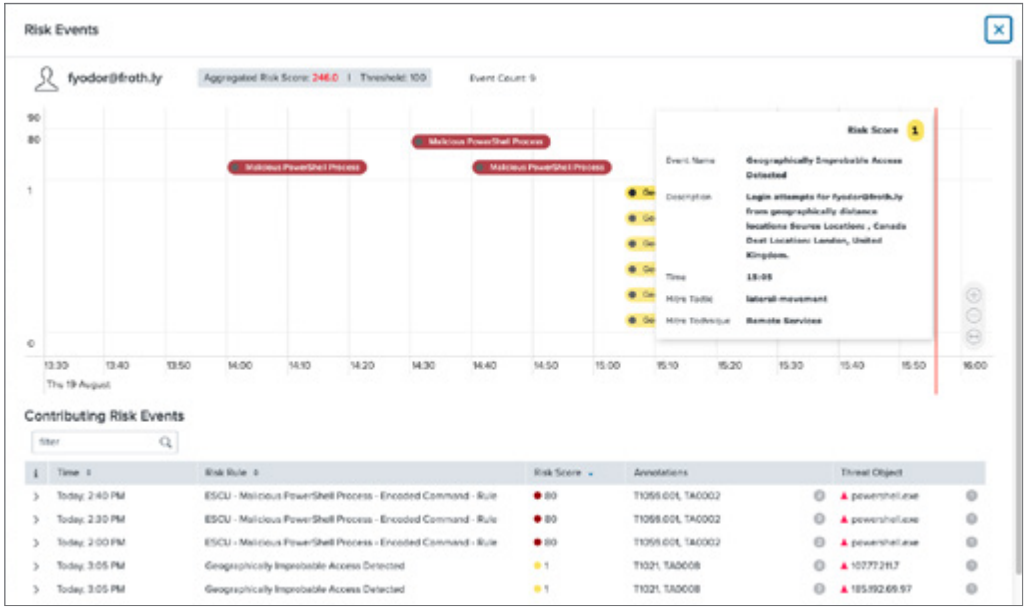
02



Kompromittierte privilegierte Benutzer

Was sind kompromittierte privilegierte Benutzer?

Wenn Hacker durch Social Engineering oder Zero Day Exploits Zugriff auf ein privilegiertes Benutzerkonto erlangen, sind diese Konten kompromittiert. Die Hacker umgehen dabei meist herkömmliche Sicherheitstools wie Firewalls oder veraltete SIEM-Lösungen (Security Information Event Management), die auf bekannte Bedrohungen ausgelegt sind. Diese Angreifer zielen auf die Führungsebene und Anwender mit umfangreichen Rechten, die Zugriff auf sensible Daten haben. Darum ist es wichtig, dass Sicherheitsanalysten es sofort erkennen, wenn ein privilegiertes Konto kompromittiert wird. Sind die Hacker erst im System, bauen sie ihre Rechte aus und sehen sich nach sensiblen Informationen wie Passwörtern oder SSH-Schlüsseln um.

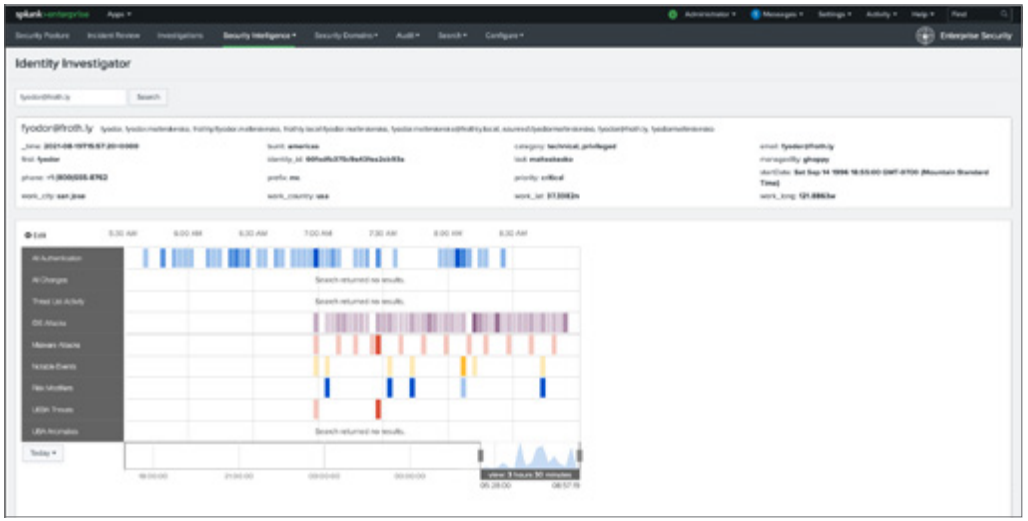


Splunk UBA ermöglicht eine Risikobewertung, die sich an einer festgelegten Normallinie ausrichtet.

Wie geht Splunk mit Kompromittierungen privilegierter Benutzer um?

Splunk Security Analytics etabliert für jedes Benutzerkonto eine Normallinie des Verhaltens und identifiziert Unregelmäßigkeiten im Abgleich mit dieser individuellen Grundlinie. Erkennbar sind daraus z. B. übermäßige Nutzung oder sehr seltener Zugriff, aber auch Hinweise auf potenzielle Sabotage oder die Versuche einer Person, ihre Spuren zu verwischen. Je länger das Verhalten vom gewohnten abweicht, desto bestimmter wird die Erkennung durch SSA, und damit steigt die Risikowahrscheinlichkeit ebenso wie die Risikostufe. Auffälligkeiten in diesem Sinne wären z. B. VPN-Zugriffe über Servicekonten, das Ausspähen von Daten, die Löschung von Prüfprotokollen oder der Zugriff auf vertrauliche Informationen.

03



Beispiel eines Splunk-Dashboard, das bei der Identifizierung von Insider-Bedrohungen hilft.

Insider-Bedrohung

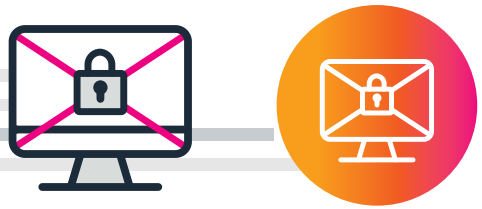
Was ist eine Insider-Bedrohung?

Von Insider-Bedrohungen spricht man, wenn Beschäftigte oder Auftragnehmer mit Zugang zu privilegierten Informationen ihre Zugänge absichtlich oder versehentlich missbrauchen und dadurch dem Unternehmen schaden. Dieses Problem ist weit verbreitet: Ganze zwei Drittel der Angriffe bzw. Datenverluste sind auf Insider-Bedrohungen zurückzuführen. Das gemeinsame Merkmal von kompromittierten Anmeldedaten, Kompromittierungen privilegierter Benutzer und Insider-Bedrohungen ist, dass in allen drei Fällen gültige Anmeldedaten missbraucht werden.

Wie geht Splunk mit Insider-Bedrohungen um?

Splunk Security Analytics erfasst den Fußabdruck eines Angreifers, der sich durch die Umgebungen des Unternehmens bewegt – inklusive Cloud und Mobile. Seine Aktivitäten werden mithilfe fortschrittlicher Algorithmen maschinellen Lernens analysiert, sodass sich anhand der Normallinie Abweichungen und Anomalien nahezu in Echtzeit erkennen lassen. Sämtliche Hacker-Aktionen in einer Umgebung werden zu einer anschaulichen Sequenz zusammengefügt, die mithilfe von Mustererkennung und intelligenter Korrelation die Kill Chain deutlich macht, sodass die Sicherheitsteams sofort Maßnahmen ergreifen können.

04



Ransomware

Was ist Ransomware?

Ransomware ist eine Sorte von Malware, die sich leider immer größerer Beliebtheit erfreut. Selbst US-Präsident Joe Biden ist bereits auf diese Bedrohung aufmerksam geworden. Ransomware-Angriffe beginnen oft damit, dass arglose Anwender durch Phishing dazu gebracht werden, ihre Zugangsdaten preiszugeben. Danach wird die eigentliche Malware eingeschleust, die bestimmte (oder alle) Daten des Opfers verschlüsselt. Die Bedrohungsakteure fordern dann Lösegeld (engl. ransom – daher der Name), das bei Unternehmen und Organisationen fünf- bis siebenstellige Summen erreichen kann. Bezahlt werden soll die Freigabe der Daten in der Regel in Kryptowährungen.

Wie geht Splunk mit Ransomware um?

Splunk Security Analytics bekommt Updates aus dem Splunk ES Content Update (ESCU), das Sicherheitsanalysten mit gebündelten Sicherheitsinhalten versorgt, die sie bei der Bekämpfung aktueller Bedrohungen, Angriffsmethoden und bei anderen Sicherheitsproblemen unterstützen. Derzeit sind im ESCU 35 Ransomware-Anwendungsfälle enthalten. Sobald neue Bedrohungen entdeckt werden, macht sich das Security Threat Intelligence Team von Splunk ans Reverse Engineering und verteilt dann Updates über das ESCU, sodass die Erkennungen jederzeit auf dem neuesten Stand bleiben.

05

Cloud-Sicherheit

Was ist Cloud-Sicherheit?

Cloud-Sicherheit beruht auf der Erkenntnis, dass sich Cybersicherheit von der Orientierung an Unternehmensgrenzen und einem netzwerkzentrierten Ansatz lösen muss (den viele der herkömmlichen Sicherheitslösungen immer noch verfolgen). Der Grund dafür liegt in den Cloud-Strategien der Wirtschaft, die zuletzt durch Covid-19 und den massenhaften Wechsel ins Homeoffice noch forciert wurden.

Weil sich Cloud Computing immer mehr durchsetzt und entsprechend immer mehr Unternehmen zentrale Bereiche ihres Geschäfts auf GCP (Google Cloud Platform), AWS (Amazon Web Services), Microsoft Azure oder eine andere Public Cloud verlagern, ist es wichtig, dass Unternehmen ihre Daten ohne Umstände in Echtzeit analysieren können. Erst damit schaffen sie die Transparenz, die nötig ist, um den Hackern stets einen Schritt voraus zu bleiben.

Was leistet Splunk für die Cloud-Sicherheit?

Splunk Security Analytics erleichtert das Onboarding von A&I (Assets and Identities) aus GCP, AWS und Azure, sodass sich die A&I-Tabellen in Splunk direkt befüllen lassen. Darüber hinaus bietet SSA für die drei großen Cloud-Anbieter einsatzfertige Erkennungsfunktionen in den Bereichen Authentifizierung, Netzwerkverkehr und Konfigurationsänderungen. Durch das Mapping der genannten Datenmodelle der Cloud-Anbieter auf das CIM (Common Information Model) von Splunk werden die bestehenden Erkennungs- und Untersuchungsworkflows des Unternehmens um die entscheidenden Cloud-Daten angereichert.

Bereit für weniger Sicherheitsverstöße

mit einem analysegestützten SIEM in der Cloud?

Erfahren Sie, wie Sie mit Splunk am besten loslegen!

Mehr erfahren

21-20968-Splunk-Top 5 Use Cases for Splunk Security Analytics-LS-104_DE