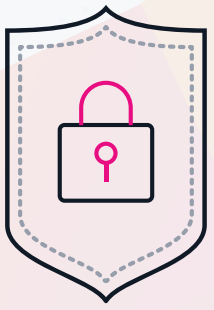
Basisleitfaden
IT-Sicherheit

Erste Schritte mit Splunk für Security zur Lösung Ihrer alltäglichen Herausforderungen



splunk>
turn data into doing™

Was ist Ihre Strategie für Cybersicherheit?

Planen Sie nur für den Ernstfall und hoffen auf das Beste?

Inhalt

Einleitung 5
- Splunk im Security Operations Center (SOC) 6

Verstehen der Grundlagen 8
- Splunks Weg zu analysegestützter Sicherheit 8
- Die Splunk Security Suite 10
- Die Security Use Cases 12

Der Beginn Ihrer analysegestützten Sicherheitsreise 15

Phase 1: Datenerfassung 16

Phase 2: Normalisierung 20

Phase 3: Erweiterung 22

Phase 4: Veredelung 24

Phase 5: Automatisierung und Orchestrierung 26

Phase 6: Komplexe Erkennung 28

Lösen häufiger Herausforderungen an die Sicherheit mit der Splunk Security Operations Suite 30
- Incident-Untersuchung und Forensik 32
  - Erkennen von Seitwärtsbewegung mit WMI 32
  - Identifizierung mehrfacher nicht autorisierter Zugriffsversuche 35
- Sicherheits-Monitoring 38
  - Erkennen öffentlicher S3-Buckets in AWS 38
  - Auffinden von Mehrfachinfektionen auf Hosts 42
- Erkennung komplexer Bedrohungen 44
  - Erkennen von Verbindungen zu neuen Domänen 44
  - Finden von E-Mails mit Doppelgänger-Domänen 48
- SOC-Automatisierung 52
  - Automatisierung von Untersuchungen auf Malware 52
  - Automatisieren von Phishing-Untersuchungen und -Reaktionen 54
- Incident Response 56
  - Erkennen von neuen Exfiltrations-DLP-Benachrichtigungen für Benutzer 58
  - Identifizieren von einfacher dynamischer DNS-Erkennung 58
- Compliance 62
  - Erkennen neuer lokaler Administratorkonten 64
  - Erkennen von Benutzern, die regelwidrig bei Systemen angemeldet sind, die Complianceregeln unterliegen 65
- Analyse und Erkennung von Betrugsversuchen 68
  - Erkennen kompromittierter Benutzerkonten 68
  - Auffinden anomaler Transaktionen im Gesundheitswesen 71
- Erkennung interner Bedrohungen 73
  - Erkennen großer Webuploads 73
  - Erkennen der erfolgreichen Anmeldung bei einem Konto eines ehemaligen Mitarbeiters 76

Wie können Sie dann Ihr Unternehmen am besten verteidigen und neue Gefahren beseitigen?

Die Antwort: mit einem ganzheitlichen Ansatz für sämtliche Verteidigungssysteme im gesamten Unternehmen.

Einleitung

Was ist Ihre Strategie für Cybersicherheit? Planen Sie lediglich für den Ernstfall und hoffen auf das Beste? Da digitale Technologien jeden Teil unseres Lebens berühren und täglich neue Bedrohungen auftauchen, ist es unerlässlich, dass Ihr Unternehmen präzise, informiert und vorbereitet ist, wenn es um die Verteidigung Ihrer Assets und die Beseitigung von Bedrohungen geht.

Schwerwiegende Sicherheitsverstöße, globale Ransomware-Angriffe und die Crypto-Mining-Plage sind gute Gründe dafür, dass Ihr Unternehmen die richtigen Daten erfassen, nutzen und verstehen muss. Darüber hinaus ist es wichtig, dass Sie frühzeitig die richtigen Prozesse und Verfahren implementieren, und das häufig in Kombination mit neuen Technologien, Methoden und Anforderungen – alles bei ständig zunehmender Geschwindigkeit und Variabilität von Maschinendaten.

Wie können Sie also Ihr Unternehmen am besten verteidigen und neue Gefahren beseitigen? Im Endeffekt benötigen Sie dazu einen ganzheitlichen Ansatz für sämtliche Verteidigungssystem im gesamten Unternehmen. Aus diesem Grund glaubt Splunk, dass jedes Unternehmen ein Security Nerve Center, ein Nervenzentrum der IT-Sicherheit benötigt, das in sechs aufeinanderfolgenden Phasen implementiert wird. Diese sechs Phasen möchten wir Ihnen im Folgenden vorstellen.

Sehen wir uns an, was dies im Einzelnen bedeutet.

Splunk im Security Operations Center (SOC)

Datengetriebene Unternehmen setzen auf das IMAA-Modell (Investigate, Monitor, Analyze and Act) zum Untersuchen, Überwachen, Analysieren und Nutzen ihrer Daten. So können sie die Sicherheit verbessern, indem sie ihre Arbeitsergebnisse, Prozesse und Technologien optimieren. Dies beinhaltet die Nutzung sämtlicher Daten aus dem Sicherheitstechnologie-Stack, um Bedrohungen zu untersuchen, aufzuspüren und schnell koordinierte Abwehrmaßnahmen in manueller, halbautomatisierter oder automatisierter Form zu ergreifen. Wenn Security-Teams in ihre Sicherheitsinfrastruktur investieren, stärkt dies ihr Sicherheitsökosystem und ihre Kompetenzen, was eine Ausweitung der Sicherheitspraktiken auf neue Bereiche und den proaktiven Umgang mit Cyberbedrohungen ermöglicht.

Splunks Data-to-Everything Plattform und das Sicherheitsportfolio von Splunk verbinden mehrere Bereiche der Cybersicherheit sowie andere Bereiche außerhalb der Cybersecurity, um die Zusammenarbeit zu fördern und Best Practices für die Interaktion mit Daten zu implementieren. Sicherheitsteams können mithilfe von Splunk-Lösungen statistische, visuelle, verhaltensbasierte und explorative Analysen vorantreiben, welche die Grundlage für Entscheidungen und Maßnahmen bilden. Davon ausgehend ermöglicht die Plattform einen modernen Workflow: vom Erfassen der Daten bis hin zum Auslösen von Maßnahmen zur Bewältigung von Cyberbedrohungen und -herausforderungen.

Abbildung 1: Splunk Enterprise Security umfasst ein gemeinsames Framework für die Interaktion mit Daten und zum Einleiten von Aktionen. Das Adaptive Operations Framework ermöglicht IT-Sicherheitsteams die schnelle und zuverlässige Anwendung von Änderungen auf die Umgebung. Mit Splunk Enterprise Security können Sie auch die Abwehrreaktionen automatisieren und so die Sicherheitsinfrastruktur für jede Domäne unter Verwendung einer Vielzahl geeigneter Aktionen auf die Angriffe abstimmen.

Klingt doch gut, oder?

Schön. Aber wie das Ganze jetzt in die Praxis umsetzen fragen Sie sich?

Um Ihnen den Einstieg zu erleichtern, haben wir diesen kurzen Leitfaden zusammengestellt. Wir stellen Ihnen die wichtigsten Anwendungsfälle im IT-Sicherheitsbereich vor, mit denen sich Unternehmen konfrontiert sehen, und zeigen Ihnen, wie die analysegestützte Plattform von Splunk Sie bei der Lösung Ihrer eigenen Sicherheitsherausforderungen unterstützen kann. Dieser Leitfaden ist in drei Abschnitte unterteilt:

1. Verstehen der Grundlagen. Hier finden Sie eine kurze Einführung, sowohl in Ihre „Security Journey“ als auch zu verschiedenen Security Use Cases, wobei jeder Use Case der entsprechenden Splunk-Lösung zugeordnet wird.

2. Ihr Weg zu analysegestützter Sicherheit. In diesem Teil erläutern wir die sechs Phasen auf dem Weg zur datengestützten Sicherheit und was Sie in den einzelnen Phasen wie gut beherrschen sollten.

3. Lösen häufiger Security-Herausforderungen mit Splunk.
Hier führen wir Sie schrittweise durch Beispiele, wie Sie gängige Sicherheitsherausforderungen lösen können, die mit den folgenden Punkten zusammenhängen:

- Incident-Untersuchung und Forensik
- Sicherheits-Monitoring
- Erkennung komplexer Bedrohungen
- SOC-Automatisierung
- Incident Response, Compliance
- Betrugs- und Analyseerkennung
- Insider-Bedrohung

Bereit, die IT-Sicherheit Ihres Unternehmens auf ein neues Level zu heben? Dann mal los.

Verstehen der Grundlagen

Cyberkriminelle ruhen nie. Das bedeutet, dass Sie ständig nach neuen Security Use Cases und Sicherheitsinformationen suchen sollten, um ein hohes Schutzniveau in Ihrer Umgebung aufrechtzuerhalten.

Wir unterstützen Sie gerne.

Mit Splunk auf die Reise zu analysegestützter Sicherheit

Jeder, dem einmal die Frage „Sind wir sicher?“ gestellt wurde, weiß, dass Cybersicherheit ein Weg und kein Ziel ist. Auch wenn die Reise keinen Endpunkt hat und es immer wieder neue Herausforderungen geben wird, gibt es Dinge, die Sie tun können, um währenddessen erfolgreich zu sein.

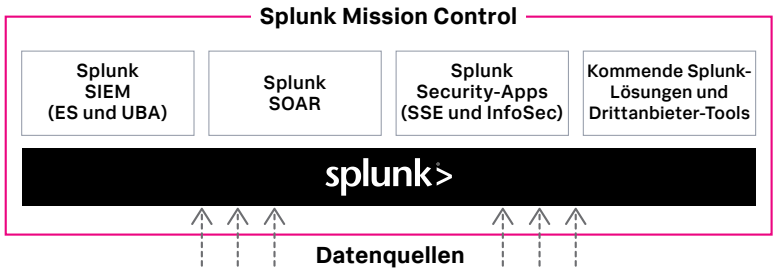
Dazu müssen Sie zuerst Ihre Umgebung verstehen und einen Einstiegspunkt finden. Fragen Sie sich Folgendes: Was versuche ich, zu schützen? Was sind meine kritischen Daten? Wie werde ich auf Bedrohungen reagieren?

Die sechsstufige, analysegestützte Sicherheitsreise, die in Abbildung 2 dargestellt ist, hilft Ihnen beim Beantworten dieser Fragen und beim Erstellen herausragender Sicherheitspraktiken, die es Ihnen ermöglichen, die Lücken in Ihrer Verteidigung zu verstehen, die nächste Herausforderung zu sehen und Maßnahmen zu ergreifen, um ihr zu begegnen.

Abbildung 2: Splunks Weg zu analysegestützter Sicherheit

Splunks Security Suite

Würden Sie sich auf eine Expedition begeben ohne Karte und einen Rucksack voller Proviant und die richtige Ausrüstung? Sicher nicht. So, wie keine Expedition ohne die richtige Ausrüstung erfolgreich sein kann, so kann auch keine Sicherheitsreise ohne die richtige Technologie erfolgreich sein.



Splunks Security Suite hilft Sicherheitsteams, sich in unbekannten Gewässern zu bewegen und Bedrohungen in dynamischen, digitalen Unternehmensumgebungen schnell zu erkennen, zu untersuchen, abzuwehren und sich ihnen anzupassen. Splunk-Lösungen können von einem Tier-1-Analysten für einfache Nachforschung zu einem Zeitraum, einem Schlüsselwort, einer IP-Adresse oder einem Computernamen verwendet werden. Die gleichen Produkte ermöglichen es Tier-2 und Tier-3-Analysten, erweiterte Korrelationen durchzuführen, analytische Modelle zu erstellen oder fortgeschrittene Forensik zu betreiben.

Splunks Security Suite	
Splunk Enterprise	Eine flexible Plattform, die eine Reihe von Sicherheits-Use Cases abdeckt und es Ihnen ermöglicht, Maschinendaten aus beliebigen Quellen schnell zu überwachen und zu analysieren, um Erkenntnisse zur Maßnahmenergreifung sowie das analysegestützte Fundament zur Stärkung Ihrer Gesamtsicherheit zu liefern. In der Cloud verfügbar.
Splunk Enterprise Security	Eine SIEM-Lösung (Security Information and Event Management), die Einblicke in von Sicherheitstechnologien erzeugte Maschinendaten liefert. Hierzu gehören Angaben über Netzwerke, Endpunkte und Zugriffe, Schwachstellen sowie Identitätsdaten. In der Cloud verfügbar.
Splunk User Behavior Analytics	Eine auf Machine Learning gestützte Lösung, die die nötigen Antworten liefert, damit Unternehmen unbekannte Bedrohungen und anomales Verhalten über sämtliche Benutzer, Endgeräte und Anwendungen hinweg aufspüren können.
Splunk Phantom	Eine SOAR-Plattform (Security Orchestration, Automation and Response), die sich in Ihre bestehenden Sicherheitstechnologien integriert und eine Schicht „Bindegewebe“ zwischen ihnen bildet, die sie intelligenter, schneller und stärker machen.
Anwendungen	Von Splunk, Partnern und unserer Community entwickelte Apps zur Steigerung und Erweiterung des Potenzials der Splunk-Plattform. Ein Beispiel ist die Splunk App for Payment Card Industry (PCI) Compliance. In der Cloud verfügbar.
Splunk Security Essentials	Untersuchen Sie neue Use Cases und stellen Sie Sicherheitserkennungen aus Splunk Security Essentials in Splunk Enterprise und Splunk Cloud sowie Splunk SIEM- und SOAR-Produkten bereit. Mit einer aktiven Splunk Cloud-Lizenz wird die App jetzt vollständig unterstützt: Stärken Sie Ihr Sicherheitsniveau und verkürzen Sie Ihre Time-to-Value mit Splunk.
Splunk Enterprise Security Content Updates	Bietet für Splunk Enterprise Security (ES)-Kunden Anleitungen zur Sicherheitsanalyse (sogenannte „Analyseberichte“ bzw. „Analytic Stories“), die erläutern, wie Splunk ES optimal für Untersuchungen und das Ergreifen von Maßnahmen gegen neue, in Ihrer Umgebung entdeckte Bedrohungen eingesetzt wird, welche Suchen implementiert werden sollten und was dabei Ihr realistisches Ziel sein sollte.

Die Security Use Cases

Die nachfolgende Tabelle enthält die jeweiligen Security Use Cases, die wir der Sicherheitsreise zugeordnet haben. Nur zu: Wählen Sie Ihr eigenes Abenteuer bzw. Ihre ganz persönliche Sicherheitsherausforderung. Dieser Leitfaden soll Ihnen zeigen, wie die analysegestützte Splunk-Plattform helfen kann, Ihre Sicherheitsherausforderungen zu lösen und Sie auf Ihrer Reise Richtung IT-Sicherheit voranzubringen:

Splunk-Lösungen und passende Security Use Cases

Use Case	Splunk-Lösung
Incident-Untersuchung und Forensik	Splunk Enterprise, Splunk Enterprise Security, Splunk Phantom
Sicherheits-Monitoring	Splunk Enterprise, Splunk Security Essentials App, Splunk Enterprise Security, Splunk Phantom
Erkennung komplexer Bedrohungen	Splunk Enterprise, Splunk Security Essentials App, Splunk Enterprise Security, Splunk User Behavior Analytics
SOC-Automatisierung	Splunk Enterprise, Splunk Enterprise Security, Splunk Phantom
Incident Response	Splunk Enterprise, Splunk Enterprise Security, Splunk Phantom
Compliance	Splunk Enterprise, Splunk Security Essentials App, PCI, Splunk Enterprise Security
Analyse und Erkennung von Betrugsversuchen	Splunk Enterprise, Splunk Security Essentials App, Splunk Enterprise Security
Erkennung interner Bedrohungen	Splunk Enterprise, Splunk Security Essentials App, Splunk User Behavior Analytics

Definition der Security Use Cases

Der folgende kurze Überblick über die Anwendungsfälle soll eine einheitliche Ausgangsbasis schaffen.

Incident-Untersuchung und Forensik

Sicherheitsrelevante IT-Ereignisse können ohne Warnung auftreten und bleiben häufig so lange unentdeckt, bis sie eine ernsthafte Bedrohung der Sicherheit einer Organisation darstellen. Bis das Sicherheitsteam ein Problem feststellt, sind höchstwahrscheinlich schon negative Auswirkungen für Ihr Unternehmen entstanden. Splunk bietet Sicherheitsteams eine einzelne Informationsquelle für sämtliche, mit Zeitstempel versehene Maschinendaten in einer Computerumgebung. Dies ermöglicht bessere, schnellere Sicherheitsuntersuchungen und senkt damit die Wahrscheinlichkeit, dass Bedrohungen über längere Zeit unentdeckt bleiben.

Sicherheits-Monitoring

Sicherheits-Monitoring ermöglicht es Ihnen, einen kontinuierlichen Strom von Daten auf Bedrohungen und weitere potenzielle Sicherheitsprobleme nahezu in Echtzeit zu analysieren. Zu den Datenquellen für das Monitoring gehören Netzwerk- und Endpunktsysteme – ebenso wie Cloud-Geräte sowie Systeme und Anwendungen in Rechenzentren. Splunks Data-to-Everything Plattform ermöglicht es Sicherheitsteams, Bedrohungen, die im Datenstrom dieser Quellen gefunden werden können, zu erkennen und zu priorisieren.

Erkennung komplexer Bedrohungen

Bei einer APT-Bedrohung (Advanced Persistent Threat) handelt es sich um eine Gruppe verdeckter, kontinuierlicher Hacking-Prozesse, die häufig von einer oder mehreren Personen angestoßen und koordiniert werden und eine bestimmte Entität zum Ziel haben. APTs zielen meist aus wirtschaftlichen oder politischen Gründen auf privatwirtschaftliche Unternehmen und/oder Staaten ab. Splunk Enterprise ermöglicht es Unternehmen, Daten zu durchsuchen und zu korrelieren, um komplexe Bedrohungen zu verfolgen. Splunk Enterprise Security und Splunk User Behavior Analytics erweitern vorhandene Fähigkeiten zur Anwendung einer Kill-Chain-Methodik um statistische Analysen, Anomalieerkennung und Machine Learning-Verfahren. So können unbekannte und komplexe Bedrohungen besser aufgespürt werden.

SOC-Automatisierung

Security Operations-Teams verwenden Splunk-Software für die Orchestrierung und Automatisierung von Veredelungs- und Reaktionsmaßnahmen sowie für das Fallmanagement (d. h. Incidents). Sie nutzen die SOC-Automatisierungslösungen von Splunk, um den Betrieb zu skalieren, schneller zu reagieren und Bedrohungen und andere Sicherheitsprobleme zu beheben. Die Splunk-Lösungen unterstützen Unternehmen außerdem bei der Operationalisierung von analysegestützten Sicherheitspraktiken und befähigen Sicherheitsteams zur Zusammenarbeit in erweiterten bzw. abteilungsübergreifenden Teams.

Incident Response

Incident Response (IR) umfasst die Überwachung und Erkennung von sicherheitsrelevanten Events auf IT-Systemen und die Ausführung von Reaktionsplänen auf diese Events. IR-Teams werden auch als Blue Teams bzw. blaue Teams bezeichnet. Blaue Teams verteidigen die Infrastruktur einer Organisation, wenn Bedrohungen erkannt werden, während rote Teams (Red Teams) versuchen, Schwachstellen in der bestehenden Konfiguration derselben Systeme zu entdecken. Splunk bietet eine Vielzahl von IR-Funktionen im Sicherheitsportfolio, abhängig von den von Ihnen gewählten Angeboten. Jedes bietet Mechanismen zur Durchführung von Untersuchungen für erkannte Events. Splunk-Lösungen können darüber hinaus Funktionen enthalten, um Tier-1-Analysten mittels standardisierter Response-Verfahren anzuleiten.

Compliance

In fast allen Umgebungen gibt es gesetzliche Anforderungen in der einen oder anderen Form, besonders im Zusammenhang mit DSGVO, HIPAA, PCI, SOX und sogar allgemeinen Richtlinien, die nicht als echte Compliance-Anforderungen gelten, wie die **20 kritischen Sicherheitskontrollen**. Es gibt viele verschiedene Wege, Compliance-Herausforderungen mithilfe von Splunk zu meistern. So kann die Plattform beispielsweise Compliance automatisch zu belegen oder zur Erstellung von Korrelationsregeln und Berichten eingesetzt werden, die Bedrohungen für sensible Daten oder Mitarbeiter in Schlüsselpositionen aufzeigen.

Analyse und Erkennung von Betrugsversuchen

Im digitalen Zeitalter sind Maschinendaten Hauptbestandteil bei der Erkennung betrügerischer Aktivitäten. Splunk kann neue Daten integrieren, so dass Betrugsbekämpfungsteams Anomalien besser erkennen und untersuchen können. Dies ermöglicht Unternehmen, finanzielle Verluste zu verringern, ihren Ruf zu schützen und eine effiziente Organisation aufrecht zu erhalten.

Erkennung interner Bedrohungen

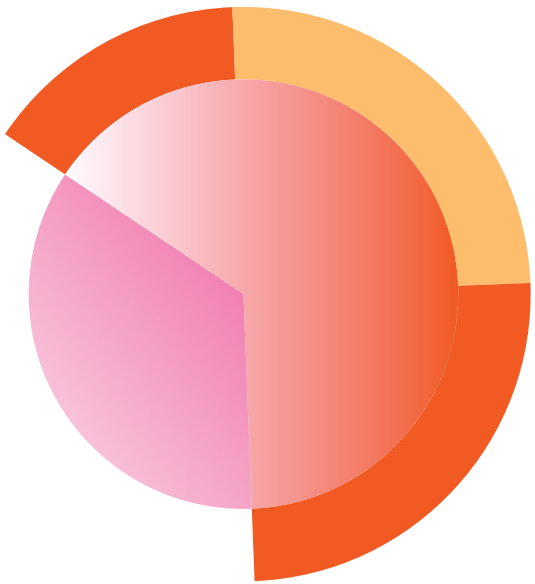
Insider-Bedrohungen gehen von aktuellen oder ehemaligen Mitarbeitern, Auftragnehmern oder Partnern aus, die Zugang zum Unternehmensnetzwerk haben und absichtlich oder unabsichtlich sensible Daten exfiltrieren, missbrauchen oder vernichten. Sie haben oftmals legitimen Zugang zu Netzwerken und die Berechtigung, vertrauliches Material herunterzuladen, wodurch herkömmliche Sicherheitsprodukte leicht ausgehebelt werden können. Durch den Einsatz von Splunk haben Sicherheitsteams die Möglichkeit, Bedrohungen durch Insider und kompromittierte Mitarbeiter zu erkennen und zu priorisieren, die sonst unbemerkt blieben.

Der Beginn Ihrer analysegestützten Sicherheitsreise

Um effektiv zu sein, muss sich ein Cybersicherheitsprogramm ständig weiterentwickeln. Das Problem ist, dass viele Organisationen kein klares Verständnis davon haben, wo sie stehen und wie sie sich verbessern können. Wenn Sie wissen, wo Sie sich auf Ihrer Reise befinden, können Sie Ihre Zeit und Ihre Ressourcen effektiver einsetzen. Und mit einer Vorstellung von dem, was kommen wird, lässt sich Erfolg in späteren Phasen besser planen.

Hier ist eine Aufstellung der sechs Phasen Ihrer Reise. Dabei werden Daten genutzt, um Angriffen immer einen Schritt voraus zu sein. Für jede Phase sehen wir uns folgende Punkte genauer an:

- Relevanz für bestimmte Security Use Cases
- Datenquellen
- Meilensteine
- Herausforderungen



Phase 1: **Datenerfassung**

Erfassen Sie grundlegende Sicherheitslogs und andere Maschinendaten aus Ihrer Umgebung.

Security Use Case Relevanz

Incident-Untersuchung & Forensik

Sicherheits-Monitoring

Erkennung komplexer Bedrohungen

SOC-Automatisierung

Incident Response

Compliance

Analyse und Erkennung von Betrugsversuchen

Insider-Bedrohungen

Beschreibung

Phase 1 konzentriert sich auf den Erwerb des Rohmaterials, das für ein tieferes Verständnis der zu verteidigenden Umgebung erforderlich ist.

Datenquellen
In dieser Phase ist es Best Practice, vier wesentliche Kategorien von Sicherheitsdaten zu erfassen:

1. **Netzwerk.** Die Transparenz des Netzwerkverkehrs ist für jedes IT-Sicherheitsteam von zentraler Bedeutung. In dieser frühen Phase hat es Priorität, sehen zu können, welche Arten von Datenverkehr in und aus Ihrem Netzwerk stattfinden. Es ist wichtig, den zugelassenen Datenverkehr und auch die blockierten Kommunikationsversuche zu sehen.

   Mögliche Datenquellen sind:

   • Firewall Traffic Logs von Anbietern wie:
   - Palo Alto Networks
   - Cisco
   - Checkpoint
   - Fortinet

2. **Endpunkt (host-basiert).** Endpunkt-Logs ergänzen die Netzwerksichtbarkeit, um Einblicke in böswillige Aktivitäten zu erhalten. Hierzu gehören beispielsweise die Ausführung von Schadsoftware, die Durchführung unbefugter Aktivitäten durch einen Insider oder die Präsenz eines Angreifers in Ihrem Netzwerk. Es ist wichtig, diese Daten von Servern, Workstations und aus sämtlichen Betriebssystemen zu erfassen.

   Mögliche Datenquellen sind:

   - Windows-Ereignisprotokolle
   - Linux-Systemprotokolle
   - Linux Auditd-Logs
   - MacOS-Systemprotokolle

3. **Authentifizierung.** Aus Authentifizierungsprotokollen können Sie ersehen, wann und von wo aus Benutzer auf Systeme und Anwendungen zugreifen. Da bei den meisten erfolgreichen Angriffen schließlich gültige Anmeldeinformationen verwendet werden, sind diese Daten kritisch, um den Unterschied zwischen einer gültigen Anmeldung und einer Account-Übernahme zu erkennen.

   Mögliche Datenquellen sind:

   - Windows Active Directory
   - Lokale Authentifizierung
   - Cloudidentität und Access Management (IAM)
   - Linux Auditd-Logs
   - MacOS-Systemprotokolle

4. **Webaktivität.** Viele Angriffe beginnen damit, dass ein Benutzer eine böswillige Website besucht, bzw. enden damit, dass wertvolle Daten zu einer Website exfiltriert werden, die der Angreifer kontrolliert. Für Untersuchungen muss daher unbedingt sichtbar sein, wer wann auf welche Websites zugreift.

Mögliche Datenquellen sind:

- Firewall-Datenverkehrsfilter der nächsten Generation (Next-Generation Firewall, NGFW)
  oder Proxy Logs von Anbietern wie:
  - Palo Alto Networks
  - Cisco
  - Checkpoint
  - Fortinet
  - Bluecoat
  - Websense

Meilensteine

Nach der erfolgreichen Integration von Daten aus diesen vier Kategorien sollten Sie die folgenden Meilensteine erreicht haben:

- Kritische Aktivitätsprotokolle wurden auf ein separaten System verschoben, auf dem sie nur schwer von Angreifern manipuliert werden können
- Daten aus den vier Kategorien sind verfügbar, um grundlegende Untersuchungen auszuführen.

Herausforderungen

Das Sammeln der verschiedenen Datenquellen ist oftmals mühsam, und es kann anstrengend sein, sicherzustellen, dass die integrierten Daten korrekt sind. Häufig wird dieser Schritt nicht ordnungsgemäß durchgeführt und es nur unzureichend Informationen erfasst, was zu Zeitverlust und unvollständigen Untersuchungen führt.

Phase 2: **Normalisierung**

Wenden Sie eine standardmäßige Sicherheitstaxonomie an und fügen Sie Asset- und Identitätsdaten hinzu.

Security Use Case Relevanz

Incident-Untersuchung & Forensik

Sicherheits-Monitoring

Erkennung komplexer Bedrohungen

SOC-Automatisierung

Incident Response

Compliance

Analyse und Erkennung von Betrugsversuchen

Insider-Bedrohungen

Beschreibung

In Phase 2 stellen Sie sicher, dass Ihre Daten mit einer standardmäßigen Sicherheitstaxonomie konform sind. Das bedeutet, dass Felder für gängige Werte, wie Quell-IP-Adresse, Port, Benutzername usw. nun allgemeine Namen haben, unabhängig davon, von welchem Gerät das Event erstellt wurde. Diese kritische Investition in die Normalisierung der Daten ermöglicht Ihnen:

- eine größere Auswahl an Erkennungsmechanismen von verschiedenen Anbietern und aus der Community zu nutzen
- mit der Implementierung eines SOC (Security Operations Center) zum Verfolgen von Systemen und Benutzern in Ihrem Netzwerk zu beginnen
- die Fähigkeiten Ihres Sicherheitsteams zu skalieren.

Selbst wenn Sie nicht vorhaben, ein formelles SOC einzurichten, werden Ihnen normalisierte Daten dabei helfen:

- die quellübergreifende Korrelation zu erleichtern
- Untersuchungen zu optimieren
- die Effektivität von Analysten zu verbessern.

Datenquellen

In Phase 2 sollten Sie die folgende Referenzinformationen erfassen:

- IT-Assets (Systeme, Netzwerke, Geräte, Anwendungen)
- Benutzeridentitäten aus Active Directory, LDAP und anderen IAM/SSO-Systemen.

Meilensteine

Phase 2 beinhaltet folgende Meilensteine:

- Daten werden dem gemeinsamen Informationsmodell (CIM, Common Information Model) korrekt zugeordnet.
- Die Suchleistung wird durch die Verwendung beschleunigter Datenmodelle im Zusammenhang mit CIM drastisch verbessert.
- Asset- und Benutzerdetails werden mit Events in Ihrer Sicherheitsprotokollplattform korreliert.

Herausforderungen

Zwar verfügen Sie über grundlegende Daten, die auch durchsuchbar sind, Ihnen fehlen aber die Erkenntnisse oder das Verständnis, die Sie für tiefere Sicherheitsermittlungen und Endpunkttransparenz benötigen.

Phase 3: **Erweiterung**

Erfassen Sie weitere, zuverlässige Datenquellen wie Endpunktaktivitäts- und Netzwerkmetadaten zur Unterstützung der Erkennung komplexer Bedrohungen.

Security Use Case Relevanz

Incident-Untersuchung & Forensik

Sicherheits-Monitoring

Erkennung komplexer Bedrohungen

SOC-Automatisierung

Incident Response

Compliance

Analyse und Erkennung von Betrugsversuchen

Insider-Bedrohungen

Beschreibung

DNS- (Domain Name System) und Endpunktdaten setzen eine Vielzahl von Erkennungsmöglichkeiten frei, die es Bedrohungsjägern ermöglichen, im Netzwerk versteckt agierende Gegner zu finden und zu verfolgen.

Datenquellen

Zu den Datenquellen in dieser Phase gehören:

1. **Netzwerk.** Die meisten Bedrohungsjäger und Threat Intelligence-Analysten werden Ihnen sagen, dass sie, wenn sie sich für nur eine einzige Datenquelle zur Analyse entscheiden müssten, DNS wählen würden.

   Mögliche Datenquellen sind:

   - Protokollspezifische Übertragungsdaten aus Quellen wie Splunk Stream oder Bro;
   - Daten der DNS-Abfrageebene aus Protokollen der Debug-Ebene oder aus Übertragungsdatenquellen
   - DHCP-Aktivität

2. **Endpunkt.** Umfangreiche Endpunkt-Aktivitäten, die die Prozesserstellung, Dateiänderungen, Registrierungsänderungen, Netzwerkverbindungen usw. erfassen, liefern eine erstaunlich klare Historie der kritischen Events, die an einem Endpunkt auftreten.

   Mögliche Datenquellen sind:

   - Sysmon
   - Osquery
   - Carbon Black Defense

Meilensteine

Durch das Sammeln zuverlässiger Datenquellen haben Sie Folgendes erreicht:

- Die Grundlage für komplexe Erkennungsvorgänge gelegt
- Sie haben jetzt die Möglichkeit, einige gängige Kompromittierungs-Indikatoren abzugleichen.

Herausforderungen

Die erfassten Netzwerk- und Endpunktdaten sind zwar detailreich, es fehlt ihnen jedoch an Kontext und sie könnten Gefährdungsindikatoren enthalten, die in Ihrer Branche bekannt sind, in Ihrer direkten Umgebung jedoch unentdeckt bleiben.

Phase 4: **Veredelung**

Reichern Sie Sicherheitsdaten mit Informationsquellen an, um ein besseres Verständnis von Kontext und Auswirkung eines Event zu erhalten.

Security Use Case Relevanz

Incident-Untersuchung & Forensik

Sicherheits-Monitoring

Erkennung komplexer Bedrohungen

SOC-Automatisierung

Incident Response

Compliance

Analyse und Erkennung von Betrugsversuchen

Insider-Bedrohungen

Beschreibung

Maschinendaten sind zwar wichtig, doch erfolgreiche IT-Sicherheitsteams veredeln ihre Daten mit zusätzlichen Informationen aus internen und externen Quellen. Dank einer Fülle von Kontext- und Untersuchungsdaten, einschließlich Feeds mit Bedrohungsinformationen, OSINT-Quellen (Open Source Intelligence) und intern erfassten Informationen, kann Ihr Sicherheitsteam, mehr Nutzen aus den gesammelten Daten ziehen, um Sicherheits-Events und -Incidents früher zu erkennen.

Datenquellen

Mögliche Datenquellen sind:

- Lokale IP/URL-Blockierungslisten
- Open Source-Feeds mit Bedrohungsinformationen
- Kommerzielle Feeds mit Bedrohungsinformationen

Meilensteine

Durch die Veredelung der Daten mit Informationen, die Kontext bereitstellen, können IT-Sicherheitsteams:

- Die Dringlichkeit einer Benachrichtigung auf Grundlage der Kritikalität eines Assets einschätzen
- Benachrichtigungen ergänzen, durch Abgleich mit Feeds mit Bedrohungsinformationen, Pivots zu anderen Systemen und Einleitung weiterer Aktivitäten zur Kontexterfassung.

Herausforderungen

Sie verfügen über umfangreiche Erkennungsmöglichkeiten, doch Ihr Team arbeitet ad-hoc oder versagt dabei, den Kontext des Gefundenen zu berücksichtigen, indem es die vorliegenden Daten mit Informationen von außerhalb des Unternehmens korreliert. Außerdem werden Anfragen nicht nachverfolgt, die Leistung wird nicht gemessen, die Zusammenarbeit ist ad-hoc organisiert und gewonnene Erkenntnisse werden nicht gespeichert und für die Zukunft genutzt.

Phase 5: **Automatisierung und Orchestrierung**

Richten Sie konsistente, wiederholbare Security Operations ein.

Security Use Case Relevanz

Incident-Untersuchung & Forensik

Sicherheits-Monitoring

Erkennung komplexer Bedrohungen

SOC-Automatisierung

Incident Response

Compliance

Analyse und Erkennung von Betrugsversuchen

Insider-Bedrohungen

Beschreibung

Die Nutzung einer SOAR-Lösung (Security Orchestration, Automation and Response) ermöglicht es Unternehmen, Gefahren auf verschiedene Weise sehr effektiv zu reduzieren. Einige der Hauptvorteile beim Implementieren von Automatisierung und Orchestrierung sind die Möglichkeit, Ihre Gefahrenabwehr durch die Integration vorhandener Sicherheitstools und Quellen von Bedrohungsinformationen zu stärken, die Reaktion auf Sicherheitsevents zu beschleunigen, den Untersuchungsvorgang zu vereinfachen und den Schaden durch Angriffe zu minimieren. Erfahrene Unternehmen sind in der Lage, eingehende Warnmeldungen kontinuierlich automatisch einzustufen und zu priorisieren, so dass sich ihre Mitarbeiter auf die kritischsten und wichtigsten Probleme konzentrieren können. Erfahrene Unternehmen erlangen auch eine bessere Konsistenz und Wiederholbarkeit durch die Ausführung standardisierter Automatisierungs-Playbooks im Vergleich zur manuellen Ausführung eines Reaktionsplans.

Datenquellen

Zu den Datenquellen in dieser Phase gehören Events, die von Datenplattformen wie Splunk Enterprise generiert werden. Korrelationssuchen, relevante Events und andere präzisierte Events werden für weitere Maßnahmen von einem Automatisierungs- und Orchestrierungssystem aufgenommen.

Meilensteine

Die Meilensteine in Phase 5 umfassen den Erwerb folgender Fähigkeiten:

- Sie können jetzt Incidents nachverfolgen
- Die Effektivität von Sicherheitsanalysten kann regelmäßig gemessen werden
- Maßnahmen können auf Basis vordefinierter Playbooks ergriffen werden
- Sie können einfache Abwehraktionen automatisieren und sie in einer anspruchsvolleren Orchestrierung kombinieren

Herausforderungen

IT-Sicherheitsteams arbeiten normalerweise hart an vorderster Front und identifizieren, analysieren und entschärfen Bedrohungen wann und wo immer möglich. Doch trotz ihrer Bemühungen wächst der Rückstau von Sicherheits-Incidents mit der Zeit, die für aufwendige Untersuchungen und bereits bekannte Bedrohungen aufgewendet wird, weiter an. (Tatsächlich gibt es einfach nicht genügend geschulte Fachkräfte, um die Menge der Incidents zu analysieren, die in den meisten Unternehmen anfallen.)

Phase 6: **Komplexe Erkennung**

Wenden Sie komplexe Erkennungsmechanismen, einschließlich Machine Learning an.

Security Use Case Relevanz

Incident-Untersuchung & Forensik

Sicherheits-Monitoring

Erkennung komplexer Bedrohungen

SOC-Automatisierung

Incident Response

Compliance

Analyse und Erkennung von Betrugsversuchen

Insider-Bedrohungen

Beschreibung

Durch die Nutzung von Machine Learning, Data Science und komplexen Statistiken für die Analyse von Benutzern, Endgeräten und Anwendungen in Ihrer Umgebung sichern Sie sich eine reelle Chance, Gegner, unbekannte Bedrohungen und Insider Threats zu erkennen – selbst wenn sie nur feine Spuren ihrer Aktivitäten hinterlassen.

Datenquellen

Die Jagd auf Gegner erfordert eine detailliertere Datenerfassung an Ihren Endpunkten. Umfangreiche Endpunkt-Aktivitäten, die die Prozesserstellung, Dateiänderungen, Registrierungsänderungen und Netzwerkverbindungen erfassen, liefern eine erstaunlich klare Historie der kritischen Events, die an einem Endpunkt auftreten.

Zu den Quellen gehören:

- Microsoft Sysmon
- Osquery
- Carbon Black Defense

Meilensteine

In Phase 6 setzen Sie Folgendes ein:

- Die fortschrittlichsten verfügbaren Techniken, um unbekannte Bedrohungen zu identifizieren
- Neue Erkennungsmechanismen, sobald sie verfügbar sind, wobei Sie sowohl die Expertise Ihres Teams als auch Forschungseinrichtungen von außerhalb einbeziehen

Herausforderungen

An diesem Punkt besteht die Herausforderung darin, Ihre Sicherheitsorganisation ständig weiter zu verbessern und neue Kompetenzen zu erwerben. Ihr Team wird wahrscheinlich auch neue Recherchen durchführen müssen. Aber indem Sie dem Weg zur Sicherheit immer weiter folgen und ihre Fertigkeiten beständig ausbauen, haben Sie die Nase vorn. Sie werden zwar immer Angriffen ausgesetzt sein, haben sich aber in die beste Position gebracht, um viele häufige und weniger häufige Bedrohungen für moderne Unternehmen zu erkennen und zu verhindern.

Lösen häufiger Herausforderungen an die Sicherheit mit der Splunk Security Operations Suite

Die Reise zur Sicherheit kann ein ziemlich holpriger Weg sein. Wäre es nicht großartig, wenn Sie ein Handbuch mit den Herausforderungen hätten, denen Sie begegnen könnten, damit Sie, wenn sie auftreten, die Werkzeuge haben, um mit der Situation umzugehen und auf Kurs zu bleiben?

Keine Sorge! Wir haben an alles gedacht.

Hier stellen wir Ihnen einige Beispiele zur Verfügung, die Sie bei der Lösung von 16 häufigen Sicherheitsproblemen unterstützen (mehr dazu finden Sie in der **Splunk Security Essentials App** oder der **Splunk Security Online Demo**). Zu jedem Beispiel wird die jeweilige Herausforderung erklärt und Auskunft über Datenquellen, Use Cases, Splunk-Lösungen, die Schwierigkeit der Programmierung, die Implementierung, den Umfang an Benachrichtigungen, bekannte Fehlalarme und die beste Reaktion gegeben.

Zu diesen Beispielen gehören:

- **Incident-Untersuchung und Forensik**
  - Erkennen von Seitwärtsbewegung (Lateral Movement, d.h. ein Ausbreiten im internen Netz) mit WMI
  - Identifizierung mehrfacher nicht autorisierter Zugriffsversuche
- **Sicherheits-Monitoring**
  - Erkennen öffentlicher S3-Buckets in AWS
  - Auffinden von Mehrfachinfektionen auf Hosts
- **Erkennung komplexer Bedrohungen**
  - Erkennen von Verbindungen zu neuen Domänen
  - Finden von E-Mails mit Doppelgänger-Domänen
- **SOC-Automatisierung**
  - Automatisierung von Untersuchungen auf Malware
  - Automatisierung von Phishing-Untersuchungen
- **Incident Response**
  - Erkennen von Webdatenexfiltrations-DLP-Benachrichtigungen für Benutzer
  - Identifizieren von einfacher dynamischer DNS-Erkennung
- **Compliance**
  - Erkennen neuer lokaler Administratorkonten
  - Erkennen von Benutzern, die regelwidrig bei Systemen angemeldet sind, die Complianceregeln unterliegen
- **Analyse und Erkennung von Betrungsversuchen**
  - Erkennen beschädigter Benutzerkonten
  - Auffinden anomaler Dienstleister im Gesundheitswesen
- **Erkennung interner Bedrohungen**
  - Erkennung großer Webuploads
  - Erkennung der erfolgreichen Anmeldung mit dem Konto eines ehemaligen Mitarbeiters

Incident-Untersuchung und Forensik

Erkennen von Seitwärtsbewegung mit WMI

PHASE 3

MITRE ATT&CK-Taktiken

Seitwärtsbewegung (Lateral Movement) | Ausführung

MITRE ATT&CK-Techniken

Remote-Services | Windows Management Instrumentation

Datenquellen

Windows Security | Endpunkterkennung und -behandlung

Sicherheitsherausforderung
Windows Management Instrumentation (WMI) hat bei Angreifern an Beliebtheit gewonnen. Grund sind vor allem dessen Fähigkeiten zur Systemaufklärung, zum Virenschutz und zur Erkennung von virtuellen Maschinen, zur Ausführung von Code und zur Seitwärtsbewegung sowie zur Persistenz und zum Datendiebstahl.

Use Case
Erkennung komplexer Bedrohungen

Kategorie
Seitwärtsbewegung (Lateral Movement)

Erforderliche Splunk-Lösungen
Simple Search Assistant

SPL-Schwierigkeitsgrad
Einfach

Implementierung
Für diesen Use Case muss Sysmon auf den zu überwachenden Endpunkten und das Sysmon-Add-On auf Ihren Forwardern und Search Heads installiert sein.

Menge an Benachrichtigungen
Gering

Bekannte False Positives
Keine bekannten False Positives

Reaktion
Wenn diese Suche ausgelöst wird, sollten Sie Ihren Incident Response-Prozess einleiten und die von diesem Prozess ausgeführten Aktionen untersuchen.

Hilfe zum Erkennen von Seitwärtsbewegung (Lateral Movement) mit WMI
Zum Erkennen von Seitwärtsbewegung mit WMI laden wir zunächst unsere Sysmon-EDR-Daten. Alle anderen Prozessstartlogs mit vollständiger Befehlszeile genügen ebenfalls. Wir suchen nach allen Instanzen der Windows Management Instrumentation Befehlszeile (WMIC), die gestartet werden (EventCode 1 zeigt einen Prozessstart an), und filtern, um sicherzustellen, dass unsere verdächtigen Felder sich in der CommandLine-Zeichenfolge befinden.

```
index=* sourcetype=XmlWinEventLog:Microsoft-
Windows-sysmon/Operational EventCode=1 Image=*wmic*
CommandLine=*node* CommandLine="*process call
create*"
| table _time host Image CommandLine
```

Identifizierung mehrfacher nicht autorisierter Zugriffsversuche

PHASE 1

MITRE ATT&CK-Taktiken

Zugriff mit Anmeldeinformationen

MITRE ATT&CK-Techniken

Brute Force-Angriff

Datenquellen

Authentifizierung | Windows Security

Sicherheitsherausforderung
Die meisten Anmeldefehler sind auf falsche Kennwörter zurückzuführen. Allerdings können mehrere Anmeldefehler bei sensiblen Systemen, für die die Benutzer einfach nicht autorisiert sind, auf böswillige Absicht hinweisen. In den meisten Unternehmen kommt es selten vor, dass ein Benutzer eine Nachricht zu fehlender Autorisierung erhält, abgesehen von Szenarien mit geringem Risiko wie Proxy-Logs. Wenn dies bei Aktivitäten mit höherem Risiko auftritt, z. B. bei Systemanmeldungen, Dateifreigabezugriff usw., und wenn es dauerhaft für einen Benutzer auftritt, ist dies normalerweise ein Grund zur Untersuchung.

Use Case
Insider-Bedrohung

Kategorie
Insider-Bedrohung

Erforderliche Splunk-Lösungen
Simple Search Assistant

SPL-Schwierigkeitsgrad
Mittel

Implementierung
Stellen Sie sicher, dass die Daten, die vom Universal Forwarder und dem Splunk Technology-Add-On erfasst werden, verfügbar sind, dann funktioniert alles automatisch.

Menge an Benachrichtigungen
Gering

Bekannte False Positives
Das wahrscheinlichste Szenario, bei dem diese Erkennung ein False Positive anzeigt, bilden Fälle, in denen der Benutzerzugriff einfach fehlerhaft gehandhabt wurde. Beispielsweise wenn es in der vorherigen Nacht eine Änderung der AD-Gruppe gab, und der Benutzer versehentlich aus der Sicherheitsgruppe "dev_system_access" entfernt wurde. Darüber hinaus gibt es kein Standardmuster, das bei falsch positiven Ergebnissen zu erwarten wäre.

Reaktion
Wenn diese Benachrichtigung ausgelöst wird:

1. Überprüfen Sie, ob der Benutzer zuvor Zugriff auf die gewünschten Ressourcen hatte.
2. Achten Sie auf kürzlich vorgenommene Änderungen der Benutzerrollen.
3. Suchen Sie nach kürzlich erfolgten Änderungen im Bereich der AD-Gruppen.

In den meisten Organisationen wäre der nächste Eskalationsschritt, mit dem Besitzer der Ressourcen und/oder dem Vorgesetzten des Benutzers Verbindung aufzunehmen, um zu überprüfen, ob dieses Verhalten beabsichtigt ist. Achten Sie auf Anzeichen für böswillige Absichten und potenzielle Kontoverletzungen.

Hilfe zur Identifizierung mehrfacher nicht autorisierter Zugriffsversuche
Um mehrere unberechtigte Zugriffsversuche mithilfe von Echtzeitdaten zu finden, verwenden wir die einfache Suche und die unten dargestellte Suchsprache. Hier nutzen wir Windows-Sicherheitsprotokolle und suchen insbesondere nach dem Statuscode 0xC000015B, der anzeigt, dass dem Benutzer nicht der angeforderte Anmeldetyp gewährt wurde. Wir suchen nach allen Benutzern, für die dieser mehrfach am Tag aufgetreten ist, was auf den versuchten Zugriff auf sensible Ressourcen hinweisen kann. Der Screenshot unten zeigt die Ergebnisse einer Suche in Beispieldaten.

```
index=* source=win*security user=* EventCode=*
action=failure Logon_Type=* Failure Reason Logon
Type Status=0xC000015B
```

Sicherheits-Monitoring

Erkennen öffentlicher S3-Buckets in AWS

PHASE 3

Datenquellen

Audit-Trail AWS

Sicherheitsherausforderung
Es passiert immer wieder: Benutzer hosten Dateien zwecks schneller Übertragung in einem AWS S3-Bucket, vergessen aber, sie wieder herunter zu nehmen, oder verwenden S3-Buckets für die Sicherung vertraulicher Daten, machen aber versehentlich Fehler bei den Berechtigungen. Da falsch konfigurierte öffentliche S3-Buckets vertrauliche Daten ohne Not der Gefahr aussetzen offengelegt zu werden und einen häufigen Typ von Sicherheitsverletzung darstellen, ist es wichtig, zu erkennen, wenn neue oder vorhandene S3-Buckets als öffentlich festgelegt werden.

Use Cases
Sicherheits-Monitoring
Erkennung komplexer Bedrohungen

Kategorie
Datenexfiltration, SaaS

Erforderliche Splunk-Lösungen
Splunk Security Essentials
Splunk Add-On for Amazon Web Services
Splunk Simple Search Assistant

SPL-Schwierigkeitsgrad
Mittel

Implementierung
Die Suche nach öffentlichen S3-Buckets wird durch normalisierte Daten erleichtert, die dem Common Information Model zugeordnet werden. Das Splunk Add-On für Amazon Web Services ermöglicht Transparenz für verschiedene AWS-Servicekomponenten, einschließlich Events des CloudTrail-Service und von S3-Buckets. Unter der Voraussetzung, dass Sie das AWS Add-On für Splunk verwenden, um diese Logs einzulesen, sollte diese Suche automatisch und ohne Probleme funktionieren. Stellen Sie bei der Implementierung sicher, dass Sie der Best Practice zur Spezifizierung des Index für Ihre Daten folgen.

Menge an Benachrichtigungen
Sehr gering

Bekannte False Positives
Es gibt zwei Arten unerwünschter Benachrichtigungen, die bei dieser Suche vorkommen. Sie treten in folgenden Fällen auf:

1. Absichtliches Erstellen eines öffentlichen Buckets. Es kann sinnvoll sein, eine Whitelist mit Marketingmitarbeitern zu erstellen, die dies regelmäßig tun, oder eine Richtlinie für die Erstellung eines öffentlichen Buckets zu definieren, damit Sie absichtlich erstellte öffentliche Buckets bei der Suche ausschließen können.
2. Erstellen eines Buckets, der augenblicklich öffentlich ist, dann aber in den privaten Modus wechselt

Reaktion
Wenn diese Suche ausgelöst wird, sollten Sie Ihren Incident Response-Prozess einleiten und die von diesem Prozess ausgeführten Aktionen untersuchen.

Hilfe zum Erkennen von Seitwärtsbewegung (Lateral Movement) mit WMI
Zum Erkennen von Seitwärtsbewegung mit WMI laden wir zunächst

unsere Sysmon-EDR-Daten. Andere Logs, welche Prozessstarts mit vollständigem Kommandozeilenparametern beinhaten, genügen ebenfalls. Wir suchen nach allen Instanzen der Windows Management Instrumentation Befehlszeile (WMIC), die gestartet werden (EventCode 1 zeigt einen Prozessstart an), und filtern,
um sicherzustellen, dass unsere verdächtigen Felder sich in der CommandLine-Zeichenfolge befinden.

Reaktion

Wenn eine Benachrichtigung wegen eines öffentlichen S3-Buckets ausgelöst wird, sollten drei Fragen gestellt werden:

1. Ist der S3-Bucket immer noch öffentlich?
2. Sind die Dateien öffentlich?
3. Was befindet sich in dem Bucket?

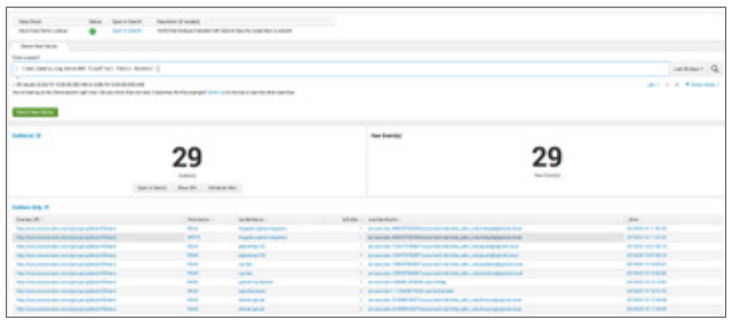
Die erste Frage lässt sich leicht beantworten: Sie suchen einfach in Ihren Logs nach dem Bucket-Namen und "PutBucketACL". Daraufhin können Sie alle nachfolgenden Änderungen an den ACLs sehen. Die Beantwortung der zweiten und dritten Frage ist etwas kniffliger und erfordert die Aktivierung der Serverzugriffsprotokollierung für den S3-Bucket (nicht standardmäßig aktiviert, außerdem ziemlich unpraktisch und daher kein Allheilmittel).

Falls Sie die AWS-Umgebung für Ihr Unternehmen nutzen, sollten Sie die Analyse aller offenen S3-Buckets priorisieren. Sie sollten sogar eventuell versuchen, die Behebung dieser Berechtigungslücken mittels AWS-Funktionen zu automatisieren.

Hilfe zum Erkennen öffentlicher S3-Buckets in AWS

Um mithilfe von Echtzeitdaten nach öffentlichen S3-Buckets zu suchen, verwenden wir die einfache Suche und die unten dargestellte Suchsprache. Die Echtzeitsuche arbeitet mit den AWS Cloudtrail-Logs und filtert nach den PutBucketAcl-Events, die bei der Änderung von Bucket-Berechtigungen auftreten, und nach allen Events, die AllUsers enthalten. Der Screenshot zeigt die Ergebnisse einer Suche in Beispieldaten.

```
index=* sourcetype=aws:cloudtrail AllUsers
eventName=PutBucketAcl
| spath output=userIdentityArn
path=userIdentity.arn
| spath output=bucketName
path="requestParameters.bucketName"
| spath output=aclControlList
path="requestParameters.AccessControlPolicy.
AccessControlList"
| spath input=aclControlList output=grantee
path=Grant{} | mvexpand grantee
| spath input=grantee
| search "Grantee.URI"=*AllUsers
| table _time, Permission, Grantee.URI,
bucketName, userIdentityArn | sort - _time
```



Auffinden von Mehrfachinfektionen auf Hosts

PHASE 1

MITRE ATT&CK-Taktiken

Erstzugriff (Initial Access) | Ausführung

MITRE ATT&CK-Techniken

Beiläufige Kompromittierung (Drive-by Compromise)

Anlage mit Malware (Spearphishing Attachment)

Link zu Malware (Spearphishing Link) | Ausführung durch Benutzer

Datenquellen

Virenschutz | Malwareschutz

Sicherheitsherausforderung
Viren kommen vor, aber mehrere Viren, die gleichzeitig auf einem einzelnen Host auftreten, sind ein größeres Problem. Derartige Vorgänge können ein Hinweis auf sowohl ein Exploit Kit sein, das verschiedene Verfahren ausprobiert, von denen einige erfolgreich sein können, als auch auf einen Host mit mehreren voneinander unabhängigen Viren. Herkömmliche Anti-Malware-Produkte können bei der Erkennung bekannter Malware effektiv sein, bei neuen oder sich gerade entwickelnden Malware-Typen können sie aber versagen. Da Malware-Varianten eine Hintertür zu internen Systemen bieten, langfristige Persistenz ermöglichen oder Daten ausfiltern können, sollten Sie die Untersuchung von mit Malware infizierten Hosts sofort priorisieren, um zu ermitteln, was möglicherweise außerdem unentdeckt geblieben ist.

Use Case
Sicherheits-Monitoring

Kategorie
Kompromittierung von Endpunkten

Erforderliche Splunk-Lösungen
Splunk Security Essentials
Splunk Common Information Model-Add-On
Splunk Simple Search Assistant

SPL-Schwierigkeitsgrad
Einfach

Implementierung
Für das Aufspüren von Hosts mit mehreren Infektionen ist das Sammeln der Logs einer Virenschutzlösung erforderlich. Wenn beispielsweise Symantec-Logs verfügbar sind, sollte diese Suche komfortabel funktionieren. Wenn Sie ein anderes Virenschutzprodukt verwenden, können Sie die Feldnamen und Quelltypen dieses Produkts leicht an die Suchkriterien anpassen – insbesondere, wenn Sie ein Splunk-Add-On verwenden, das sie auf das Common Information Model abbildet (suchen Sie auf **Splunkbase**).

Menge an Benachrichtigungen
Gering

Bekannte False Positives
Keine bekannten False Positives.

Reaktion
Wenn mehrere Infektionen auf demselben Host auftreten, sollte Ihr Reaktionsplan der gleiche wie für jedes Malware-Event sein, nur entsprechend dringlicher.

Hilfe zum Auffinden von Mehrfachinfektionen auf Hosts
Um Hosts mithilfe von Echtzeitdaten zu finden, für die in einem kurzen Zeitraum mehrere Infektionen protokolliert wurden, wird in unserem Beispiel die einfache Suche mit der unten dargestellten Suchsprache genutzt. Zunächst importieren wir unser Basis-Dataset, Symantec Endpoint Protection Risks, für die letzten 24 Stunden. Es gibt zwar verschiedene Ansätze, Events zu gruppieren ("stats" ist der schnellste), wir verwenden aber "transaction", weil es der einfachste Ansatz ist. Dadurch können wir alle Events nach "Computer_Name" gruppieren. Schließlich können wir danach filtern, ob es mindestens drei Events gibt, die sich zumindest über einige Minuten erstreckten. Der Screenshot unten zeigt die Ergebnisse einer Suche in Beispieldaten.

```
index=* sourcetype=symantec:* earliest=-24h
| transaction maxpause=1h Computer_Name
| where eventcount >=3 AND duration>240
```

Erkennung komplexer Bedrohungen

Erkennen von Verbindungen zu neuen Domänen

PHASE 2

MITRE ATT&CK-Taktiken

Exfiltration | Command & Control

MITRE ATT&CK-Techniken

Exfiltration über den Command-and-Control-Kanal

Exfiltration über alternatives Protokoll

Standard-Anwendungsschichtprotokoll

Datenquellen

Web-Proxy | NGFW

Sicherheitsherausforderung

In den meisten Organisationen decken sich die Domänen, die Benutzer heute besuchen, sehr stark mit denen, die sie gestern besucht haben. Aber was ist mit dem kleinen Prozentsatz an Domänen, die heute von Ihrem Netzwerk angefordert wurden, aber bisher keine Ziele Ihrer Systeme waren? Natürlich wird es heute legitimen Datenverkehr zu einigen wenigen Domänen geben, die noch nie im Netzwerk aufgetreten sind, aber gemessen an der Gesamtmenge der besuchten Domänen wird das wohl nur ein kleiner Prozentsatz sein. Der Rest dieser neuen, noch nie aufgetretenen Domänen stellt eine potenzielle Bedrohung dar.

Das Wissen darum, wann Benutzer zu neuen Domänen surfen, kann in verschiedenen Szenarien relevant sein, vor allem aber dann, wenn Ihr System eine Verbindung mit einer von Angreifern gesteuerten Domäne herstellt, die als Hub für Command & Control-Kommunikation dient oder einen Staging-Server für Datenexfiltration oder die Bereitstellung von Malware betreibt. Wenn Sie vermuten, dass ein Host infiziert ist, sollten Sie unbedingt überprüfen, ob er neue Domänen besucht hat.

Use Case

Erkennung komplexer Bedrohungen

Kategorie

Command & Control, Datenexfiltration

Erforderliche Splunk-Lösungen

Splunk Enterprise

Splunk Security Essentials

Splunk URL Toolbox

Splunk Simple Search Assistant

SPL-Schwierigkeitsgrad

Mittel

Implementierung

Bei dieser Methode der Anomalieerkennung werden der früheste und der späteste Zeitpunkt für das Auftreten einer beliebigen Wertemenge nachverfolgt (z. B. die Kombination aus der ersten Anmeldung je Benutzer + Server oder die Kombination aus dem ersten Anzeigeaufruf gemäß Code-Repository + Benutzer oder der ersten Windows-Ereignis-ID je System, die auf die Verwendung eines USB-Sticks hinweist). Bei normalem Gebrauch würden Sie prüfen, ob der aktuellste Wert innerhalb der letzten 24 Stunden liegt, und in diesem Fall eine Benachrichtigung auslösen. Dies ist eine wichtige Funktion vieler der angebotenen sicherheitsbezogenen Data Science-Tools (nicht jedoch von Splunk UBA), die Sie problemlos mit Splunk Enterprise einsetzen können.

Die Implementierung dieser Suche ist relativ einfach, da sie CIM-konforme Daten erwartet. Integrieren Sie zunächst Ihre Proxy-Daten (oder sonstige Webbrowsing-Sichtbarkeitsdaten wie stream:http oder bro), und stellen Sie sicher, dass ein URI-Feld vorhanden ist. Als einzigen weiteren Schritt stellen Sie sicher, dass die URL Toolbox-App installiert ist, die es Splunk ermöglicht, die Domänen zu extrahieren. Beim Skalieren dieser Suche auf größere Datenmengen (oder häufigere Ausführungen) empfehlen wir, Beschleunigungsfunktionen zu nutzen.

Menge an Benachrichtigungen

Sehr groß

Bekannte False Positives

In den meisten Organisationen ist der Prozentsatz neuer Domänen klein. Wenn Sie jedoch alle diese Warnungen zur Untersuchung an die Analysten schicken würden, wäre das eine völlige Überforderung, da die Mehrheit der "new domain"-Warnmeldungen durch legitimen Datenverkehr ausgelöst wird. Zwar gibt es keine bekannten False Positives, der Wert jeder einzelnen Warnmeldung zu neuen Domänen ist jedoch so klein, dass es sinnvoll ist, diese Benachrichtigungen anders als die meisten Korrelationssuchen zu behandeln. Diese eigenen sich besonders für kontextbezogene Daten oder für die Korrelation mit anderen Indikatoren.

Reaktion

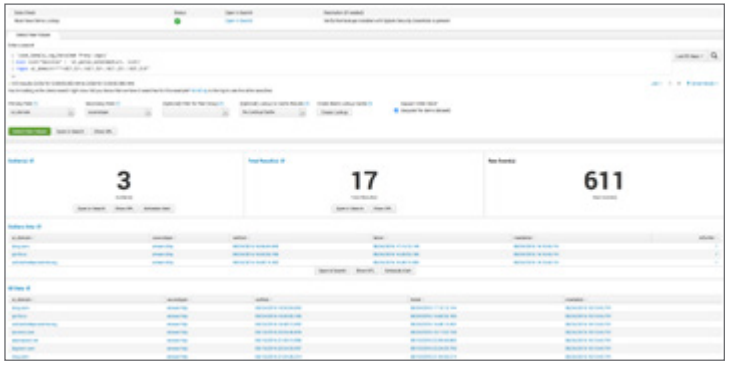
Diese "new domain"-Events werden im allgemein am besten als Kontextdaten für ein anderes Event betrachtet, z. B. nicht bereinigte Malware, neue Services oder ungewöhnliche Anmeldungen. Der einfachste Weg zu einer solchen Korrelation besteht darin, die Events in einem Zusammenfassungsindex aufzuzeichnen und dann die Suche in diesem Index in Ihre Untersuchungsaktionen einzuschließen. Kunden von Splunk Enterprise Security können dies komfortabel mit dem Risikomanagement-Framework erledigen. Durch Erstellen einer adaptiven Abwehrreaktion für den Risikoindikator beim Speichern dieser Suche wird dann die Risikoeinstufung der beteiligten Assets angepasst und beim Analysieren eines Assets in der Untersuchungs-Workbench angezeigt. Um die Wirksamkeit einer bestimmten Benachrichtigung in diesem Zusammenhang letztendlich zu analysieren, empfehlen wir, die Domänen in einer Quelle für Open Source Intelligence wie VirusTotal oder ThreatCrowd nachzuschlagen.

Hilfe zum Erkennen von Verbindungen zu neuen Domänen

Um mithilfe von Echtzeitdaten nach Verbindungen zu neuen Domänen zu suchen, verwenden wir die einfache Suche und die unten dargestellte Suchsprache. Zunächst bringen wir unser Proxy-Dataset ein, wobei wir Felder des Common Information Models nutzen und nur nach Events filtern, für die ein URI vorliegt.

Im nächsten Schritt verwenden wir URL Toolbox, um die Domäne aus der URL zu extrahieren. Schließlich schließen wir IP-Adressen mithilfe des Regex-Filterbefehls aus der Suche aus. Zwar ist dies ein optionaler Schritt, wir haben aber festgestellt, dass das Verhältnis von relevanten zu irrelevanten Daten beim Einbeziehen von IP-Adressen ziemlich hoch sein kann, da einige Anwendungen im normalen Betrieb Verbindungen mit vielen IPs von kurzlebigen AWS-Instanzen herstellen. Schließlich verwenden wir den stats-Befehl, um zu berechnen, wann diese Kombination von Feldern zuerst und zuletzt aufgetreten ist, und zu überprüfen, ob der früheste Zeitpunkt, zu dem dieses Event aufgetreten ist, innerhalb des letzten Tags lag (also brandneu ist). Der Screenshot unten zeigt die Ergebnisse einer Suche in Beispieldaten.

```
tag=web url=*
| eval list="mozilla" | `ut_parse_
extended(url,list)`
| regex ut_domain!="^\d{1,3}\.\d{1,3}\.\
d{1,3}\.\d{1,3}$"
| stats earliest(_time) as earliest latest(_
time) as latest by ut_domain, sourcetype
| where earliest >= relative_time(now(),
"-1d@d")
```



Finden von E-Mails mit Doppelgänger-Domänen

PHASE 4

MITRE ATT&CK-Taktiken

Erstzugriff (Initial Access)

MITRE ATT&CK-Techniken

Link zu Malware (Spearphishing Link)

Datenquellen

E-Mail

Sicherheitsherausforderung
E-Mails mit Doppelgänger-Domänen stellen eine gängige Phishing-Taktik dar. Einige Angreifer vertauschen leicht zu verwechselnde Buchstaben, etwa wenn splunk.com eine E-Mail von spiunk.com erhält. Oder sie nutzen eine glaubhafte Unterdomäne (beispielsweise .help.com, .support usw.) Das Problem ist hier, dass Menschen eine E-Mail mit größerer Wahrscheinlichkeit öffnen, wenn sie glauben, dass sie von einer legitimen Quelle stammt. Bei der gefälschten E-Mail ist der Unterschied kaum wahrnehmbar.

Use Case
Erkennung komplexer Bedrohungen

Kategorie
Endpunkt-Kompromittierung, SaaS

Erforderliche Splunk-Lösungen
Splunk Search Assistant

First Time Seen Assistant

URL Toolbox-App

SPL-Schwierigkeitsgrad
Fortgeschritten

Implementierung
Die Implementierung dieser Suche ist in der Regel ziemlich einfach. Wenn Sie CIM-konforme Daten integriert haben, sollte diese Suche ohne weitere Konfiguration funktionieren. Es ist jedoch immer besser, den Index und Quelltyp Ihrer E-Mail-Daten anzugeben – besonders dann, wenn Sie mehrere Quellen für E-Mail-Logs haben, wie z. B. eine Mail-Sicherheitsanwendung am Umkreisnetzwerk und eine Exchange-Umgebung im Kern. Es sollte problemlos funktionieren, wenn Sie die URL Toolbox installiert haben und die richtigen Felder für index, sourcetype und src_user verwenden.

Menge an Benachrichtigungen
Sehr gering

Bekannte False Positives
Diese Suche durchsucht eingehende E-Mails nach Domänen, die den normalerweise von Ihrem Unternehmen angeforderten Domänen ähnlich sind, fast wie bei der Ausführung von dnstwist für einen Domänennamen. Wenn es eingehende E-Mails gibt, deren Quelldomänen ähnliche – aber nicht die gleichen – Namen wie die auf täglicher Basis auftretenden Domänen haben, ist es möglich, dass die Suche falsch positive Benachrichtigungen generiert. Nehmen wir an, ein Unternehmen, das Holzplanken für Piratenschiffe herstellt – plank.com – sendet eine E-Mail an seine Vertriebsmitarbeiter unter splunk.com. Dies wäre eine Levenshtein-Distanz von zwei (aus dem "a" in plank wird ein "u", und wir haben ein zusätzliches "s"), und würde gemeldet werden (zu schade...). Um die Anzahl der Fehlbenachrichtigungen zu verringern, könnten Sie bekannte Beispiele aus der Suche herausfiltern oder die Ergebnisse in eine First Time Seen-Erkennung weiterleiten, um frühere Beispiele automatisch zu entfernen.

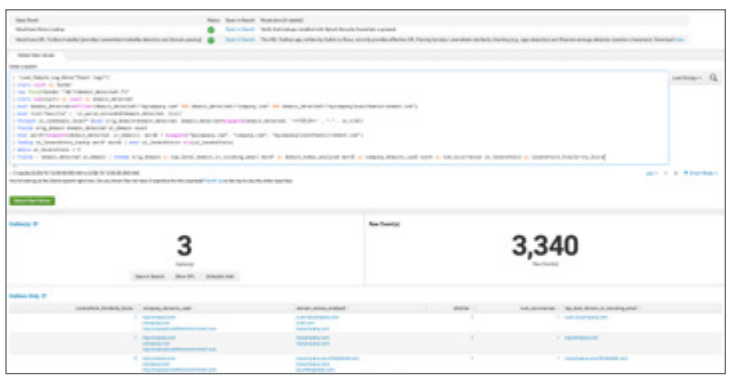
Reaktion

Wenn diese Suche Werte zurückgibt, lösen Sie Ihren Incident Response-Prozess aus und erfassen die Zeit des Events, den Absender, den Empfänger, den Betreff der E-Mail und etwaige Anhänge. Kontaktieren Sie den Absender. Ist das Verhalten autorisiert, dokumentieren Sie, dass dies autorisiert ist und von wem. Bei nicht autorisiertem Verhalten wurden die Benutzeranmeldeinformationen vielleicht von einer anderen Person verwendet, und es sollte eine weitere Untersuchung durchgeführt werden.

Hilfe zum Finden von E-Mails mit Doppelgänger-Domänen

Um mithilfe von Echtzeitdaten E-Mails mit Doppelgänger-Domänen zu finden, verwenden wir den Assistenten für die einfache Suche, URL Toolbox und die unten dargestellte Suchsprache. Wir beginnen, indem wir E-Mail-Logs abrufen, die uns eine Quelladresse liefern, und aggregieren nach der Quelladresse. Als Nächstes extrahieren wird die Domäne und aggregieren nach tatsächlicher Domäne, die wir analysieren werden. Wir filtern außerdem alle Domänen heraus, die wir besitzen und von denen wir E-Mails zu erhalten erwarten. Mithilfe der kostenlosen URL Toolbox-App extrahieren wir Unterdomänen aus den Top-Level-Domänen. Da es sich bei dem Feld, das wir an den Levenshtein-Algorithmus übergeben, um domain_detected handelt, fügen wir dem mehrwertigen Feld domain_detected jede Unterdomäne hinzu. URL Toolbox werden zwei mehrwertige Felder übergeben, und es führt die Gegenprüfung durch, um den Levenshtein-Wert für jede Kombination zu berechnen. Wir ziehen den niedrigsten Punktwert aus dieser Gruppe heraus. Schließlich filtern wir nach Levenshtein-Punktzahlen von weniger als drei. Der Screenshot unten zeigt die Ergebnisse einer Suche in Beispieldaten.

```
index=* sourcetype=cisco:esa* OR
sourcetype=ms:o365:*:messagetrace OR
sourcetype=MSExchange*:MessageTracking OR tag=email
src_user=*
| stats count by src_user
| rex field=src_user "\@(?.*)"
| stats sum(count) as count by domain_detected
| eval domain_detected=mvfilter(domain_
detected!="mycompany.com" AND domain_
detected!="company.com" AND domain_
detected!="mycompanylovestheenvironment.com")
| eval list="mozilla" | `ut_parse_
extended(domain_detected, list)`
| foreach ut_subdomain_level* [eval
orig_domain=domain_detected, domain_
detected=mvappend(domain_detected, '<>' . "." .
ut_tld)]
| fields orig_domain domain_detected ut_domain
count
| eval word1=mvappend(domain_detected, ut_
domain), word2 = mvappend("mycompany.com",
"company.com", "mycompanylovestheenvironment.
com")
| lookup ut_levenshtein_lookup word1 word2 |
eval ut_levenshtein= min(ut_levenshtein)
| where ut_levenshtein < 3
| fields - domain_detected ut_domain | rename
orig_domain as top_level_domain_in_incoming_
email word1 as domain_names_analyzed word2 as
company_domains_used count as num_occurrences
ut_levenshtein as Levenshtein_Similarity_Score
```



SOC-Automatisierung

Automatisierung von Untersuchungen auf Malware

PHASE 5

Datenquellen

Authentifizierung | Windows Security

Sicherheitsherausforderung

Wenn die gleiche Malware auf mehreren Systemen auftritt, befinden Sie sich möglicherweise kurz vor einem größeren Sicherheits-Incident (dies ist häufig bei Würmern, Ransomware und breit angelegten Phishing-Kampagnen zu beobachten). Das Untersuchen von und Reagieren auf Malware-Benachrichtigungen kann jeweils 30 Minuten oder länger dauern. Durch die Automatisierung dieser Untersuchung und Reaktion liefert Splunk Phantom die Bestätigung, dass der Prozess bösartig ist, und ergreift sofort Maßnahmen, um den Hash an den infizierten Endpunkten zu blockieren.

Use Cases

Sicherheits-Monitoring

Erkennung komplexer Bedrohungen

SOC-Automatisierung

Kategorie

Endpunkt-Kompromittierung, Seitwärtsbewegung (Lateral Movement)

Erforderliche Splunk-Lösungen

Splunk Phantom

SPL-Schwierigkeitsgrad

Nicht zutreffend

Implementierung

Lesen Sie Malware-Events aus Ihrer Datenquelle in Ihre SOAR-Plattform ein. Führen Sie Untersuchungsaktionen durch, wie etwa das Abrufen von Reputationsinformationen zu in Frage kommenden IPs, URLs und Dateien, um schneller Entscheidungen treffen zu können. Diese Aktionen zur Kontextsammlung sind hervorragende Kandidaten für eine Automatisierung. Führen Sie abhängig von Ihren Entscheidungen Eindämmungs- und/oder Lösungsschritte aus, entweder manuell oder mit Hilfe von Automation Playbooks.

Menge an Benachrichtigungen

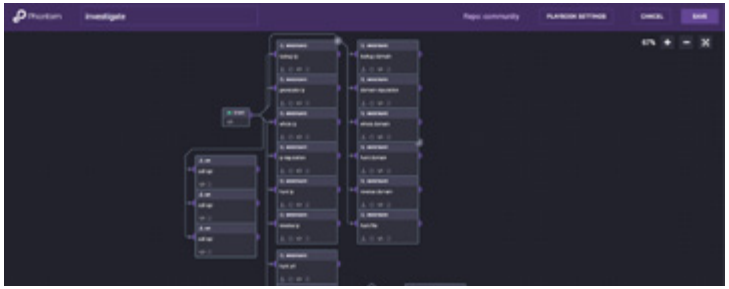
Sehr gering

Bekannte False Positives

Nicht zutreffend

Reaktion

Das Playbook untersucht Malware-Infektionen am Endpunkt und beseitigt sie. Indem Sie diese Reaktionen automatisieren, gewinnen Sie Zeit, da Sie sich nicht mehr selbst darum kümmern müssen. Es werden außerdem mehr Sofortmaßnahmen ergriffen, um infizierte Endpunkte zu blockieren. Sie beginnen, die Ermittlungen und Entdeckungen im Zusammenhang mit Use Cases zu automatisieren, wie etwa beim Verbergen von Dateien und Verzeichnissen, der Erstellung von Shim-Datenbankdateien, dem Ausführen einer Datei mit mehreren Dateierweiterungen, Prozessen mit nur einem Buchstaben an einem Endpunkt und mehr.



Hilfe zur Kontextveredelung von Benachrichtigungen

Automatisieren von Phishing-Untersuchungen und -Reaktionen

PHASE 5

Datenquellen

Audit-Trail | AWS

Sicherheitsherausforderung

Phishing-E-Mails können für ein Unternehmen schädlich sein, wenn sie nicht erkannt werden. Die Untersuchung jeder einzelnen E-Mail kann zeitaufwendig sein, da ein Analyst möglicherweise den Inhalt des E-Mail-Textes, aber auch die Anhänge sowie alle Benutzer überprüfen muss, die die E-Mail erhalten haben. Durch die Automatisierung der Untersuchung können Analysten viel schneller auf diese Angriffe reagieren.

Use Cases

Sicherheits-Monitoring

Erkennung komplexer Bedrohungen

SOC-Automatisierung

Kategorie

Phishing, gegnerische Taktiken, Kontenkompromittierung

Erforderliche Splunk-Lösungen

Splunk Phantom

SPL-Schwierigkeitsgrad

Nicht zutreffend

Implementierung

Nehmen Sie verdächtige E-Mails in die SOAR-Plattform auf. Führen Sie Ermittlungsaktionen durch, wie etwa das Abrufen von Reputationsinformationen zu in Frage kommenden IPs, URLs , und Dateien, um schneller Entscheidungen treffen zu können. Diese Aktionen zur Kontextsammlung eignen sich hervorragend für eine Automatisierung. Ergreifen Sie ausgehend von Ihren Entscheidungen Maßnahmen, um mithilfe eines Automation Playbooks alle Kopien der Phishing-E-Mail aus Ihrem Mailsystem zu löschen.

Menge an Benachrichtigungen

Sehr gering

Bekannte False Positives

Nicht zutreffend

Reaktion

Die Implementierung und Automatisierung der richtigen Untersuchungen beim Erstellen eines Playbooks gibt Ihnen die Möglichkeit, das Ausmaß der für die Durchführung von Maßnahmen erforderlichen menschlichen Reaktion zu begrenzen – die im Playbook implementierte Reaktion trägt dazu bei, Phishinguntersuchungen zu rationalisieren, so dass die Behebung und Gegenmaßnahmen schneller möglich sind.

Automatisierung von Phishing-Untersuchungen

Incident Response

Erkennen von neuen Exfiltrations-DLP-Benachrichtigungen für Benutzer

PHASE 3

MITRE ATT&CK-Taktiken

Exfiltration

MITRE ATT&CK-Techniken

Exfiltration

Datenquellen

DLP

Sicherheitsherausforderung

Wenn ein Benutzer, der normalerweise keine DLP-Datenexfiltrations-benachrichtigungen generiert, plötzlich damit anfängt, hat das höhere Relevanz als eine herkömmliche Benachrichtigung. Bei wichtigen Regeln oder Benutzern mit umfangreichen Rechten sollten Sie diese Events untersuchen, um zu bestimmen, ob vertrauliche Unternehmensinformationen aus dem Unternehmen gelangen.

Use Case

Insider-Bedrohung

Kategorie

Insider-Bedrohung

Erforderliche Splunk-Lösungen

Simple Search Assistant

SPL-Schwierigkeitsgrad

Mittel

Implementierung

Die Implementierung dieser Regel ist einfach – die einzige Voraussetzung ist die Fähigkeit zur Erfassung, welche DLP-Benachrichtigungen Datenexfiltration darstellen. Diese Nomenklatur oder Konfiguration kann von einer Organisation zur anderen stark variieren, hier ist also Koordination mit Ihrem DLP-Team erforderlich. Davon abgesehen wird die Suche funktionieren, sofern Sie über ein definiertes Benutzerfeld und ein Signaturfeld verfügen.

Menge an Benachrichtigungen

Hoch

Bekannte False Positives

Da es sich um eine rein verhaltensbasierte Suche handelt, ist die Definition von "False Positive" hier etwas anders. Jede Auslösung dieser Benachrichtigung gibt das erste Vorkommen im durchsuchten Zeitraum genau wieder (oder bei Verwendung der Nachschlage-Cache-Funktion das erste Vorkommen im Zeitraum, für den die Suche erstellt wurde). Aber während es keine "False Positives" im herkömmlichen Sinn gibt, gib es fraglos eine ganze Menge „Rauschen“.

Reaktion

Da es sich um eine Verhaltensbenachrichtigung handelt, sollten Sie diese im Allgemeinen nicht isoliert verwenden, es sei denn:

- Der Schweregrad der Benachrichtigung oder die Priorität des Benutzers machen zweifelsfrei deutlich, dass der Vorfall so kritisch ist, dass er isoliert betrachtet werden muss, oder
- Ihre DLP ist so sorgfältig abgestimmt, dass Benachrichtigungen selten vorkommen.

In allen anderen Szenarien sollten die meisten Benachrichtigungen nur in Kombination mit anderen Benachrichtigungen berücksichtigt werden, unter Nutzung eines Verfahrens zur Zusammenfassung von Gefahren in Splunk ES oder der Bedrohungsmodelle in Splunk UBA.

Hilfe zum Erkennen von neuen Exfiltrations-DLP-Benachrichtigungen für Benutzer

In diesem Beispiel wird der Assistent für die einfache Suche (Simple Search Assistant) verwendet. Unser Dataset ist ein Basis-Dataset aus DLP-Events. Im Rahmen dieser Analyse filtern wir nach Datenexfiltrations-Benachrichtigungen. Der Screenshot unten zeigt die Ergebnisse einer Suche in Beispieldaten.

```
index=* tag=dlp tag=incident
| stats earliest(_time) as earliest latest(_time)
as latest by user, signature
| where earliest >= relative_time(now(), "-1d@d")
```

Identifizieren von einfacher dynamischer DNS-Erkennung

PHASE 1

MITRE ATT&CK-Taktiken

Command & Control | Adversary OPSEC | Aufbau und Wartung von Infrastruktur

MITRE ATT&CK-Techniken

Dynamische DNS | Standard-Anwendungsschichtprotokoll

Datenquellen

Web-Proxy | NGFW | DNS

Sicherheitsherausforderung

Angreifer wünschen sich Flexibilität in ihren Befehls- und Steuerungsfähigkeiten, und dynamische DNS kann diese Flexibilität bieten. Es gibt zwar legitime Nutzungen von dynamischer DNS (viele IT-Fachleute nutzen sie für den Zugriff auf Heimnetzwerke), aber die Gefahren durch mangelnde Überwachung davon können erheblich sein. Glücklicherweise ist es mithilfe von Splunk und einer von Malware Domains bereitgestellten Liste einfach, dynamische DNS in Ihrer Umgebung zu finden.

Use Cases

Sicherheits-Monitoring, Erkennung komplexer Bedrohungen

Kategorie

Command & Control

Erforderliche Splunk-Lösungen
Simple Search Assistant
URL Toolbox

SPL-Schwierigkeitsgrad
Einfach

Implementierung
Der erste Schritt bei der Implementierung dieser Erkennung besteht im Abrufen einer Liste mit dyndns-Anbietern. Nach dem Herunterladen müssen Sie die Liste so formatieren, dass sie mit dem Splunk-Nachschlageformat übereinstimmt. Sobald Ihnen diese Datei zur Verfügung steht, sollte der Rest reibungslos ablaufen.

Menge an Benachrichtigungen
Mittel

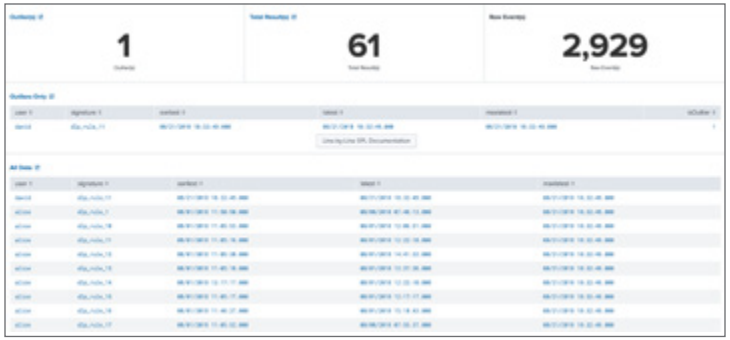
Bekannte False Positives
Es ist zwar selten, aber es kommt vor, dass in der Produktion genutzte Services dynamische DNS verwenden. Diese werden ein gewisses Grundrauschen an False Positives verursachen – allerdings sollte es sich hier nie um geschäftskritische Services handeln. Das häufigste Szenario für dynamische DNS bilden Benutzer, die ihre Hunde zu Hause über eine Webcam beaufsichtigen – oder ähnliche Vorkommnisse. Ob Sie dieses Benutzerverhalten erlauben – und entsprechend ausblenden – oder es untersagen, ist letztlich eine Frage Ihrer Firmen-Policy.

Reaktion
Wenn diese Benachrichtigung ausgelöst wird, sehen Sie sich die normalerweise zulässigen Szenarien an, insbesondere die Fälle von Benutzern, die auf ihr Heimnetzwerk zugreifen. Wenn dies nicht der Fall zu sein scheint:

1. Ziehen Sie Daten von Splunk Stream oder von Ihrer Paketerfassung zu Rate, um zu bestimmen, welche Art von Daten gesendet wurden
2. Überprüfen Sie den DNS-Namen und die IP-Adresse in Open-Source-Informationen, um nachzuprüfen, ob es etwas Auffälliges gibt (allerdings ist das für dieses Szenario oftmals schwierig).
3. Wenn es sich um einen kritischen Host handelt, sollten Sie Endpoint-Logging über Microsoft Sysmon oder andere Endpunkt-Reaktionsmechanismen in Betracht ziehen, um den Prozess zu identifizieren, der diese Verbindungen herstellt.

Hilfe zur Identifizierung einfacher dynamischer DNS-Erkennung
In diesem Beispiel werden die einfache Suche (simple search) und die unten dargestellte Suchsprache verwendet, um ausgehende Kommunikation an Server mit dynamischer DNS mithilfe von Echtzeitdaten zu erkennen. Zuerst bringen wir unser Dataset aus Proxylogs ein. Zum Aufspüren von Anbietern dynamischer DNS trennen wir mithilfe von URL Toolbox Unterdomänen von der registrierten Domäne. Im nächsten Schritt können wir unsere Nachschlagefunktion (lookup) für ddns-Domänen verwenden. Dadurch wird für alle Treffer ein Feld mit dem Namen "inlist" und dem Wert "true" hinzugefügt. Schließlich können wir nach den übereinstimmenden Einträgen suchen. Der Screenshot unten zeigt die Ergebnisse einer Suche in Beispieldaten.

```
index=* sourcetype=pan:threat OR (tag=web
tag=proxy) earliest=-20m@m earliest=-5m@m
| eval list="mozilla" | `ut_parse_
extended(url,list)`
| lookup dynamic_dns_lookup domain as ut_domain
OUTPUT inlist
| search inlist=true
| table _time ut_domain inlist bytes* uri
```



Compliance

Erkennen von neuen Exfiltrations-DLP-Benachrichtigungen für Benutzer

PHASE 1

MITRE ATT&CK-Taktiken

Umgehung von Abwehrmaßnahmen | Persistenz

MITRE ATT&CK-Techniken

Gültige Konten | Konto erstellen

Datenquellen

Audit-Trail | Windows Security

Sicherheitsherausforderung

Lokale Administratorkonten werden von zulässigen Technikern verwendet, aber sie stellen auch den Heiligen Gral für Angreifer dar. Sobald ein Angreifer in das Netzwerk gelangt, wird er oder sie höchstwahrscheinlich versuchen, in den Besitz von Administratorrechten zu gelangen, um sich unerkannt und ungehindert Zugriff auf die gewünschten Konten und Assets zu verschaffen. Eine einfache Möglichkeit dazu besteht darin, ein bestehendes Konto zu kompromittieren und dann die Benutzerrechte heraufzustufen.

Use Cases

Erkennung komplexer Bedrohungen, Sicherheits-Monitoring, Compliance

Kategorie

Kompromittierung von Endpunkten

Erforderliche Splunk-Lösungen

Splunk Security Essentials
Splunk Enterprise

SPL-Schwierigkeitsgrad

Mittel

Implementierung

Stellen Sie zunächst sicher, dass Sie Windows-Sicherheitsprotokolle empfangen und die Kontoänderungsüberwachung implementiert ist. Hilfe dazu finden Sie in der Dokumentation zu Datenquellen von Windows Security.

Sobald Sie Logs empfangen, sollten Sie nach “sourcetype=”WinEventLog:Security” EventCode=4720 OR EventCode=4732” suchen können, um Events zur Kontoerstellung oder Kontoänderung anzuzeigen. Stellen Sie abschließend sicher, dass Ihr lokaler Admin-Gruppenname "Administrators" lautet, damit Sie nach Änderungen bei der richtigen Gruppenzugehörigkeit suchen.

Menge an Benachrichtigungen

Mittel

Bekannte False Positives

Die einzige wirkliche Quelle für False Positives für diese Suche wären Help Desk-Administratoren, die lokale Administratorkonten erstellen. Wenn dies in Ihrer Umgebung üblich ist, sollten Sie ihre Nachrichten zur Erstellung von Administratorkonten herausfiltern, indem Sie ihre Benutzernamen von der Basissuche ausschließen. Enthält Ihre lokale Administratorgruppe den Begriff "Administrators" nicht, werden eventuell False Negatives erzeugt.

Reaktion

Wenn diese Suche Werte zurückgibt, leiten Sie Ihren Incident Response-Prozess ein, und erfassen Sie folgende Informationen:

- Name des neuen Kontos
- Zeitpunkt der Erstellung
- Benutzerkonten, von denen das Konto erstellt wurde
- System, das die Anfrage ausgelöst hat
- Alle sonstigen sachbezogenen Informationen

Kontaktieren Sie den Besitzer des Systems. Wenn es sich bei dem Event um autorisiertes Verhalten handelt, dokumentieren Sie dies, und auch von wem es autorisiert wurde. Bei nicht autorisiertem Verhalten wurden die Benutzeranmeldeinformationen vielleicht von einer anderen Person verwendet, und es sollte eine weitere Untersuchung durchgeführt werden. Zusätzlich zu dieser Untersuchung ist jetzt ein guter Zeitpunkt, um sicherzustellen, dass die legitimen Administratorkonten die zugewiesenen Berechtigungen wirklich benötigen und durch komplexe und lange Kennwörter geschützt sind.

Hilfe zum Erkennen neuer lokaler Administratorkonten

In diesem Beispiel werden die einfache Suche (simple search) und die unten dargestellte Suchsprache verwendet, um nach neu erstellten Konten zu suchen, die auf den Status eines lokalen Administrators heraufgestuft wurden. Unser Dataset ist eine Sammlung aus Windows Security-Logs mit Events zur Kontoerstellung oder mit Kontoänderungs-Events mit Gruppenmitgliedschaft. Der Screenshot unten zeigt die Ergebnisse einer Suche in Beispieldaten.

```
index=* source="winEventLog:Security"
EventCode=4720 OR (EventCode=4732 Administrators)
| transaction Security_ID maxspan=180m
| search EventCode=4720 (EventCode=4732
Administrators)
| table _time EventCode Account_Name Target_
Account_Name Message
```

Erkennen von Benutzern, die regelwidrig bei Systemen angemeldet sind, die Compliance-Regeln unterliegen

PHASE 4

MITRE ATT&CK-Taktiken

Zugriff mit Anmeldeinformationen | Erfassung | Rechteausweitung (Privilege Escalation)

MITRE ATT&CK-Techniken

Gültige Konten | Daten aus Informations-Repositories | Kontomanipulation

Datenquellen

Authentifizierung | Windows Security

Sicherheitsherausforderung

Gemäß der Datenschutz-Grundverordnung (DSGVO) sind Unternehmen verpflichtet, einen vollständigen Audit Trail über den autorisierten Zugriff von Mitarbeitern, Dienstleistern und/oder Datenverwertern auf Systeme und Anwendungen zu führen, die personenbezogene Daten verarbeiten. Die DSGVO räumt einzelnen Bürgern der Europäischen Union und des Europäischen Wirtschaftsraums das Recht ein, bei einer Organisation anzufragen, wo ihre Daten gespeichert sind und welche Stellen auf die Daten zugreifen.

Um eine solche Anfrage zu beantworten, muss ein Unternehmen feststellen, welche Mitarbeiter, Dienstleister und Datenverwerter auf die jeweiligen persönlichen Daten zugegriffen haben; und es muss ferner feststellen und darüber berichten, welche sonstigen Services diese Daten regelmäßig verarbeiten. Wenn Daten im Auftrag eines Datenverantwortlichen verarbeitet werden, besteht außerdem die Notwendigkeit zu belegen, dass nur autorisierte Personen auf die betreffenden Daten zugegriffen haben. Wenn es einen Audit Trail gibt, der einen unberechtigten Zugriff zeigt, muss dies dokumentiert und den Datenschutzbehörden gemeldet werden.

Durch die Verwendung einer Datenzuordnung, die durch zusätzliche Kontrollen zur Erkennung von Verstößen verstärkt wird, kann ein Unternehmen identifizieren:

- welche Mitarbeiter, Dienstleister und Datenverwerter auf die Daten zugegriffen haben
- wo die Daten gespeichert sind
- welche sonstigen Services die Daten regelmäßig verarbeiten.

Wenn Sie Daten im Namen eines Datenverantwortlichen verarbeiten, kann mit dieser Suche nachgewiesen werden, dass nur autorisierte Personen auf die Daten zugegriffen haben.

Use Cases
Interne Bedrohung, Compliance

Kategorie
DSGVO, IAM-Analysen, Seitwärtsbewegung (Lateral Movement), Operations

Erforderliche Splunk-Lösungen
Splunk Enterprise

SPL-Schwierigkeitsgrad
Einfach

Implementierung
Erstellen Sie zunächst mit den Ergebnissen Ihrer Datenzuordnung ein Lookup, das Systeme ihrer DSGVO-Kategorie zuordnet. Dann tun Sie dies auch für Benutzer. Sofern Sie CIM-konforme Daten integriert haben, sollte alles problemlos funktionieren.

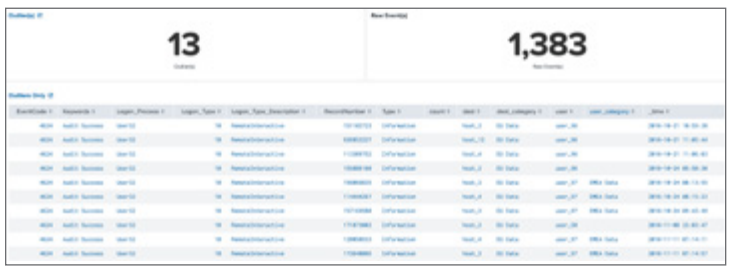
Menge an Benachrichtigungen
Hoch

Bekannte False Positives
Diese Suche wird ausgelöst, wenn eine Person, die nicht in der dokumentierten Liste aufgeführt ist, auf die Daten zugreift. Das wahrscheinlichste Szenario für falsch positive Ergebnisse ist, dass die dokumentierte Liste der autorisierten Benutzer veraltet ist.

Reaktion
Suchen Sie nach Hinweisen darauf, dass jemand zur Dokumentation hinzugefügt werden sollte, klären Sie dies jedoch im Vorfeld mit Ihrem Datenschutzbeauftragten (DSB) oder dessen Team ab. Ziehen Sie in Betracht, die Aktualisierung der Liste der autorisierten Benutzer zu automatisieren und sie aus der Quelle abzurufen, in der Ihr DSB den endgültigen Datensatz der autorisierten Benutzer unterhält. Eine weitere Option besteht darin, die Informationen für berechtigte Abteilungen zu generalisieren und zu veredeln, indem Sie die Benutzernamen um die Abteilungsnamen anreichern.

Hilfe zur Suche nach Benutzern, die regelwidrig bei Systemen angemeldet sind, die Compliance-Regeln unterliegen
In diesem Beispiel werden die einfache Suche und die unten dargestellte Suchsprache verwendet, um in Echtzeitdaten nicht autorisierte Benutzer zu finden, die sich bei bei Systemen angemeldet haben, die Compliance-Regeln unterliegen (In-Scope-Systeme). Bei diesem Dataset handelt es sich um eine Sammlung von Windows-Authentifizierungslogs, die Anmeldungen aus Windows-Sicherheitsprotokollen beinhalten. Unsere Suche sucht nach dem Host in der DSGVO-Kategorisierungssuche und filtert nur nach Hosts, die in den Bereich der DSGVO fallen. Als nächstes suchen wir den Benutzer in der DSGVO-Kategorisierungssuche und schließlich nach Benutzern, die keine passende DSGVO-Kategorie haben oder überhaupt nicht für DSGVO-Informationen autorisiert sind. Der Screenshot unten zeigt die Ergebnisse einer Suche in Beispieldaten.

```
index=* source=win*security user=* dest=*
action=success
| bucket _time span=1d
| stats count by user, dest
| lookup gdpr_system_category.csv host as dest
OUTPUT category as dest_category | search dest_
category=*
| lookup gdpr_user_category user OUTPUT category as
user_category
| makemv delim="|" dest_category | makemv delim="|"
user_category
| where isnull(user_category) OR user_category !=
dest_category
```



Analyse und Erkennung von Betrugsversuchen

Erkennen kompromittierter Benutzerkonten

PHASE 1

Datenquellen

Anwendungslogs | Webzugriffslogs

Sicherheitsherausforderung

Ganz gleich ob Bank-, Kreditkarten-, E-Mail-Konten oder eine beliebige Anzahl von Konten bei unzähligen Serviceanbietern: Betrüger können Onlinekonten übernehmen, ohne dass Sie es bemerken. Durch Phishing-, Spyware- und/oder Malware-Angriffe gelangen Angreifer an wichtige Zugangsdaten, um Zugriff auf Konten zu erhalten. Kontoübernahmen finden insbesondere bei Kreditkartenbetrug, der Verwendung von Kontoberechtigungen und der Nutzung von Kontoabonnements Anwendung. Indem sie sich als der echte Kunde ausgeben, können Betrüger die Kontodaten ändern, Einkäufe tätigen, Geld abheben und die gestohlenen Informationen nutzen, um auf andere Konten und noch sensiblere Daten zuzugreifen. Je nach gewählter Aktivität verzichten Hacker unter Umständen darauf, Änderungen an einem Konto vorzunehmen und verwenden es möglicherweise zur gleichen Zeit wie der Besitzer.

Use Cases

Analyse und Erkennung von Betrugsversuchen

Kategorie

Kontoübernahme, Angriff mit Kennwortliste (Credential Stuffing)

Erforderliche Splunk-Lösungen

Splunk Enterprise

SPL-Schwierigkeitsgrad

Mittel bis hoch

Implementierung

Bestimmen Sie die kritischen Benutzerkontendaten, und stellen Sie sicher, dass die Felder ordnungsgemäß extrahiert werden. Es ist außerdem sinnvoll, Verbesserungen der Sicherheit zu implementieren, wie etwa das Blockieren ungültiger Authentifizierungen, mehrstufige Authentifizierung, die Verwendung von Captchas für alle Authentifizierungen, Identifizierung mithilfe von Machine Learning oder biometrischen Daten – dies sind nur einige der Möglichkeiten. Durch gut durchdachte Verbesserungen wird die Erstellung von Workarounds erschwert, und jeder implementierte Mehraufwand für den Angreifer kann dazu beitragen, unberechtigten Zugriff zu verhindern. Auch Maßnahmen wie das Begrenzen der Durchsatzrate, das Blockieren von IP-Adressen und das Sperren ungültiger Anforderungen können helfen, das Ausmaß von Angriffen in Grenzen zu halten.

Menge an Benachrichtigungen

Mittel

Bekannte False Positives

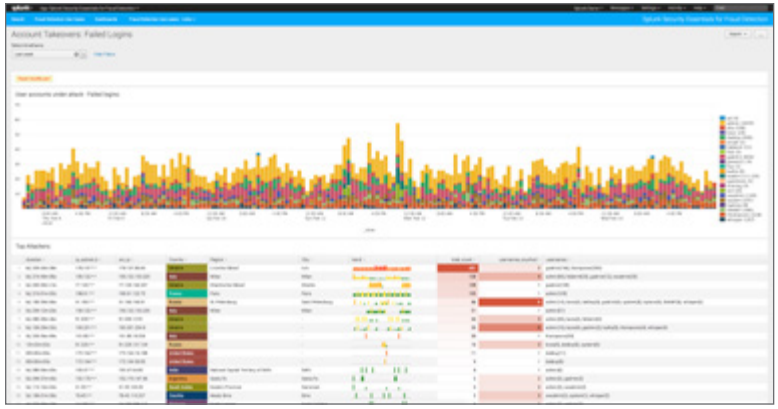
Keine

Reaktion

Es handelt sich hauptsächlich um Brute-Force-Angriffe mit dem Ziel, Benutzerkonten zu übernehmen. Untersuchen Sie angreifende IPs und Subnetze, und passen Sie die Firewall-Regeln entsprechend an, um das Übernahmerisiko zu minimieren. Achten Sie auf Spitzen in einem Zeitdiagramm, und untersuchen Sie Konten, die eine hohe Angriffszahl aufweisen.

Hilfe zum Erkennen kompromittierter Administratorkonten
Verwenden Sie Weblogs, um das Verhalten von Benutzern oder IP-Adressen aufzuzeigen, und Authentifizierungslogs, damit Sie wissen, welche Konten tatsächlich kompromittiert wurden. Dies liefert nützliche Informationen bei der Untersuchung hoher Fehlerraten. Andere Kontoprotokolle können ebenfalls helfen zu verstehen, ob weitere Änderungen vorgenommen wurden, z. B. E-Mail-Änderungen. Die Daten müssen Informationen über Anmeldeversuche enthalten und kennzeichnen, ob der Versuch erfolgreich oder ein Fehlschlag war. Die Suchsprache ist unten dargestellt. Der Screenshot darunter zeigt die Ergebnisse einer Suche in Beispieldaten.

```
index=web-logs action=login result=failure
| stats count, sparkline as trend by src_ip | where
count>5
| sort - count
| table _time src_ip trend count
```



Auffinden anomaler Transaktionen im Gesundheitswesen

PHASE 1

Datenquellen

Anwendungslogs

Sicherheitsherausforderung
Zuletzt wurden in den USA landesweit mehr als 400 Personen wegen Beteiligung am Betrug mit verschreibungspflichtigen Medikamenten angeklagt. Derartige Betrugsfälle können sich auf Vorschriften und Anforderungen auswirken, was Anbietern die Abwicklung des Tagesgeschäfts und Patienten den Zugang zu benötigten Rezepten erschwert. Diese Suche findet Anomalien bei der Abrechnung von Medikamentenverordnungen auf Bundes- und Landesebene (Hinweis: Wir beziehen uns in diesem Beispiel auf das US-Gesundheitswesen).

Use Cases
Analyse und Erkennung von Betrugsversuchen

Kategorie
Kontoübernahme

Erforderliche Splunk-Lösungen
Splunk Enterprise, Splunk Machine Learning Toolkit (MLTK), Splunk Stream

SPL-Schwierigkeitsgrad
Mittel

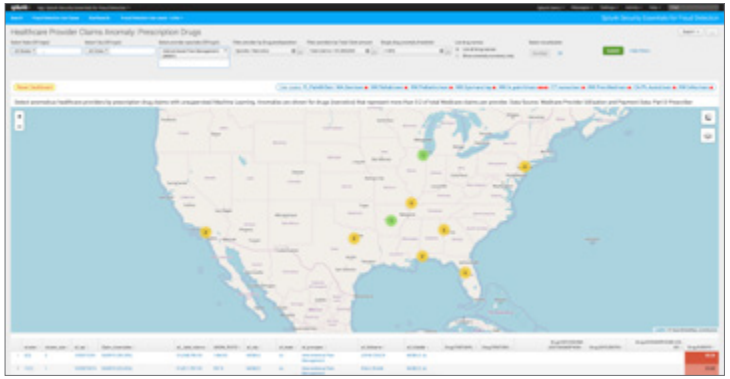
Implementierung
Die Datasets können von **https://data.cms.gov/** heruntergeladen werden (ein deutsches Equivalent hierzu ist z. B. **GovData**). Die Daten liegen im CSV-Format vor und können daher leicht eingelesen werden. Sie können die App herunterladen, um das Dashboard anzuzeigen, und einen Drilldown zum Quell-SPL ausführen. Die App verfügt jedoch bereits über gepackte CMS-Datasets.

Menge an Benachrichtigungen
Mittel

Bekannte False Positives
Die Ergebnisse werden in Form von Anomalien und Ausreißern angezeigt. Es gibt keine definitiven Anhaltspunkte dafür, ob die angezeigten Anbieter betrügerisch handeln oder nicht. Bei weiteren Recherchen haben wir jedoch festgestellt, dass in vielen Fällen anomale Anbieter (die vor allem Opioide in großen Mengen verschreiben) an fragwürdigen Geschäftspraktiken beteiligt waren, manchmal noch Jahre nach der Veröffentlichung der Datasets.

Reaktion
Durch Klicken auf einen Anbieternamen wird das Dashboard mit einer detaillierten Profilanalyse geöffnet. Dadurch können Sie Detaildaten zu den Verschreibungen untersuchen und ggf. bestätigen, dass das Verschreibungsverhalten eines Anbieters im Rahmen eines bundesweiten Vergleichs der Anbieterprofile vom Verschreibungsverhalten vergleichbarer Anbieter abweicht.

Hilfe zum Finden anomaler Dienstleister im Gesundheitswesen
Anomalien werden in einer Karte angezeigt. Durch Klicken auf den gelben Kreis wird eine Zusammenfassung zu einer bestimmten Anomalie eingeblendet. Beim Klicken auf einen Anbieternamen wird das Dashboard mit der detaillierten Profilanalyse geöffnet, das spezifische Daten für den betreffenden Anbieter enthält.



Erkennung interner Bedrohungen

Erkennen großer Web-Uploads

PHASE 1

MITRE ATT&CK-Taktiken

Exfiltration

MITRE ATT&CK-Techniken

Exfiltration über den Command-and-Control-Kanal

Exfiltration über alternatives Protokoll

Datenquellen

Web-Proxy

NGFW

Sicherheitsherausforderung
Datenexfiltration erfolgt heutzutage in der Regel über Standardkanäle, wobei Insider Daten an Google, Dropbox, Box, kleinere File-Sharing-Sites oder sogar nicht aufgeführte Drop-Sites hochladen. Da ausgehende HTTPS-Verbindungen immer gestattet sind, ist die Exfiltration bei den meisten Unternehmen relativ einfach.

Use Cases
Sicherheits-Monitoring, Insider-Bedrohung

Kategorie
Datenexfiltration

Erforderliche Splunk-Lösungen
Splunk Enterprise
Splunk UBA
Splunk einfache Suche

73

SPL-Schwierigkeitsgrad
Einfach

Implementierung
Diese Suche sollte in Palo Alto Networks-Umgebungen sofort funktionieren und lässt sich leicht anpassen, um auch auf andere Quellen für Proxy-Sichtbarkeit angewendet werden zu können. Dazu gehören dedizierte Proxys sowie Tools zur Netzwerktransparenz wie Splunk Stream oder Bro. Passen Sie einfach den Sourcetyp und die abzugleichenden Felder an, und schon sind Sie startklar.

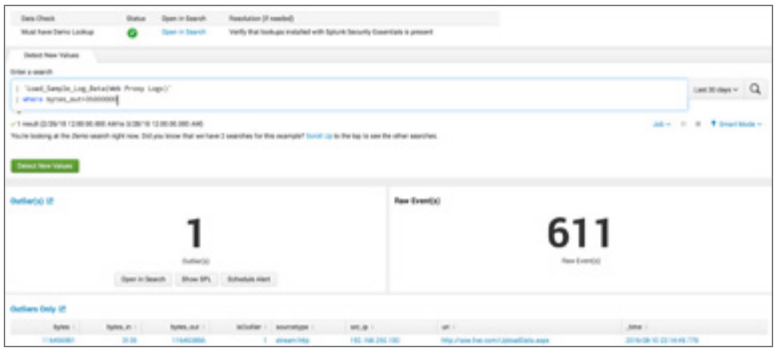
Menge an Benachrichtigungen
Mittel

Bekannte False Positives
Diese Suche liefert Ergebnisse für viele völlig harmlose Vorkommnisse, wie etwa das Hochladen von Urlaubsfotos usw. Viele Unternehmen werden versuchen, diese Zahl durch Filter zu reduzieren, indem sie sich auf Benutzer konzentrieren, die auf einer Watch-List stehen, entweder weil sie Zugang zu sensiblen Daten haben (Geschäftsführung, Wissenschaftler usw.) oder aus Gründen der Beschäftigung (Leistungsplan, Kündigung, Vertragsbeendigung etc.). Diese Watch-Lists können mithilfe von Lookups implementiert werden.

Reaktion
Wenn diese Benachrichtigung ausgelöst wird, hat dies in der Regel legitime Gründe (Hochladen von Urlaubsfotos usw.). Als Reaktion darauf werden viele Analysten überprüfen, wohin die Daten gesendet wurden, und ob der Benutzer bereits zuvor Daten auf diese Site hochgeladen hat. Oftmals rufen Analysten den Benutzer an, um eine Bestätigung für die Aktivität zu erhalten, vorzugsweise im Wissen um die Stellung des Mitarbeiters im Unternehmen. Beispielsweise, ob der Mitarbeiter an einem Leistungsplan teilnimmt oder das Ende seines Vertrags bevorsteht. Beide Szenarien weisen auf ein größeres Risiko der Datenexfiltration hin. Wenn Sie die SSL-Prüfung über Ihre Firewall der nächsten Generation (NGFW) oder DLP für diese Site aktiviert haben, können Sie manchmal die tatsächlich übertragenen Dateien sehen und dadurch den Kontext besser beurteilen.

Hilfe zum Erkennen großer Webuploads
In diesem Beispiel werden die einfache Suche (simple search) und die unten dargestellte Suchsprache verwendet. Die Suche in Echtzeitdaten verwendet ein Dataset aus Proxy-Protokollen und sucht nach allen Events, die größer als 35 MB sind. Der Screenshot unten zeigt die Ergebnisse einer Suche in Beispieldaten.

```
index=* sourcetype=pan:traffic OR (tag=web
tag=proxy) OR (sourcetype=opsec URL
Filtering) OR sourcetype=bluecoat:proxysg* OR
sourcetype=websense* earliest=-10m
| where bytes_out>35000000
| table _time src_ip user bytes* app uri
```



Erkennen der erfolgreichen Anmeldung bei einem Konto eines ehemaligen Mitarbeiters

PHASE 4

MITRE ATT&CK-Taktiken

Rechteausweitung (Privilege Escalation)

Zugriff mit Anmeldeinformationen

MITRE ATT&CK-Techniken

Gültige Konten

Kontomanipulation

Datenquellen

Authentifizierung

Windows Security

Sicherheitsherausforderung
Benutzer, die aus Ihrem Unternehmen ausgeschieden sind, sollten sich im Allgemeinen nicht anmelden. Das könnte bedeuten, dass ihre Anmeldeinformationen früher kompromittiert wurden oder sie versuchen, sich anzumelden, um unangemessene Handlungen durchzuführen. In beiden Fällen sollte dies erkannt werden.

Use Cases
Sicherheits-Monitoring, Insider-Bedrohung

Kategorie
Kontokompromittierung, Insider-Bedrohung

Erforderliche Splunk-Lösungen
Splunk Simple Search Assistant

SPL-Schwierigkeitsgrad
Einfach

Implementierung
Wenn Sie die Anleitungen für die Datenintegration in der Splunk Security Essentials-App befolgt haben, funktioniert diese Suche für Sie ohne weitere Änderungen. Im Allgemeinen sollten Sie den Index angeben, in dem Sie Windows-Sicherheitsprotokolle speichern (z. B. index=oswinsec). Wenn Sie für die Integration dieser Daten einen anderen Mechanismus als den Splunk Universal Forwarder verwenden, überprüfen Sie den Quelltyp und die verwendeten Felder. Der Rest ist einfach!

Menge an Benachrichtigungen
Gering

Bekannte False Positives
Wenn Ihr Unternehmen Konten nicht deaktiviert oder entfernt, ist diese Suche unter Umständen nicht durchführbar. Wenn dies bei Ihnen der Fall ist, sollten Sie erwägen, gewisse Grenzen für dieses Verhalten festzulegen, indem Sie Systeme bestimmen, auf denen nach dem Beschäftigungsende mit „akzeptablen“ Aktivitäten gerechnet werden kann, wie beispielsweise die E-Mail-Umgebung. Richten Sie zudem eine Kontrollmaßnahme ein, die sicherstellt, dass Kennwörter geändert werden, wenn sich der Status eines Mitarbeiters von aktiv in inaktiv ändert. Versuchen Sie außerdem, die Kontennutzung nach dem Ausscheiden des Mitarbeiters einzuschränken.

Reaktion
Wenn diese Benachrichtigung auftritt, muss zunächst geklärt werden, ob es sich um eine Fortsetzung des normalen Systembetriebs handelt (war beispielsweise der Desktop-PC unter dem Schreibtisch des Mitarbeiters noch angemeldet oder das iPhone-Konto noch aktiv) oder um eine vorsätzliche Aktion. Außerdem fällt natürlich der Erfolg bzw. Misserfolg des Zugriffsversuchs ins Gewicht. Zuletzt muss besonders im Fall von Mitarbeitern, die als Systemadministrator in weniger strukturierten Unternehmen beschäftigt waren, unbedingt sichergestellt werden, dass keine Services oder geplanten Aufträge unter deren Konto ausgeführt werden, sodass sich durch die Deaktivierung des Kontos Auswirkungen auf den Betrieb ergeben könnten.

Hilfe zum Erkennen der erfolgreichen Anmeldung bei einem Konto eines ehemaligen Mitarbeiters

In diesem Beispiel werden die einfache Suche (simple search) und die unten dargestellte Suchsprache verwendet, um in Echtzeitdaten eine erfolgreiche Authentifizierungsaktivität bei Konten ehemaliger Mitarbeiter zu erkennen. Unser Dataset stellt eine Sammlung anonymisierter Windows-Authentifizierungslogs mit erfolgreicher Anmeldung dar. Ein Lookup zeigt den Benutzerstatus an, so dass wir nach Benutzern filtern können, die entweder deaktiviert sind, oder bei denen die Ablaufzeit mindestens einen Tag zurückliegt. Der Screenshot unten zeigt die Ergebnisse einer Suche in Beispieldaten.

```
index=* (source=win*security
OR sourcetype=linux_secure OR
tag=authentication) user=* user!= ""
action=success
| lookup user_account_status.csv user
| where _time > relative_
time(terminationDate, "+1d")
```

Erfahren Sie **mehr.**

Sind Sie bereit, mehr darüber zu erfahren, wie Sie Ihr IT-Sicherheitsniveau mithilfe von Splunks analysegestützter Sicherheit optimieren können? Erfahren Sie kostenlos, wie Sie 300 unterschiedliche Sicherheitsherausforderungen lösen können, indem Sie die **Splunk Security Essentials**-App von Splunkbase herunterladen. Arbeiten Sie dann mit den Sicherheitsexperten und Partnern von Splunk daran, die Use Cases in Ihrer Umgebung zu implementieren.
Legen Sie noch heute los – **Kontaktieren Sie uns.**

splunk> turn data into doing™

2020-Splunk-SEC-Essential Guide to Security-116_Web-EB-DE