

Der große Leitfaden zu **Zero Trust**





Inhalt

Was ist Zero Trust?	4
Die Evolution von Zero Trust	5
Das Zero Trust-Modell.....	6
Der Weg zu Zero Trust mit Splunk Data Analytics	9
Phase 1: Sammeln relevanter Daten	12
Phase 2: Verstehen und Kontextualisieren Ihrer Daten.....	13
Phase 3: Erweitern Ihrer Datenbasis	16
Phase 4: Veredeln und Anreichern Ihrer Daten.....	18
Phase 5: Fortgeschrittene Automatisierung und Orchestrierung.....	19
Phase 6: Advanced Threat Detection	21
Zero Trust erfordert einen „Ökosystem-Ansatz“	23
Ihr Zero Trust-Ökosystem in Aktion	26
Ein datenzentrierter Ansatz für Zero Trust.....	27



Immer mehr Unternehmen setzen auf eine Zero Trust-Strategie, um ihre Daten und Systeme zu schützen. Zero Trust ist nach COVID-19 für jedes Unternehmen enorm wichtig, ganz unabhängig von der Größe oder Branche. Auch öffentlichkeitswirksame Sicherheitsverletzungen (siehe: [SolarWinds](#)), die Migration in die Cloud und eine immer größer werdende Angriffsfläche machen neue Ansätze notwendig.

Ein solches Vorhaben kann überwältigend wirken. Besonders, wenn dabei die Sicherheitssysteme des gesamten Unternehmens neu gestaltet werden müssen – *und* auch jedes Gerät, jede Anwendung und jeder Benutzer berücksichtigt werden muss. Erschwerend kommt hinzu, dass sich Zero Trust nicht nur auf die traditionelle IT beschränkt, sondern auch für operative Technologien, industrielle Steuerungssysteme (OT/ICS) und das Internet der Dinge (IoT) gilt, die allesamt beliebte Angriffspunkte von Hackern darstellen.

Und wie lautet die gute Nachricht? Ein Zero Trust-Modell kann die Sicherheitslage Ihres Unternehmens radikal verbessern *und* den operativen Aufwand minimieren, indem es der reinen Ausrichtung auf perimeterbasierten Schutz ein Ende setzt. Abweichend von traditionellen Methoden, etabliert Zero Trust ein bestimmtes Maß an Vertrauen an jedem Access Point und schützt so Benutzer, Assets und Ressourcen effektiv. Das bedeutet allerdings nicht, dass ganz auf perimeterbasierte Sicherheit verzichtet wird. Es ändert sich vielmehr der organisatorische Ansatz beim Schutz der wichtigsten Assets.

Fazit: Zero Trust ist *nicht nur* ein architektonisches Framework. Zero Trust ist ein Mindset, das Unternehmen dazu zwingt, die Überwachung, Prüfung und Behebung von Problemen zu überdenken. In diesem Leitfaden befassen wir uns mit den Faktoren, die eine Zero Trust-Strategie erforderlich machen. Außerdem beleuchten wir, was eine solche Strategie beinhaltet, wie sie implementiert werden kann und wie man letztlich neu definiert, was Sicherheit wirklich bedeutet.

Was ist Zero Trust?

Das Grundprinzip von Zero Trust besteht darin, die Daten eines Unternehmens zu schützen, ganz gleich, wo diese gespeichert sind, und gleichzeitig nur *legitimen* Benutzern und Entitäten den Zugriff auf relevante Ressourcen und Assets zu gewähren. Bei diesem Konzept gilt jeder Benutzer, jedes Gerät und jeder Service, der bzw. das Zugriff auf das Netzwerk eines Unternehmens anfordert, bis zum Beweis des Gegenteils als feindlich.

Einfach ausgedrückt: Das Wichtige bei diesem Konzept ist es, zu verstehen, wer Zugriff wünscht und von welchem Gerät die Anfrage ausgeht, und dies dann mit den Zugriffsrichtlinien der jeweiligen Anwendung bzw. des Assets abzugleichen. Im Prinzip handelt es sich hierbei um eine Whitelist-Methode für Zugriffsrechte, die auf dem Gerät, den Benutzeranmeldeinformationen und dem Verhalten eines Mitarbeiters basiert. Die Authentifizierung muss für jede Session auf Geräte- und Benutzerebene erfolgen, sodass eine durchgängige, adaptive Autorisierung auf granularer Ebene sichergestellt ist.

Ein erfolgreiches Zero Trust-Sicherheitsprogramm muss Folgendes leisten:

- Es muss davon ausgehen, dass das Netzwerk immer feindlich ist.
- Es muss annehmen, dass es ständig externe und interne Bedrohungen im Netzwerk gibt.
- Es muss wissen, dass ein Netzwerkstandort nicht als Nachweis der Vertrauenswürdigkeit im Netzwerk ausreicht.
- Es muss jeden Geräte-, Benutzer- und Netzwerkdatenstrom authentifizieren und autorisieren.
- Es muss Richtlinien implementieren, die dynamisch sind und anhand so vieler Datenquellen wie möglich bewertet werden.

Wie ein solches System aussieht, zeigen wir Ihnen am Beispiel eines Mitarbeiters, der autorisiert wird, ein Ticket-Management-System eines Unternehmens auf einem neu zugewiesenen Gerät zu nutzen. Der Mitarbeiter stellt die Zugriffsanfrage von dem betreffenden Gerät, und der Zugriff wird gewährt. Irgendwann lädt der Mitarbeiter einen Treiber von einer Website herunter, der nützlich zu sein scheint. Da das Gerät im Zuge der Zero Trust-Strategie kontinuierlichem Monitoring unterliegt, wird die Aktualisierung gemeldet.

Durch die neu hinzugefügte Komponente hat sich die Konfiguration – und damit auch die Bewertung der Vertrauenswürdigkeit (Trust Score) – des betreffenden Geräts geändert. Wenn der Mitarbeiter nun versucht, sich mit dem System zu verbinden, könnte ihm der Zugriff verweigert oder auf eine geringere Zugriffsstufe reduziert werden – dies hängt von seinem neuen Trust Score und der zugehörigen Richtlinie ab. Dies zeigt, wie die Nutzung mehrerer Faktoren (in diesem Fall die kombinierten Bewertungen von Benutzer, Gerät und Ressource) Security-Teams hilft, das Risiko für Unternehmensressourcen dynamisch zu senken. Ein Zero Trust-System ist in der Lage, geänderte Bedingungen zu berücksichtigen und damit eine durchgängige Bewertung und kontinuierlichen Schutz zu bieten.



Die Evolution von Zero Trust

Bevor Zero Trust von [Forrester im Jahr 2010](#) zum ersten Mal definiert wurde, hielten sich Sicherheitsexperten an ein netzwerkbasierendes Segmentierungsmodell, das auf traditionellen Netzwerksicherheitslösungen aufbaute. Bei diesem Modell wird ein geschützter Perimeter wie ein Bollwerk um das Netzwerk einer Organisation aufgebaut, in dem sich alle wertvollen Ressourcen und Daten befinden. Sollte jedoch eine Bedrohung in das Netzwerk gelangen und den Perimeter durchbrechen, hätte der Hacker freie Hand und könnte sich lateral durch das Netzwerk und alle damit verbundenen Systeme bewegen, Assets kompromittieren und irreparable Schäden anrichten.

Das Ende des reinen Perimeterschutzes

Irgendwann gaben Security-Teams den netzwerkorientierten Ansatz auf und wandten sich einem neuen Ansatz zu: Dieser basiert auf der Grundannahme, dass kein Gerät, Benutzer oder System – ob unternehmensintern oder -extern – implizit vertrauenswürdig ist und der Zugriff auf alle Ressourcen explizit authentifiziert und autorisiert werden sollte. Bis vor kurzem war dies jedoch viel leichter gesagt als getan. Bei bestimmten Technologien fehlten einfach die notwendigen Integrationsmöglichkeiten, wodurch Unternehmen nur beschränkte Möglichkeiten hatten, die Gesamtsicherheit ihrer Ressourcen zentral und ganzheitlich zu überwachen. Diese führte zu weiterer Fragmentierung und machte eine detaillierte Implementierung durch Sicherheitsingenieure notwendig.



Heute gibt es viele Technologien rund um das Thema Zugriffskontrolle. Damit sind Regeln gemeint, die festlegen, wer Zugang zu einem zu schützenden Standort bzw. Zugriff auf kritische Informationen erhalten soll. Eine Zero Trust-Architektur kann diese Systeme vereinen und so die Komplexität reduzieren, die von der unabhängigen Verwaltung mehrerer Kontrollen verursacht würde.

Zu diesen Technologien gehören u. a.:

- IAM (Identity and Access Management)
- MFA (Mehrfaktoren-Authentifizierung)
- DLP (Data Loss Prevention)
- CASB (Cloud Access Security Broker)
- CIEM (Cloud Infrastructure Entitlement Management)

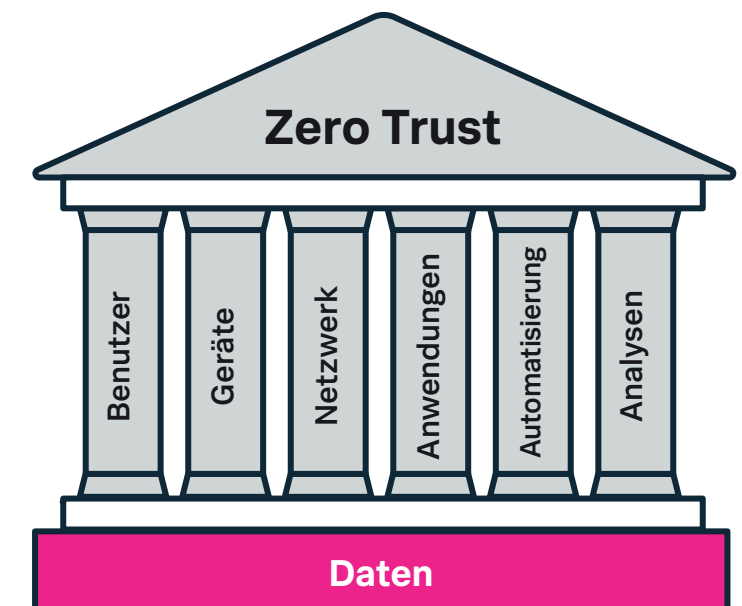
Dank dieser technologischen Fortschritte lässt sich Zero Trust leichter implementieren. Auch COVID-19 veranlasste Organisationen und Unternehmen rund um den Globus, ihre digitale Transformation zu beschleunigen. Praktisch über Nacht waren Mitarbeiter zu Remote-Arbeit gezwungen, wodurch die IT- und Sicherheitsinfrastruktur gehörig unter Druck geriet. Diese neuen Herausforderungen machten in Kombination mit der Abwendung von perimeterbasiertem Schutz und einer wachsenden Angriffsfläche Zero Trust weltweit zu einem absoluten Muss.

Das Zero Trust-Modell

Der American Council for Technology and Industry Advisory Council ([ACT-IAC](#)) – eine gemeinnützige, öffentlich-private Partnerschaft mit dem Ziel, die Arbeit der öffentlichen Hand durch Informationstechnologie zu verbessern – beschreibt die sechs Grundpfeiler eines Zero Trust-Sicherheitsmodells, die alle zusammen von einem Fundament aus Daten getragen werden.

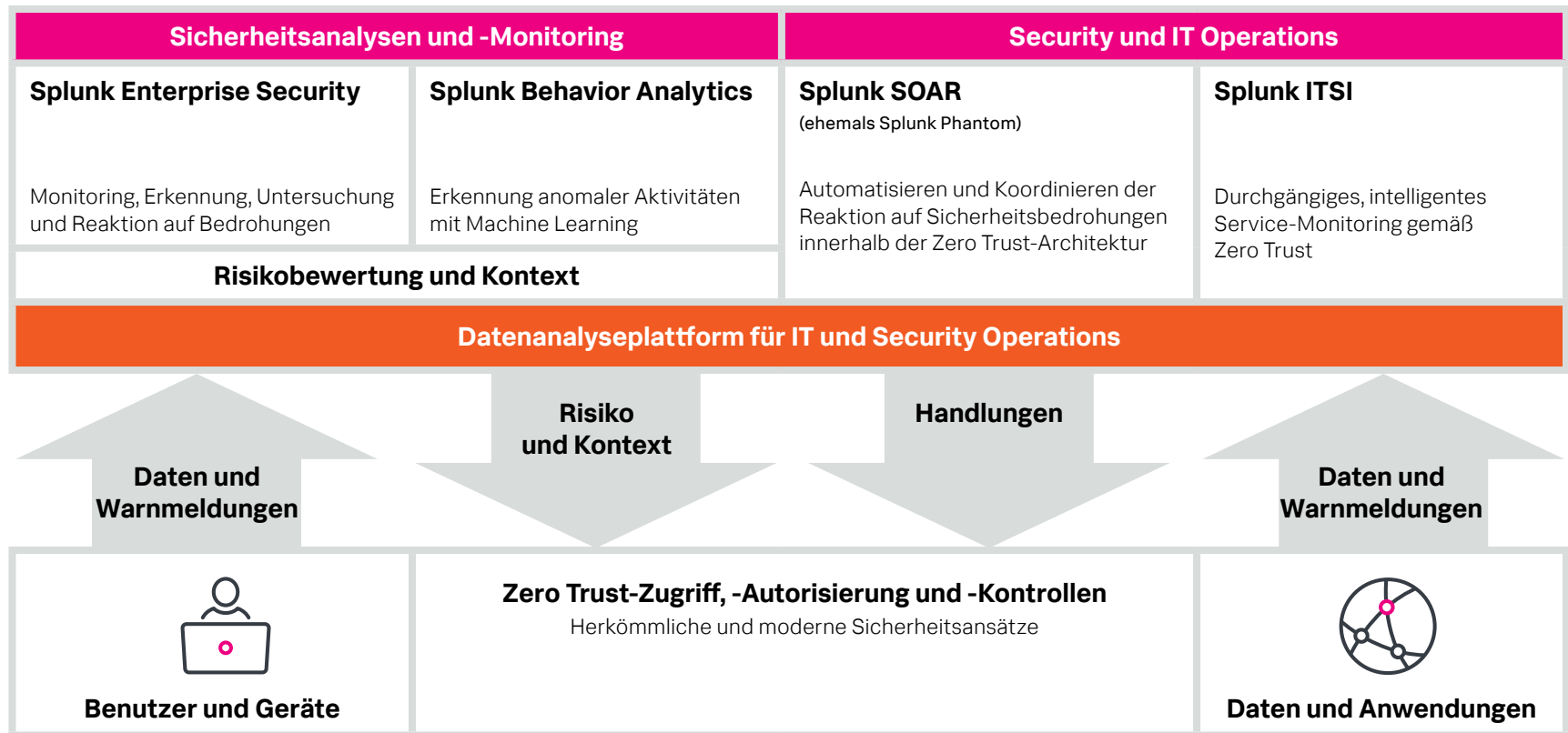
Diese Grundpfeiler lassen sich wie folgt zusammenfassen:

- **Benutzer:** Ständiges Authentifizieren vertrauenswürdiger Benutzer sowie kontinuierliches Monitoring und Überprüfen der Vertrauenswürdigkeit von Benutzern, um ihren Zugriff und ihre Berechtigungen zu kontrollieren
- **Geräte:** Messen der Echtzeit-Cybersicherheitslage und der Vertrauenswürdigkeit von Geräten
- **Netzwerk:** Die Möglichkeit, das Netzwerk zu segmentieren, zu isolieren und zu kontrollieren – dies schließt Software-definierte Netzwerke, Software-definierte WANs (Wide Area Networks) und Internet-basierte Technologien ein.
- **Anwendungen:** Schutz und ordentliche Verwaltung der Anwendungsebene sowie der Container und virtuellen Maschinen (VMs)
- **Automatisierung:** SOAR-Systeme (Security Automation, Orchestration and Response) ermöglichen Unternehmen, Aufgaben durch Workflows produktübergreifend zu automatisieren und zur interaktiven Kontrolle von Endbenutzern einzusetzen.
- **Analysen:** Mit Tools, die Transparenz und Analysen ermöglichen, wie etwa SIEM-Systeme (Security Information and Event Management), Advanced Security Analytics und UEBA (User and Entity Behavior Analytics), können Sicherheitsexperten das Geschehen im Blick behalten und ihre Abwehrmaßnahmen entsprechend ausrichten.



Ihre praktische Checkliste zum Thema Zero Trust

☐	Ein Zero Trust-Modell sollte den Benutzerzugriff auf alle Assets und Ressourcen autorisieren und authentifizieren. Der Zugriff sollte auf der Basis der entsprechenden Unternehmensrichtlinien und pro Session gewährt werden.
☐	Zero Trust-Kontrollen müssen identifiziert und auf Ihre Systeme, Benutzer und Daten ausgerichtet werden. Dies sollte aus zwei Perspektiven geschehen:
☐	Sicherheitskontrollen zum Schutz von interner bzw. Cloud-basierter Infrastruktur, Netzwerken, Systemen, Anwendungen und Daten, manchmal auch als „Objekt“ bezeichnet.
☐	Sicherheitskontrollen mit dem Zweck, Benutzer und Endpunkte beim Zugriff auf Ressourcen zu schützen und zu autorisieren. Dies sollte auch Verwaltungszugriff beinhalten. Oftmals als „Subjekt“ bezeichnet.
☐	Es sollte einheitliche Richtlinien, Verfahren und Protokolle geben, um die Identität und den Trust Score von Benutzern und Geräten in allen Systemen, einschließlich externer Ressourcen (z. B. Software-as-a-Service), zu verwalten.
☐	Die Verwaltung von Zero Trust-Kontrollen muss vereinheitlicht werden. Außerdem muss dynamischer End-to-End-Zugang auf der Basis der Geschäftslogik und nicht auf der Grundlage traditioneller Sicherheitsregeln (z. B. IP-basierter Kontrollen) bereitgestellt werden.
☐	Es sollten End-to-End-Datenanalysen eingerichtet werden, um Monitoring und Bedrohungserkennung für die gesamte Architektur zu ermöglichen und sowohl IT- als auch SecOps-Anforderungen zu unterstützen.
☐	Sicherheitsmaßnahmen werden zentral umgesetzt, mit kontextualisiertem Risiko-Profil und fortschrittlicher Richtlinienlogik für die Autorisierung.
☐	Bestehende Sicherheitskontrollen und -prozesse müssen berücksichtigt werden. Zudem müssen ihre Eignung und Kompatibilität innerhalb der weiter gefassten Zero Trust-Architektur geprüft werden.



Nachdem Sie nun alles über die Geschichte und Grundprinzipien von Zero Trust wissen, können wir uns der Umsetzung einer Zero Trust-Strategie zuwenden. In den folgenden Abschnitten befassen wir uns damit, wie der Aufbau eines modernen Security Operations Center (SOC) das für Zero Trust notwendige Sicherheits-Monitoring unterstützen kann und wie Splunk Unternehmen dabei helfen kann, ihre Zero Trust-Ziele im Handumdrehen zu erreichen.

Der Weg zu Zero Trust mit Splunk Data Analytics

Für Unternehmen, die eine Zero Trust-Strategie umsetzen möchten, sind die Aspekte Monitoring, Erkennung und Untersuchung von Sicherheits-Incidents im Zusammenhang mit Zero Trust-Kontrollen und -Richtlinien unerlässlich. Dies gilt ganz besonders für die Schutzmaßnahmen in Bezug auf Benutzer, Systeme, Anwendungen und Daten.

Splunk unterstützt schon seit vielen Jahren Kunden bei der Implementierung von Datenanalyzelösungen. Vor diesen Hintergrund – und mithilfe von branchenspezifischen Best Practices sowie der gesammelten Splunk-Erfahrung – hat Splunk die sogenannte Security Data Analytics Journey entwickelt.

Dieses Reifegradmodell unterteilt die Security Journey eines Unternehmens in einzelne Phasen. Jede Phase deckt dabei spezifische Ziele ab und sieht vor Beginn der nächsten Phase schrittweise, iterative Verbesserungen vor. Obwohl dieser Weg auf Sicherheitsziele ausgelegt ist, lässt er sich durch die Wiederverwendung und Wiederaufbereitung von Daten auch auf die Entwicklung von IT-Monitoring-Funktionen anwenden.

Dieser Ansatz ist perfekt dazu geeignet, um: 1. Ihre IT- und Sicherheitsprozesse besser auf eine Zero Trust-Strategie auszurichten und 2. ein modernes SOC aufzubauen, das eine Zero Trust-Architektur unterstützt und bestehende Lücken schließt. In den folgenden Abschnitten werden die einzelnen Phasen der Datenanalyse beschrieben, sodass Sie die Zero-Trust-Anforderungen erfüllen und effiziente IT- und Sicherheitsabläufe gewährleisten können.

Die Splunk Security Data Analytics Journey

PHASE 6

Advanced Detection

Anwenden komplexer Erkennungsmechanismen wie Machine Learning

PHASE 5

Automatisierung und Orchestrierung

Einrichten konsistenter, wiederholbarer Security Operations

PHASE 4

Veredelung

Anreichern von Sicherheitsdaten mit Informationsquellen für ein besseres Verständnis vom Kontext und von den Auswirkungen eines Events

PHASE 3

Erweiterung

Erfassen weiterer zuverlässiger Datenquellen wie Endpunktaktivitäts- und Netzwerkmetadaten zur Unterstützung der Erkennung komplexer Bedrohungen

PHASE 2

Normalisierung

Anwenden einer standardmäßigen Sicherheitstaxonomie und Hinzufügen von Asset- und Identitätsdaten

PHASE 1

Erfassung

Erfassen grundlegender Sicherheitslogs und anderer Maschinendaten aus Ihrer Umgebung

In den einzelnen Phasen Ihrer Zero Trust-Journey werden wir Ihnen jeweils zeigen, wie unsere Produktpalette die verschiedenen Anforderungen in puncto Sicherheit und IT-Monitoring für Zero Trust erfüllt. Zu diesen Produkten gehören:

- **Splunk Enterprise: Plattform für Datenanalysen und -untersuchungen**

- Skalierbare Datenanalyseplattform, unterstützt Use Cases aus den Bereichen IT, Security und Betrugsbekämpfung für Zero Trust-Architekturen.
- Kann eine breite Palette an strukturierten und unstrukturierten Daten aufnehmen
- Umfassendes **Partnernetzwerk**: Bietet Zero Trust-Lösungen zur Unterstützung der Integration und des schnellen Onboardings und Normalisierens von Datenquellen.

- **Splunk Enterprise Security: SIEM (Security Information and Event Management)**

- Umfassende Library mit Use Cases zu Sicherheits-Monitoring und Bedrohungserkennung, unterstützt von **Splunk Security Essentials** (SSE) und **Enterprise Security Content Update** (ESCU)
- Wichtige Frameworks, die die Anreicherung und Kontextualisierung von Asset- und Identitätsdaten, die Risikobewertung und das Sicherheitsniveau im Rahmen von Zero Trust-Zielsetzungen unterstützen.
- Risikobasierte Warnmeldungen helfen bei der erweiterten Risikobewertung und der Erkennung mit mehreren Indikatoren, die sich am MITRE ATT&CK-Framework orientieren. Über Zero Trust-Kontrollen hinweg werden Aktivitätssequenzen geprüft, die auf böswilliges Verhalten hindeuten könnten.

- **Splunk User and Entity Behavior Analytics (UEBA)**

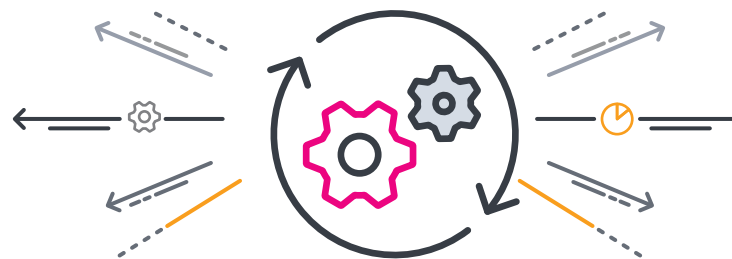
- Out-of-the-box einsetzbares Unsupervised Machine Learning für die fortschrittliche Verhaltenserkennung und automatische Identitätsauflösung

- **Splunk SOAR für Security Orchestration, Automation and Response (ehemals Splunk Phantom)**

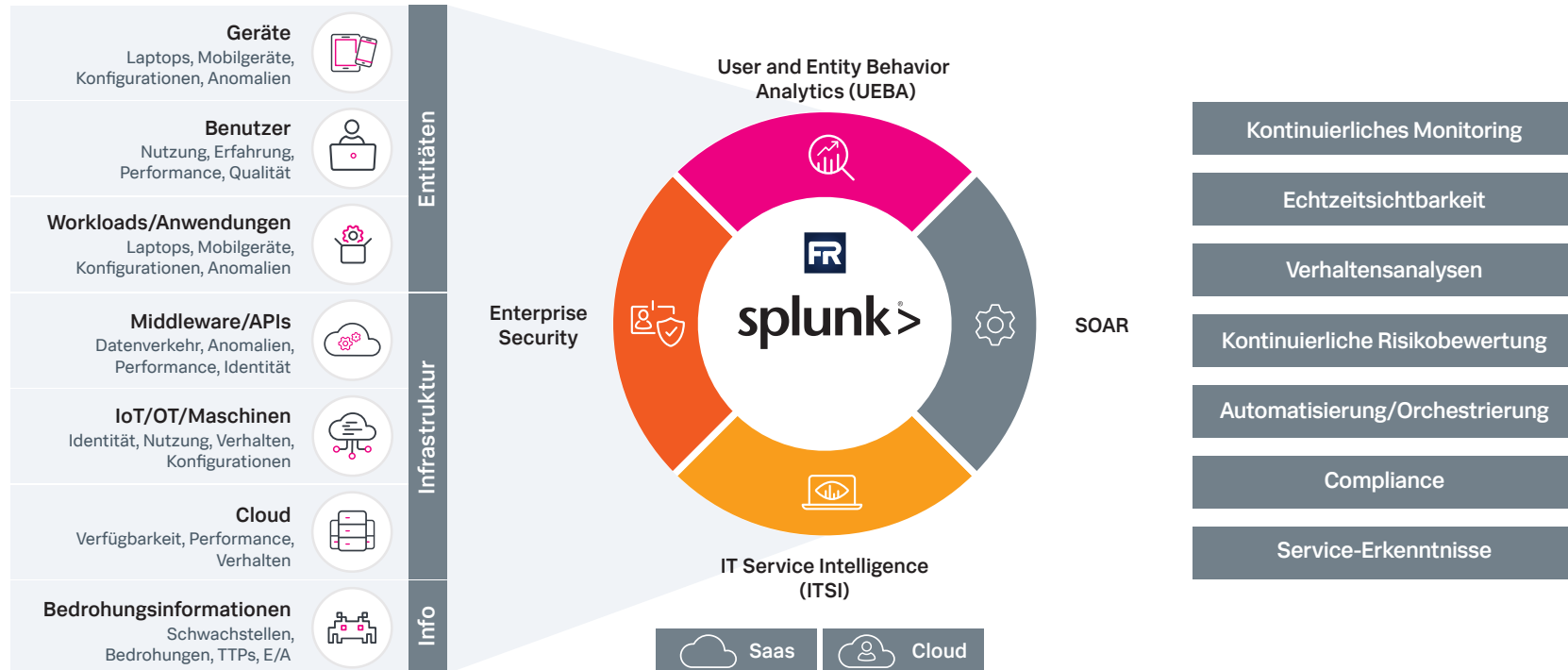
- Umfassendes Ticket-Management, Incident-Untersuchung, Orchestrierung und Automatisierung für die Reaktion auf Sicherheits- und Service-Incidents innerhalb einer Zero Trust-Architektur

- **Splunk IT Service Intelligence (ITSI)**

- Durchgängiges Service-Monitoring von Zero Trust-Kontrollen und der zugrundeliegenden Infrastruktur der zugehörigen Anwendungen und Services



Splunk Lösungsüberblick für Zero Trust IT und Security Operations





Phase 1: Sammeln relevanter Daten

Ermitteln Sie zuerst die wichtigsten Assets Ihres Unternehmens – also die Assets, die Sie schützen und überwachen müssen, geordnet nach Priorität. Nach der Sichtung der Assets wird klarer, wo Sie Ressourcen zuweisen und wo Sie mit der Datenaufnahme beginnen sollten.

Da Zero Trust viele unterschiedliche Arten von Technologien umfasst, verwendet Ihr Unternehmen wahrscheinlich bereits einige dieser Systeme. Diese Technologien sind eine wichtige Datenquelle für das IT- und Security-Monitoring und das Fundament eines umfassenden End-to-End Zero Trust-Programms.

Beispiele für diese Technologien sind:

- Next-Generation Firewalls (NGFW)
- Software-definierte Netzwerke (SDN) und Mikrosegmentierungslösungen
- CASB (Cloud Access Security Broker)
- Remote-Zugriff
 - VPN (Virtual Private Network)
 - Virtuelle Desktop-Infrastruktur (VDI)
 - Zero Trust-Zugriff (Zero Trust Access, ZTA)
- Identity Access Management (IAM) und Directory Services
- Mehrfaktoren-Authentifizierung (MFA)
- Privileged Authentication Management (PAM)
- Endpoint Detection and Response (EDR)
- Lösungen zur Stärkung des Sicherheitsniveaus (z. B. Patch- und Schwachstellenmanagement)
- Web-Proxy, Webfilter und sichere Webzugangsservices
- Data Loss Prevention (DLP)
- Secure Access Service Edge (SASE)
- UEM- (Unified Endpoint Management) und MDM-Lösungen (Mobile Device Management)

Elemente, aus denen die zugrundeliegende Infrastruktur von Systemen und Services besteht, wie etwa Speicher und Netzwerke sowie Komponenten zur Unterstützung von IT-Verwaltungsfunktionen sind ebenfalls wichtige Datenquellen und sollten in dieser Phase berücksichtigt werden.

Beispiele:

- **Netzwerk:** Die Netzwerkinfrastruktur des Rechenzentrums und der Cloud, wie Switches, Router, Load Balancer sowie alle virtualisierten Netzwerkdienste.
- **Speicher:** Speichersysteme und -Services des Rechenzentrums und der Cloud wie Speicher-Arrays, Systemlaufwerke, Network-Attached Storage (NAS/SAN) und Cloud-Speicherservices
- **Computing:** Computing-Ressourcen des Rechenzentrums und der Cloud, einschließlich Monitoring physischer und virtualisierter Computing-Systeme und der zugehörigen Betriebssysteme
- **Verwaltung:** Systeme und Anwendungen zur Unterstützung von Verwaltungsfunktionen wie Monitoring-Systeme, Jump-Hosts, Verwaltungsauthentifizierung und privilegierte Zugangskontrolle

Das mag nach einer Menge Arbeit klingen, doch ein wichtiger Aspekt der Splunk-Datenanalyse besteht darin, Einzelschritte durchzuführen, die jeweils auf dem betreffenden System oder Service sowie auf dem speziellen Use Case basieren, den Sie zu diesem Zeitpunkt implementieren. Mit dem Identifizieren und Definieren der kritischsten Assets und Entitäten legen Sie die Grundlage für die Kontextualisierung und Priorisierung von Benachrichtigungen zu IT- und Security-Incidents. Beim Ausbau Ihrer Datenquellen können Sie diese Daten dann wiederverwenden, während Sie auf der Reifegradkurve voranschreiten.

Phase 2: Verstehen und Kontextualisieren Ihrer Daten

Das Kontextualisieren Ihrer Daten ist der Schlüssel jeder Zero Trust-Strategie. Um Ihre Daten zu verstehen, müssen Sie eine Standardtaxonomie für alle Datenquellen implementieren, andernfalls bleibt Ihnen nur eine Menge Datenrauschen. Die Festlegung einer Taxonomie für Ihre Daten sorgt für Klarheit, vor allem in den späteren Phasen der Security Journey.

Ein Beispiel hierfür sind die unterschiedlichen Logformate und Datenstrukturen, die Firewall-Anbieter für verschiedene Systeme verwenden. Für ein zentrales Monitoring müssen Firewall-Logdaten so strukturiert sein, dass die Feldnamen und -werte normalisiert sind und ein einheitliches Format aufweisen.

Strukturieren oder nicht strukturieren? Das ist hier die Frage

Splunk hat ein Common Information Model (CIM) entwickelt, bei dem es sich um einen offenen, erweiterbaren Ansatz für die Erstellung einer gemeinsamen Taxonomie handelt. Mit Splunk CIM werden Feldnamen und -werte strukturiert und standardisiert, die aus Rohdaten extrahiert und anschließend in Datenmodelle umgewandelt werden, die eine breite Palette von Kategorien abdecken. Bei Splunk erfolgt dies nach der Datenaufnahme und ohne Änderung der eigentlichen Rohdaten.

Das heißt, Sie können Datenstrukturen bei geänderten Anforderungen weiterhin aktualisieren, *ohne* die Rohdaten ändern oder die Daten mit viel Aufwand erneut einspeisen zu müssen. Ein weiterer Vorteil ist die Beschleunigung von Datenmodellen, bei der Sie Datensets mithilfe einer Pivot-Suche beschleunigen können, was die Suchleistung bei strukturierten Daten erhöht. Ergebnisse, die für den Gesamtzustand Ihres Zero Trust-Modells wichtig sind, werden schnell und kalkulierbar zurückgegeben.

Splunk CIM unterstützt diese nativen Monitoring- und Erkennungsmöglichkeiten innerhalb von [Splunk Enterprise Security](#) (ES) und lässt sich auf alle Ihre dedizierten Zero Trust-Datenquellen anwenden. Das Onboarding und die Normalisierung von Daten wird auch durch unser Splunk-Partner- und Anwender-Ökosystem unterstützt, das ein breites Spektrum an Splunk Add-Ons für Kunden bereithält.

Fazit? Splunk Add-Ons unterstützen zahlreiche Zero Trust-Datenquellen und werden laufend aktualisiert, um auch neue und veränderte Anforderungen zu erfüllen.

Die neue Normalisierung

Jetzt können wir uns an die Implementierung von Use Cases machen, die auf normalisierte Daten ausgelegt sind. Ein hervorragender Ausgangspunkt für Sicherheitserkennungen ist die Use Case Bibliothek von [Splunk Security Essentials](#) (SSE). SSE enthält eine umfassende Palette von Use Cases, die den einzelnen Phasen der Security Analytics Journey entsprechen.

Darüber hinaus gibt es jetzt eine neue Kategorie in SSE, die Zero Trust-Anwendungsfälle identifiziert und in Anlehnung an das [MITRE ATT&CK-Framework](#) den einzelnen Entwicklungsphasen zuordnet. Das MITRE ATT&CK-Framework bietet eine umfassende Wissensdatenbank zu realen Bedrohungstaktiken und -techniken und wird von vielen Security-Teams genutzt.



Wir nutzen das Potenzial von MITRE ATT&CK

Durch die Bewertung der Bedrohungen, die mit einer Zero-Trust-Strategie verhindert werden sollen, haben wir eine umfassende Liste von Sicherheitsanwendungsfällen identifiziert, die auf den entsprechenden MITRE ATT&CK-Taktiken basieren. Angesichts der Komplexität und des Umfangs einer vollständigen Zero Trust-Implementierung kann dies Unternehmen helfen, einen [auf Kontrollen basierenden Ansatz](#) mit geeigneten Sicherheitserkennungs- und Monitoring-Use Cases für Zero Trust auszubauen.

Bitte beachten Sie jedoch, dass diese Tipps und Hinweise im Kontext einer breiter angelegten Security-Monitoring-Strategie zu sehen sind, da es noch genügend andere Bedrohungen gibt, die unter bestimmten Umständen eintreten *können* und *werden*.

Wir haben folgende [MITRE ATT&CK-Taktiken](#) herangezogen, um die primären Sicherheitserkennungs-Use Cases in SSE für Zero Trust in Kategorien zu unterteilen:

- **Erstzugriff (Initial Access):** Der Angreifer versucht, in Ihr Netzwerk einzudringen.
- **Persistenz (Persistence):** Der Angreifer versucht, in Ihrem System Fuß zu fassen.
- **Rechteauserweiterung (Privilege Escalation):** Der Angreifer versucht, sich weiterreichende Berechtigungen zu verschaffen.
- **Zugriff mit Anmeldeinformationen (Credential Access):** Der Angreifer versucht, Kontonamen und -kennwörter zu stehlen.
- **Laterale Bewegung (Lateral Movement):** Der Angreifer versucht, sich durch Ihre Umgebung zu bewegen.
- **Exfiltration:** Der Angreifer versucht, Daten zu stehlen.



Die folgenden Use Cases können für Phase 2 der Security Journey (Normalisierung von Daten) gelten und basieren auf grundlegenden Datenquellen wie Authentifizierungs-, Netzwerk- und Endpunktdaten (die in Phase 1 eingebunden wurden):

- Änderungen in der Kontoverwaltung
- Erstellung neuer Konten
- Änderungen an Sicherheitsrichtlinien oder -kontrollen
- Brute Force-Authentifizierungsaktivitäten
- Löschen von Verwaltungs- oder Sicherheitslogs
- Nicht autorisierte Änderungen an der Systemkonfiguration

Da die Datennormalisierung Teil dieser Phase ist, können wir Splunk Enterprise Security für das Monitoring und Reporting von Aktivitäten im Zusammenhang mit Zero Trust nutzen. Dazu gehören:

- Monitoring von Malware auf Endpunkten und Servern sowie von Änderungen der Systemkonfiguration
- Endpunkt- und Serverwachstellen sowie Patch-Verwaltung
- Verwaltung von Benutzerzugriff und -konten
- Monitoring der Webaktivitäten von Benutzern
- Monitoring des Netzwerkverkehrs

Jetzt können wir damit beginnen, Informationen wie das Risikoprofil der zu schützenden Systeme sowie relevanten Kontext rund um die Benutzeridentität einzubinden. Diese Informationen sind ein wichtiger Teil der Sicherheitsanalysen, da sie die Grundlage für die Risikobewertung und die Priorisierung von Sicherheitswarnmeldungen darstellen. Und da Sie bereits festgestellt haben, welche Assets und Entitäten geschützt werden müssen (siehe Phase 1), können Sie diese Informationen als weiteren Aspekt hinzufügen.

Beispiele für wichtige Kontextinformationen sind:

- **Risikoprofile des Assets:** Welche Auswirkungen für das Unternehmen hat ein Incident, der dieses Asset betrifft? Wie wahrscheinlich ist ein Incident, der dieses Asset betrifft? Wie ist die Sicherheitslage dieses Assets? Wie sensibel oder wichtig sind die Daten, die in diesem System verarbeitet werden bzw. enthalten sind? Welche Arten von Benutzern greifen in der Regel auf dieses System zu bzw. nutzen es?
- **Risikoprofile der Identität:** Wie wichtig ist diese Identität? Handelt es sich um ein Servicekonto, ein Verwaltungskonto, ein Benutzerkonto auf Führungsebene oder ein Vertragspartnerkonto? Handelt es sich um ein Konto mit einer hohen Wahrscheinlichkeit, Ziel von Angriffen zu werden, oder ist das Konto von Haus aus nicht vertrauenswürdig? Welche Auswirkungen hätte eine Kompromittierung dieser Identität? Ist dieser Benutzer abwanderungsgefährdet?

Das in Splunk ES integrierte Asset- und Identitäten-Framework ist ein integraler Bestandteil dieser Erkundungsphase und stellt die Grundlage der Risikobewertung dar. Für jedes in ES erfasste Asset bzw. jede Identität wird eine Aufzeichnung über einen Zeitraum erstellt, die auf Sicherheits-Events, ihrem Schweregrad und der Bedeutung des betreffenden Assets bzw. der Identität basiert. In der letzten Phase Ihrer Security Journey (fortgeschrittene Erkennung) werden wir diese Prinzipien bei der Einführung risikobasierter Warnmeldungen erneut anwenden.

Zu Datenquellen, die im Asset- und Identitäten-Framework erfasst, aggregiert und strukturiert werden, zählen:

- CMDBs (Configuration Management Databases)
- Tools für die Erkennung von Netzwerk-Assets
- Directory Services und Authentifizierungs-Services
- HR-Systeme
- Cloud-Umgebungen





Phase 3: Erweitern Ihrer Datenbasis

In den meisten Fällen werden komplexe Sicherheitsbedrohungen beim kontinuierlichen Monitoring von Sicherheitskontrollen nicht erkannt. Deshalb sollte beim Sicherheits-Monitoring berücksichtigt werden, wie die Zielsysteme funktionieren und wie eine autorisierte Nutzung aussieht. Außerdem muss für eine holistische Sicht auf Systeme, Daten und Benutzer gesorgt werden – mit Verhaltens- und Infrastruktur-Monitoring.

Warum? Weil Zero Trust Betrug, Insider-Bedrohungen oder komplexe Angriffe, die über autorisierte Wege erfolgen (z. B. durch ein kompromittiertes Benutzerkonto), nicht immer verhindern kann. Eine Zero Trust-Strategie *kann* jedoch, auch wenn ein Incident auftritt, den potenziellen Schaden eingrenzen. Sucht man aber an der falschen Stelle, werden solche Bedrohungen mit großer Wahrscheinlichkeit nicht rechtzeitig erkannt. Werden Zero Trust-Richtlinien und die Verhaltensweisen autorisierter Benutzer berücksichtigt, lassen sich Anomalien identifizieren, die Gegenstand von Monitoring sein *sollten*, um böswilligen Zugriff besser aufdecken zu können.

Mehr Daten = weniger Stress

Dies bedeutet, dass zusätzliche Datenquellen – und nicht nur Daten im Zusammenhang mit Sicherheitskontrollen – aufgenommen werden sollten, um für weitere Einblicke in das Benutzerverhalten zu sorgen. Ein Beispiel ist die Erfassung von Netzwerkverkehrsdaten zur Korrelation der Netzwerkaktivität mit der Anwendungs- und Prozessaktivität. Dies würde die Erkennung nicht autorisierter Anwendungen erleichtern, die autorisierte Netzwerkkommunikation nutzen, und könnte sogar dazu beitragen, Lateral Movement über mehrere Anwendungen und Benutzerkonten hinweg aufzudecken.

Selbst wenn man dank der Kontrollen und Richtlinien im Rahmen von Zero Trust über eine gute Monitoring-Abdeckung verfügt, sollte man trotzdem die Aktivitäten genau im Blick behalten, die autorisierte Benutzer und Systeme an den Tag legen, nachdem ihnen der Zugriff gewährt wurde. Wenn man nicht nur die Erkenntnisse aus den Sicherheitskontrollen betrachtet, kann dies in Situationen helfen, in denen Anmeldedaten kompromittiert oder Geräte entwendet wurden.

Die folgenden Datenquellen können zur Erkennung solcher Abweichungen im Benutzer- und Geräteverhalten beitragen:

- **Endpunkt:** Verschaffen Sie sich Klarheit in Bezug auf die Anwendungs- und Prozessausführung, das Monitoring der Dateiintegrität und Netzwerkverbindungen. Verwenden Sie dazu erweiterte EDR-Funktionen zur Endpunkterkennung und -behandlung oder Tools wie Sysmon und osquery.
- **Anwendung:** Beginnen Sie mit geschäftskritischen Anwendungen wie Finanzsystemen, Systemen zur Verarbeitung sensibler Daten, Kundendaten und Logs, die Benutzeraktivitäten aufzeichnen.
- **Datenbank:** Analysieren Sie Audit- und Transaktionslogs, um ungewöhnliche Verhaltensmuster, Änderungen oder Löschungen von Datensätzen und potenziell nicht autorisierten Zugriff auf sensible oder zugriffsbeschränkte Datensätze zu erkennen.
- **Cloud:** Hier liegt der Schwerpunkt hauptsächlich auf SaaS-Geschäftsanwendungen (Software as a Service) für das Benutzer-Monitoring. Es werden aber auch Umgebungen vom Typ IaaS (Infrastructure as a Service) und PaaS (Platform as a Service) berücksichtigt, um verdächtige Verwaltungsaktivitäten aufzudecken, die eventuell gegen Zero Trust-Richtlinien verstoßen.
- **Cloud-Speicherservices:** Hier werden Bewegungen sensibler Daten und ungewöhnliche Muster bei Datenbewegungen untersucht.

In Erweiterung der anfänglichen Erkennungs- und Monitoring-Maßnahmen aus Phase 2 können wir diese Use Cases mit fortschrittlicheren Erkennungen ausbauen, die durch in Phase 3 eingebundene Datenquellen möglich werden. Dies gilt für die von SSE bereitgestellten Use Cases sowie die Use Cases aus Splunk Enterprise Security und den [Enterprise Security Content Updates](#).

Analyseberichte

ESCU Use Cases werden als „Analyseberichte“ definiert, die den kompletten Incident- und Erkennungslebenszyklus unterstützen und eine Erläuterung zum Use Case, Details zu den Datenquellen sowie Suchvorgänge enthalten, die zur Erkennung und Untersuchung des Incidents beitragen.

Beispiele für Use Cases für Phase 3 sind:

- Lateral Movement
- Benutzerauthentifizierung oder -zugriff zu einer ungewöhnlichen Uhrzeit bzw. an einem ungewöhnlichen Ort
- Neuer Benutzerzugriff auf Systeme oder Anwendungen
- Neues Wechselmedium
- Erstellung eines neuen lokalen Kontos
- Interaktive Nutzung von Standard-, System- und Servicekonten
- Ungewöhnliche, seltene oder völlig unbekannte Prozesse/Anwendungen
- Ungewöhnliche Befehlszeilenaktivität (verschleierte Powershell)
- Ungewöhnliche oder seltene Nutzung von Cloud-Anwendungen (File Sharing)
- Endpunktänderungen und -status (Installation von Software, Änderung von Systemdateien)



Phase 4: Veredeln und Anreichern Ihrer Daten

In dieser Phase sehen wir uns Datenquellen an, die noch mehr Kontext liefern, wie z.B. Bedrohungsinformationen, Informationen aus Tools für die Schwachstellen- und Patch-Verwaltung sowie Lösungen für das Angriffsflächenmanagement.

Einschätzen der Bedrohungslandschaft

Bedrohungsinformationen helfen Ihnen, Kompromittierungsindikatoren (Indicators of Compromise, IOCs) innerhalb von Zero Trust-Kontrollen und geschützten Systemen zu identifizieren. Benutzer können auf diese Systeme in Echtzeit über das Splunk ES Threat Intelligence Framework oder als Teil eines Anreicherungs-Playbooks mit den Automatisierungsfunktionen von Splunk SOAR zugreifen.

Dies hilft uns, die Bedrohungslandschaft und ihre Beziehungen zu den von uns geschützten Systemen und Benutzern zu verstehen und bekannte IoCs zu identifizieren, die ansonsten von Zero Trust-Sicherheitskontrollen nicht entdeckt würden. Beispiele hierfür sind IP-Adressen, URLs oder Datei-Hashes im Zusammenhang mit Phishing-Aktivitäten oder Identifikationsdaten für ein SSL-Zertifikat, das bekanntermaßen für böswillige Zwecke genutzt wird.

Außerdem erleichtert es die Risikobewertung und Priorisierung von Security-Incidents sowie die Zugriffsautorisierung, wenn man den Status geschützter Assets – und auch der Systeme, die für den Zugriff auf diese Ressourcen genutzt werden – versteht. So besteht dann beispielsweise die Möglichkeit, den Zugriff für Benutzersysteme mit fehlenden oder ungenügenden System-Patches auf kritische Systeme einzuschränken und Sicherheits-Incidents im Zusammenhang mit bekannten Schwachstellen zu priorisieren.

Darüber hinaus können Lösungen für das Angriffsflächenmanagement das Sicherheitsniveau insgesamt verbessern, da dabei das Augenmerk besonders auf die Optimierung von Sicherheitskontrollen und die End-to-End-Transparenz gelegt wird. Wenn man weiß, dass es Lücken bei den Kontrollen gibt, kann man versuchen, diese zu schließen oder verbessertes Monitoring implementieren.

Alles in allem hilft die Veredelungsphase bei folgenden Aspekten:

- **Echtzeit-Bedrohungsinformationen:** Das Splunk Enterprise Security TI-Framework nimmt mehrere TI-Feeds auf und kuratiert sie (kommerziell und Open Source) und stützt sich auf Transportprotokolle wie STIX und TAXII. Diese Informationen werden anschließend genutzt, um IoCs übergreifend für verschiedene Zero Trust-Datenquellen abzugleichen und bekannte Bedrohungen proaktiv zu identifizieren.

Beispiele für typische Bedrohungsdaten-IoCs sind:

- IP-Adressen
- FQDN/URLs
- Dateinamen und Datei-Hashes
- SSL-Zertifikatsinformationen

- **Monitoring der Bedrohungslandschaft:** Das Splunk Enterprise Security TI-Framework bietet zudem Monitoring-Möglichkeiten, mit denen Sie die Bedrohungslandschaft und -trends speziell für Ihre Umgebung besser verstehen. Beim Bedrohungsdaten-Monitoring wird auf die Häufigkeit des Auftretens verschiedener Arten von Bedrohungen sowie IoCs innerhalb Ihrer Umgebung und verschiedenen Feeds geachtet.
- **Echtzeit-Sicherheitsniveau:** Splunk Enterprise Security und Splunk CIM bieten eine Reihe von Möglichkeiten für die Aufnahme und Auswertung von Daten aus Lösungen für die Schwachstellen- und Patch-Verwaltung. Mit diesen Daten kann eine unternehmensweite Sicht auf aggregierte Daten im Zusammenhang mit dem Sicherheitsniveau erstellt und zugleich Kontext für die Priorisierung von Security-Incidents bereitgestellt werden.

Phase 5: Fortgeschrittene Automatisierung und Orchestrierung

Wir haben jetzt ein tragfähiges Fundament für Monitoring-Aufgaben und Sicherheitserkennungen gelegt, das von drei Faktoren gestärkt wird: zentralisierten, normalisierten und veredelten Daten. Nun können wir uns der Untersuchung und Reaktion auf Incidents zuwenden.

Splunk SOAR setzt auf Orchestrierung und Automatisierung, um die Untersuchung und Behebung von Incidents zu rationalisieren und zu beschleunigen. Splunk SOAR nutzt Automatisierung, um Sicherheits-Incidents bei Zero Trust-Kontrollen schnell einzudämmen und zu beheben, und kann über erweiterte Playbooks oder einmalige Anfragen ausgeführt werden.

Wieder mehr PEP(P) im Alltag

Diese Playbooks basieren auf einer Entscheidungslogik, die je nach Kontext der erforderlichen Reaktion unterschiedliche Aktionen initiiert. Dadurch kann die erweiterte Richtlinienlogik auf den Zero Trust Policy Enforcement Point (PEP) und die Network Access Control (NAC) ausgeweitet werden. Dies beinhaltet auch die Echtzeit-Risikobewertung, was zu einer weiteren Verbesserung der Zero Trust-Autorisierung führt.

Splunk SOAR kann auch standardisierte Betriebsabläufe in Übereinstimmung mit branchenüblichen Frameworks wie **NIST 800-61** definieren, sodass Analysten den Incident-Typ, für den sie zuständig sind, mithilfe des zugehörigen Workbooks oder der Ticket-Vorlage verfolgen können. Dadurch können sich Analysten auf das konzentrieren, was sie am besten können: Daten interpretieren.

SOAR verleiht Ihren Daten Flügel

Ähnlich wie bei der stufenweisen Entwicklung zur Datenanalyse gehen wir auch bei **SOAR** in Phasen vor:

1. Zuerst identifizieren wir manuelle, sich wiederholende Aufgaben, die meist von Analysten durchgeführt werden. Hier bringt Automatisierung den größten Nutzen.
2. Analysieren und dokumentieren Sie den gesamten Prozess, einschließlich der verschiedenen technologischen Berührungspunkte, und erfassen Sie auch die Dauer der einzelnen Schritte. Der Prozess kann mit Splunk SOAR-Workbooks dokumentiert werden.
3. Erstellen Sie ein Prozessablaufdiagramm mit allen Schritten, für die Entscheidungen oder Genehmigungen notwendig sind. Das ist die Grundlage des Playbooks zur Automatisierung des Prozesses. Identifizieren Sie Prozessabschnitte, die sich für die Modularisierung eignen und als Teil-Playbooks wiederverwendet werden könnten.
4. Identifizieren, installieren und konfigurieren Sie Splunk SOAR-Anwendungen, um die Integration mit bestimmten Komponenten zu unterstützen.
5. Beginnen Sie mit der Umsetzung des in Workbooks definierten Prozesses. Untersuchen und beheben Sie Incidents und nutzen Sie alle Möglichkeiten mithilfe von Ad-hoc-Aktionen.
6. Erstellen und optimieren Sie ein Playbook, um nach und nach möglichst viele Teile des Prozesses zu automatisieren. Legen Sie dabei modulare Playbooks an, wenn die Möglichkeit zur Wiederverwendung besteht.
7. Prüfen Sie Playbooks und überwachen Sie die Analysten-Performance, um festzustellen, ob die Maßnahmen Erfolg hatten. Suchen Sie weitere Verbesserungsmöglichkeiten.

Einige Beispiele für Zero Trust-Anwendungsfälle für Splunk SOAR sind:

- Workbooks/Ticket-Vorlagen, die Incident-Untersuchungen und -Reaktionen im Zusammenhang mit Zero Trust definieren Hier einige Beispiele:
 - Konto-Kompromittierung
 - Sicherheitsverstoß
- Playbooks zur Automatisierung der Incident Response im Zusammenhang mit Zero Trust. Hier einige Beispiele:
 - Passwortrücksetzung oder Kontosperrung für Active Directory
 - Eindämmung und Reaktion auf kompromittierte E-Mails
 - Untersuchung und Reaktion bei Phishing-E-Mails
 - Schadensbegrenzung bei Geräteverlust/-diebstahl
 - Eindämmung von böswilligen Insidern
 - Eindämmung und Reaktion bei Malware
 - Eindämmung und Reaktion bei böswilligen Webressourcen

Es wird sogar noch besser. Analysten müssen sich nicht mehr direkt bei Zero Trust-Kontrollen anmelden. Splunk SOAR lässt sich in PAM-Lösungen (Privileged Access Management) integrieren, sodass Benutzer aus dem System heraus Maßnahmen ergreifen können.

Es gibt auch die Möglichkeit, eine erweiterte Autorisierungsebene zu implementieren, die über die PEP/NAC-Lösungen im Rahmen von Zero Trust hinausgeht. Wenn wir uns die Risikolage und -bewertung in Echtzeit ansehen, können wir noch mehr Informationen auswerten, bevor wir den Benutzerzugriff gestatten, und haben damit die Möglichkeit, die Kontrollen herkömmlicher Zero Trust-Richtlinien für Zugriff und Autorisierung noch auszubauen. Dadurch können wir die Risikowertungen sowohl für den Benutzer *als auch* für das System, auf das er zuzugreifen versucht, kombinieren und beurteilen und damit das Risikoprofil des betreffenden Endpunkts besser verstehen.

Automatisieren manueller SOC-Aufgaben

Während (und sogar nach) der Autorisierungsphase kann Splunk SOAR dazu verwendet werden, das Risikoprofil von Assets und Identitäten in Splunk ES zu bewerten und festzustellen, ob der Zugriff gewährt oder entzogen werden sollte oder ob sonstige Maßnahmen notwendig sind. Diese Informationen können dann für die NAC- oder Richtlinien-Engine von Zero Trust freigegeben und genutzt werden, um Zugriff zu gewähren, zu verwehren oder zu entziehen. Wird der Zugriff verwehrt, kann Splunk SOAR weitere Maßnahmen ergreifen, die davon abhängen, aus welchem Grund der Zugriff verwehrt wird.

Hier einige Beispiele:

- Der Benutzerzugriff wird verwehrt und eine Warnmeldung wegen einer erhöhten Risikobewertung wird übermittelt.
- Der Benutzerzugriff wird eingeschränkt, wenn der Benutzer nach der anfänglichen Autorisierung ein ungewöhnliches oder riskantes Verhalten zeigt.
- Initiieren von Schwachstellen- oder Bestands-Scans für Assets, bei denen nach der Autorisierung ungewöhnliches Verhalten festzustellen war.
- Automatische Erstellung von IT-Support-Tickets für Systeme, die die Compliance nicht einhalten, wenn der Zugriff verwehrt wurde.
- Automatische Erledigung von Aktivitäten wie Patching, Deaktivieren nicht autorisierter Software/Services oder (erneutes) Anwenden von Sicherheitskontrollen.



Phase 6: Advanced Threat Detection

Nun sind wir endlich bei der letzten Phase der Einrichtung einer Zero Trust-Architektur angelangt. Wir werden jetzt fortgeschrittene Sicherheitserkennungen mit **risikobasierten Warnmeldungen** (Risk Based Alerting, RBA) definieren. Dies trägt dazu bei, dass die Bedrohungen in Ihrer Warteschlange wirklich glaubwürdig sind, und minimiert die Gesamtzahl der Warnmeldungen. Außerdem können wir damit beginnen, die Möglichkeiten von Splunk Enterprise Security mit **Splunk UEBA** zu erweitern.

Es gilt folgende Aspekte zu berücksichtigen: 1. Die Richtlinien im Zusammenhang mit Zero Trust 2. Wie Benutzer die Systeme, auf die sie Zugriff haben, normalerweise nutzen, und 3. Wie man Verhaltensmuster identifiziert, die auf ungewöhnliche oder böswillige Aktivitäten hindeuten könnten.

Zuerst müssen Sie auf den früheren Erkennungs-Anwendungsfälle aufbauen, damit Sie sich die verschiedenen Phasen eines Security-Incidents (also die Kill Chain) ansehen und verschiedene Hinweise auf verdächtige Aktivitäten nutzen können, um Warnmeldungen zu erzeugen.

Risk Based Alerting als Retter in der Not

Bei risikobasierten Warnmeldungen wird nicht beim ersten Anzeigen einer potenziellen Bedrohung eine Benachrichtigung generiert, sondern es wird nur das Ereignis aufgezeichnet. Nach der Protokollierung werden weitere Hinweise auf böswillige Aktivitäten erfasst. Das heißt, wir können jetzt die Abfolge bzw. das Muster der Events in Bezug auf das betreffende Asset oder die Identität übersichtlich zusammengefasst in einer einzelnen Warnmeldung sehen.

Im folgenden Beispiel kann man erkennen, wie der Datenexfiltration eine Reihe ungewöhnlicher Events vorausging. Vor dem Einsatz von risikobasierten Warnmeldungen wäre für jedes Event eine eigene Benachrichtigung erzeugt worden, die (höchstwahrscheinlich) irgendwo im Getümmel untergegangen wäre. Dadurch, dass wir die Kill Chain überblicken und mehrere Hinweise nutzen, können wir eine einzelne Benachrichtigung mit großer Glaubwürdigkeit generieren.

Risk Based Alerting für Zero Trust

Mehrere mit Zero Trust zusammenhängende Events werden als Kontext für High-Fidelity-Warnmeldungen herangezogen



Außerdem können wir fortschrittlichere Risikobewertungsfunktionen einrichten, die bei der Priorisierung von Warnmeldungen noch tiefer gehen. Beim standardmäßigen Risikobewertungs-Framework für Splunk ES wird beispielsweise die Bedeutung des Assets bzw. der Identität betrachtet und auch der Schweregrad der Benachrichtigung berücksichtigt, um die laufende Risikobewertung zu ermitteln.

Beim Risk Based Alerting können wir weitere Dimensionsebenen einbeziehen, um Zero Trust umzusetzen. Beispiele für relevante Use Cases sind:

- Verfahren, die mehrere Zero Trust MITRE-Taktiken in einem Zeitraum von 24 Stunden beinhalten
- Mehrere Zero Trust MITRE-Verfahren im Rahmen einer einzelnen Taktik in einem Zeitraum von 24 Stunden

Obwohl sich die operativen Prozesse von RBA und UEBA unterscheiden, ähneln sie sich darin, dass mehrere Indikatoren für die Erkennung verdächtiger oder böswilliger Aktivitäten genutzt werden. Dank der vielen Referenzpunkte, die diese Tools heranziehen, sind sie besser darin, Warnmeldungen mit höherer Glaubwürdigkeit zu generieren und die Zahl der False Positive-Meldungen zu reduzieren.

UEBA (User and Entity Behavior Analytics)

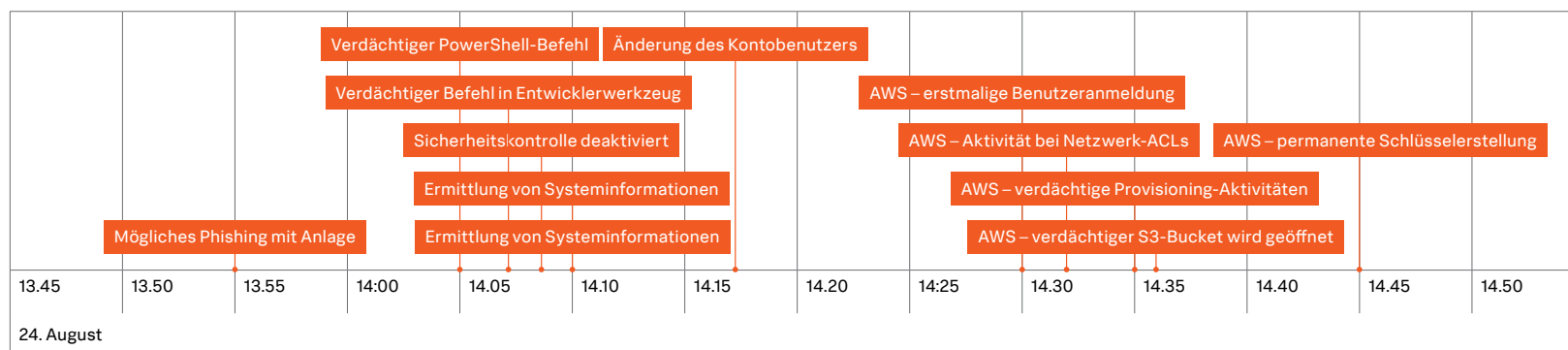
Durch Unsupervised Machine Learning erleichtert es Splunk UEBA, Abweichungen bei Benutzeraktivitäten, Geräten und Anwendungen zu erkennen. Oftmals sind diese Events harmlos (und dennoch ungewöhnlich). Doch mit einem ähnlichen Ansatz wie RBA sucht UEBA nach Mustern und Abfolgen, die den verschiedenen Phasen eines Security-Incidents zugeordnet werden können, und gruppiert diese anomalen Events automatisch in einer einzelnen Warnmeldung oder Bedrohung.

Wie bei RBA erhöht dies die Glaubwürdigkeit der Warnmeldung und vereinfacht gleichzeitig Analysten die Aufgabe, die zugehörigen Events manuell zu identifizieren. Neben der Verhaltensanalyse tragen die von Splunk UEBA bereitgestellten Funktionen zudem zur Kontextanreicherung bei und ermöglichen, die Benutzeraktivität den Systemen und Daten zuzuordnen, auf die zugegriffen wurde.

Beispiele für einen verhaltensbasierten Zero Trust-Ansatz (bei Insider- und komplexen Bedrohungen) sind:

- Datenexfiltration durch ein kompromittiertes Benutzerkonto
- Datenexfiltration durch einen internen Akteur oder abwanderungsgefährdeten Benutzer
- Erkennung von komplexem Lateral Movement
- Komplexe Rechteausweitung (Privilege Escalation)

Ansicht der Zero Trust-Bedrohungszeitachse bei RBA



Zero Trust erfordert einen „Ökosystem-Ansatz“

Für die Umsetzung einer umfassenden Zero Trust-Strategie ist eine Reihe integrierter Komponenten notwendig. Zusammen liefern diese Kontrollen die notwendigen Daten und Erkenntnisse für ein zentralisiertes Monitoring.

Durch die Ausrichtung der Zero Trust-Methoden auf Splunks Partner-Ökosystem können wir die Sicherheitslage der Unternehmen und ihrer gesamten Sicherheitsprozesse dramatisch verbessern.

Im Folgenden stellen wir Ihnen die Möglichkeiten unserer Zero Trust-Partner vor und erläutern, wie diese Sie beim Erreichen Ihrer Zero Trust-Ziele unterstützen können.





Zscaler

Zscaler, einer unserer wichtigsten strategischen Partner, ist ein führender Anbieter und Innovator im Security-Bereich, der Benutzer sicher mit dem Internet und einer Vielzahl privater Anwendungen verbindet. Die Zero Trust Exchange von Zscaler ist eine Cloud-native Proxy-Architektur, die Benutzer und Anwendungen direkt mit Unternehmensressourcen verbindet, ohne dass zusätzliche, unerwünschte Angriffspunkte entstehen. Zscaler ergänzt diese Architektur mit der Security Sockets Layer-Prüfung (SSL), starker Authentifizierung und umfassenden richtlinienbasierten Kontrollen.

Zwei der wichtigsten Zero Trust-Lösungen von Zscaler:

Zscaler Internet Access (ZIA) bietet umfassende Sicherheit für den Internetzugriff von Benutzern, und zwar völlig unabhängig von ihrem Standort. Dieser Zscaler-Service wird mit 150 Rechenzentren auf der ganzen Welt bereitgestellt und bietet Benutzern eine schnelle, sichere und problemlose Nutzungserfahrung.

Zscaler Private Access (ZPA) unterstützt nahtlosen Zugriff nach dem Prinzip der geringsten Rechte auf herkömmliche und Cloud-basierte Anwendungen für lokale und Remote-Benutzer – ganz ohne die Komplexität, die sich aus der traditionellen Netzwerksegmentierung und den Lösungen für den Remote-Zugriff ergibt. Die Angriffsfläche von Anwendungen wird deutlich verkleinert, da sie für öffentliche Kanäle nicht sichtbar sind.

Splunk nimmt die zuverlässigen Telemetriedaten von Zscaler mit einer out-of-the-box einsetzbaren Cloud-to-Cloud-Integration auf und gibt damit Security-Teams Einblick in den Cloud- und Netzwerkdatenverkehr, wodurch sie neue Bedrohungen im gesamten Unternehmen besser erkennen und abwehren können. Die Zscaler-API ermöglicht es Sicherheitsanalysten zudem, mithilfe von Splunk SOAR koordinierte Maßnahmen über die Zscaler-Plattform und andere Sicherheitstools zu ergreifen, um den Benutzerzugriff und das Richtlinienmanagement über ein in Splunkbase verfügbares [Anwendungs- und Technologie-Add-On](#) zu orchestrieren.

DTEX-Systeme

DTEX ist die erste und einzige Workforce Cyber Intelligence Plattform. Sie erfasst endpunktübergreifende Verhaltenstelemetrie, erzeugt daraus dynamische „Absichtsindikatoren“ und bietet damit ganzheitliche Echtzeiteinblicke in die Aktivitäten des Unternehmens – ohne gegen den Datenschutz zu verstoßen.

Dank komplexer Scoring-Frameworks kann DTEX Ihnen helfen, kontextbezogene Informationen zu erkennen, zu verstehen und als Grundlage für Handlungen zu nutzen. Damit haben Sie und Ihr Unternehmen mehr Möglichkeiten, Insider-Bedrohungen zu stoppen, Datenverlust zu verhindern, den Nutzen von Softwareinvestitionen zu maximieren und Ihre Mitarbeiter zu schützen. Sichtbarkeit in diesem Maß ist für die Erkennung komplexer Insider- und externer Bedrohungen unerlässlich und liefert zudem eine umfassende Datenquelle für die Erkennung von Verhaltensanomalien.

Wenn Sie die Implementierung Ihrer fortgeschrittenen Sicherheitserkennungs- und Monitoring-Use Cases für Zero Trust verbessern möchten, sehen Sie sich am besten die [DTEX-Splunk-Integration in Splunkbase](#) an, die als Anwendungs-Add-On bereitgestellt wird.

CloudKnox

Die vielen neuen Identitäten und Richtlinien bei Cloud-nativen Services machen es immer schwieriger, verschiedene Benutzertypen und ihren Zugriff zu verwalten und zu sichern. Momentan klafft eine riesige Lücke zwischen den gewährten und den genutzten Berechtigungen, denn die meisten Identitäten nutzen weniger als 5 % der Berechtigungen mit hohem Risiko. Das bedeutet, dass es viel schwieriger geworden ist, Richtlinien nach dem Prinzip der geringsten Rechte durchzusetzen, wodurch Unternehmen einem hohen Risiko ausgesetzt werden und eine angemessene Verwaltung des Zero Trust-Zugriffs im Prinzip unmöglich wird.

Das bringt uns zu CloudKnox und seiner Permissions Management-Plattform: Diese Plattform für das Management und Monitoring von Berechtigungen in Multi-Cloud/Hybrid-Cloud-Umgebungen schützt kritische Cloud-Infrastrukturressourcen und -identitäten, indem sie für umfassende Sichtbarkeit, automatisierte Korrekturmaßnahmen und ein kontinuierliches Monitoring von Berechtigungen sorgt. Mit der von CloudKnox patentierten „Activity Based Authorization“-Technologie ermöglicht die CloudKnox-Plattform Unternehmen, Zero Trust-Richtlinien mit einem einzigen Betriebsmodell Cloud-übergreifend zu implementieren. CloudKnox unterstützt VMware vSphere (sowohl lokal als auch in der Cloud), AWS, Azure und GCP.

CloudKnox ist ein Splunk-Partner für strategische Sicherheit gemäß Zero Trust. Die Unterstützung erfolgt über das [in Splunkbase verfügbare Add-On](#). Die CloudKnox Permissions Management-Plattform wurde weltweit bereits bei vielen Unternehmen, darunter zahlreiche Fortune 500-Unternehmen, bereitgestellt und mit Splunk integriert.

Okta

Okta ist eine Cloud-native, vertrauenswürdige Plattform für den Schutz jeder Identität, vom Kunden bis zum Mitarbeiter. In Bezug auf die Anmeldung, Autorisierung und Verwaltung des Benutzerzugriffs auf wichtige Anwendungen und Daten in hybriden Architekturen vertrauen mehr als 10.000 Unternehmen auf Identitätslösungen von Okta und unterstützen damit einen wichtigen Aspekt eines umfassenden Zero Trust-Ansatzes. Die Authentifizierungs- und Autorisierungsdaten stellen zusammen mit dem Kontext der Identitäten von Okta eine umfassende Informationsquelle dar, die das notwendige Sicherheits-Monitoring im Rahmen von Zero Trust mit dem Splunk-Ansatz unterstützt. Durch die bestehende Integration mit Splunk – [ermöglicht durch das Okta-Add-On in Splunkbase](#) – können Kunden ihre Daten zur Unterstützung von Zero Trust-Zielsetzungen schnell einbinden und nutzen.

Illumio

Mit seinem branchenführenden Ansatz hat Illumio die Security-Landschaft transformiert, indem es Unternehmen hilft, eine Map mit ihren Anwendungen, Verbindungsmöglichkeiten, Endpunkten und Workloads zu erstellen und damit die für Zero Trust notwendige Mikrosegmentierung zu implementieren, sodass übergreifend über alle Cloud-, Hybrid-, Multi-Cloud- und On-Premises-Systemen nur vertrauenswürdige Kommunikation stattfindet. Entdecken Sie Illumios breit gefächerte Zero Trust-Funktionen wie etwa die umfassende Netzwerksicherheitstelemetrie, indem Sie die [Illumio-App](#) aus der Splunkbase herunterladen. Die Anwendung bietet fortgeschrittene Monitoring- und Reporting-Möglichkeiten für die Unterstützung von IT-, Sicherheits- und Compliance-Teams und beinhaltet die erweiterte Sichtbarkeit des gesamten Anwendungsverkehrs in Splunk, damit Sie verdächtige Workloads blitzschnell mit einem einzigen Klick isolieren können.

Ihr Zero Trust-Ökosystem in Aktion:

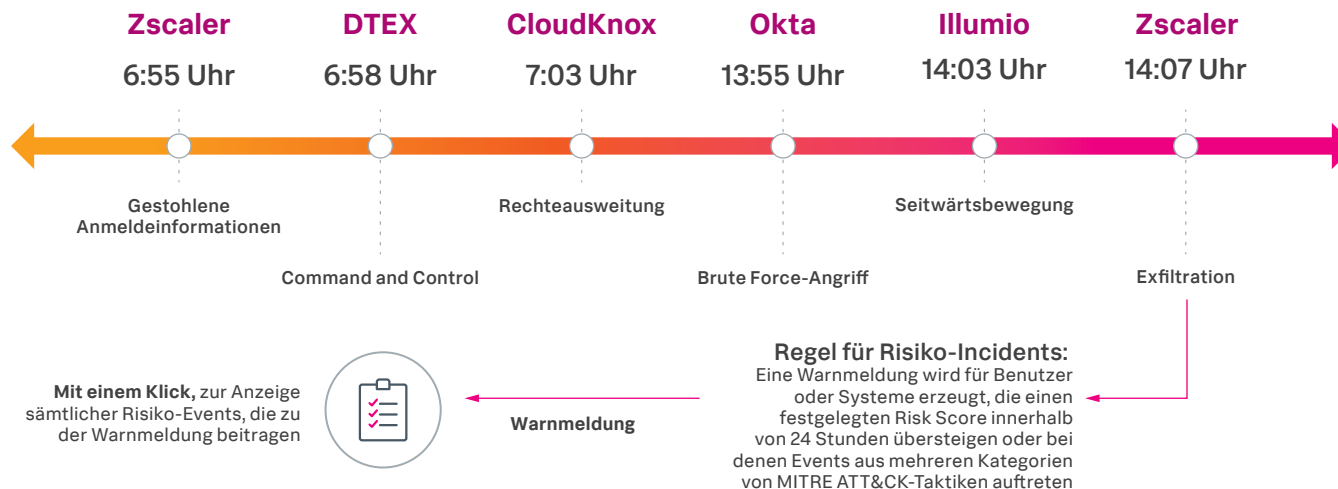
Wenn wir die MITRE ATT&CK-Kategorien betrachten, die wir Ihnen hier vorgestellt haben, und zusätzlich die vielen unterschiedlichen Phasen Ihrer Security Journey berücksichtigen, wird deutlich, wie die hier beschriebenen Zero Trust-Technologien die einzelnen Use Cases unterstützen. Das folgende Diagramm zeigt ein praktisches Beispiel für die Möglichkeiten dieses kombinierten Ansatzes. Jede dieser Partnerlösungen bietet eine breite Abdeckung, um die Erkennung mithilfe dieser mit Zero Trust zusammenhängenden MITRE ATT&CK-Taktiken zu unterstützen, und kann für noch mehr Sichtbarkeit mit anderen Datenquellen kombiniert werden.

- **Erstzugriff:** Zscaler Private Access bietet die nötige Telemetrie zur Erkennung von verdächtigem oder anormalem Zugriff auf geschützte Anwendungen, für den eventuell gültige Anmeldedaten gestohlen oder entwendet wurden.
- **Persistenz (Persistence):** Die detaillierten Endpunktdaten von DTEX erleichtern die Erkennung der unnachgiebigen Verfahren, mit denen Angreifer bei Command & Control-Angriffen versuchen, Fuß zu fassen.

- **Rechteauserweiterung:** Mit den fortgeschrittenen Monitoring-Möglichkeiten von CloudKnox können wir Änderungen an Administrator- oder Entwicklerberechtigungen in Hybrid-Cloud-Umgebungen erkennen, wie z. B. die anomale Verwendung gültiger Administrator-Anmeldeinformationen.
- **Zugriff mit Anmeldeinformationen:** Okta stellt detaillierte Authentifizierungs- und Autorisierungsdaten bereit, mit denen Splunk anomale Aktivitäten aufspüren kann, die Anzeichen für verdächtigen Zugriff mit Anmeldeinformationen wie bei Brute Force-Angriffen sein könnten.
- **Laterale Bewegungen:** Mit dem Illumio-Ansatz für Mikrosegmentierung, der für detaillierte Sichtbarkeit bei der Netzwerkaktivität innerhalb einer hybriden Umgebung sorgt, können wir versuchte und erfolgreiche Seitwärtsbewegungsverfahren erkennen.
- **Exfiltration:** Zscaler Internet Access unterstützt das Monitoring von Webaktivitäten. Dies ermöglicht die Anomalieerkennung mit Splunk, um mögliche Datenexfiltration über eine breite Palette von Web-Services hinweg aufzuspüren.

Übersicht über das Spektrum an MITRE ATT&CK-Taktiken

Warnmeldungen mit mehreren Quellen, mehreren Indikatoren und hoher Glaubwürdigkeit für Zero Trust mit RBA



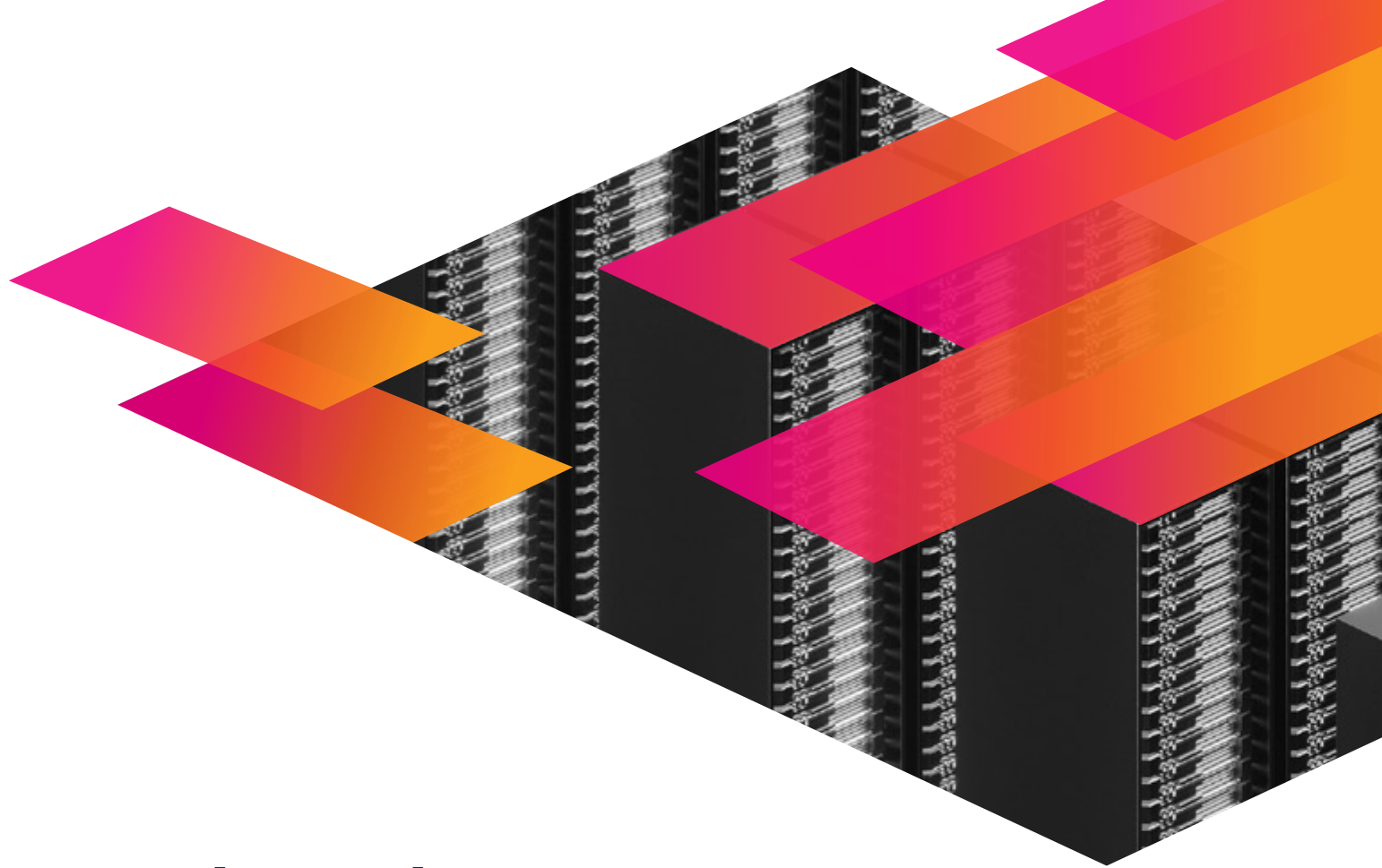
Ein datenzentrierter Ansatz für Zero Trust

Damit sind wir am Ende unseres Weges zu Zero Trust angekommen. Den folgenden, äußerst wichtigen Punkt sollten Sie immer im Hinterkopf behalten: Ein datenzentrierter Sicherheitsansatz hat jede Menge Vorteile, ganz besonders beim Aufbau einer Zero Trust-Architektur.

Daten sind der Mittelpunkt jeder erfolgreichen Strategie, vor allem aber einer jeden erfolgreichen *Sicherheitsstrategie*. Viel zu oft führen die Systeme und Strukturen, auf die wir uns verlassen, dazu, dass unsere Daten abgeschottet oder segmentiert werden, was es deutlich schwieriger macht, ihren immensen Wert zu nutzen.

Und die gute Nachricht? Sie können diese Hindernisse beseitigen und von den in den Daten verborgenen Schätzen an Erkenntnissen und Möglichkeiten profitieren. Das gelingt mithilfe von Datenanalysen in Kombination mit einem echten Verständnis der Zero Trust-Richtlinien, -Rollen und -Ressourcen Ihres Unternehmens. Dank der Flexibilität und offenen Ausrichtung des Splunk-Portfolios können Teams jetzt separate Technologien verknüpfen und präzise Maßnahmen ergreifen. Dies führt zu besseren, schnelleren und effektiveren Entscheidungen im gesamten Unternehmen und letztlich auch zu einer robusten Zero Trust-Strategie.





Von Splunk Zero zum (Splunk) Hero

Unabhängig davon, wo Sie sich auf Ihrer Zero-Trust-Journey befinden, kann Splunk Ihnen helfen, neuen und alten Bedrohungen stets einen Schritt voraus zu sein. Erfahren Sie, wie Sie Ihren Sicherheitsbetrieb modernisieren und das Sicherheitsniveau Ihres Unternehmens verbessern können, indem Sie [Splunk Security Essentials](#) noch heute herunterladen.

Splunk, Splunk>, Data-to-Everything, D2E und Turn Data Into Doing sind Marken und eingetragene Marken von Splunk Inc. in den Vereinigten Staaten und anderen Ländern. Alle anderen Markennamen, Produktnamen oder Marken gehören den entsprechenden Inhabern. © 2021 Splunk Inc. Alle Rechte vorbehalten.21-18251-Splunk-The Essential Guide to Zero Trust-EB-109_DE

splunk>
turn data into doing™