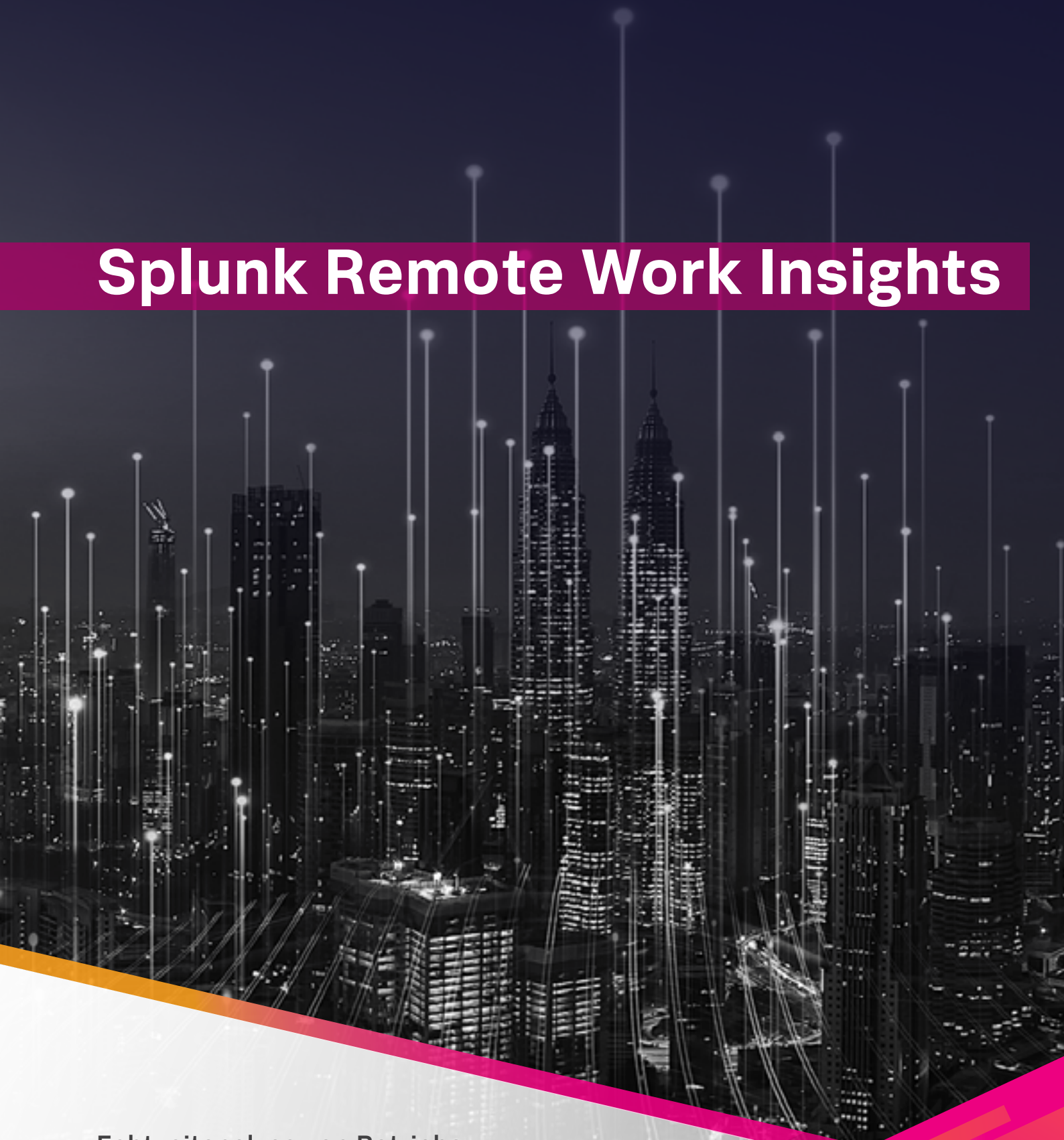
SOLUTION GUIDE

Splunk Remote Work Insights



Echtzeitanalyse von Betriebs- und Sicherheitsdaten bei Remote-Zugriff in der Cloud

splunk>
turn data into doing™

Zugriffsmöglichkeiten für Remote-Arbeit

Da immer mehr Unternehmen ihren Mitarbeitern die Möglichkeit geben, von zu Hause aus zu arbeiten, werden Remote-Systeme zunehmend erfolgskritisch. Auch Performance-Optimierung und das Eindämmen von Sicherheitsrisiken sind wichtiger als je zuvor.

Splunk bietet Bestands- und Neukunden, die auf der Suche nach besseren Monitoring- und Security-Möglichkeiten in Zeiten erhöhter Remote-Arbeit sind, ein kostenloses Programm namens Remote Work Insights. Dieses Programm liefert die Grundlage, auf der aussagekräftige Erkenntnisse schnell und skalierbar über das gesamte Unternehmen hinweg gewonnen und bereitgestellt werden können.

Zusammen mit Remote Work Insights erhalten teilnehmende Kunden eine kostenlose Splunk Cloud[1]-Instanz für einen festgelegten Zeitraum (in der Regel 90 Tage). In Zusammenarbeit mit Splunk integrieren Sie Ihre Daten und implementieren Best Practices für ausgewählte Use Cases. Zusätzlich ermöglicht Ihnen Splunk, wichtige Leistungsindikatoren (KPIs) zu überwachen, entstehende Probleme zu identifizieren und tiefgreifende Kernursachenanalysen über eine repräsentative Teilmenge Ihrer Gesamtumgebung hinweg durchzuführen – und all dies über eine einzige Plattform.

1. Weitere Informationen zu Splunk Cloud im Allgemeinen finden Sie auf dieser **Webseite**.

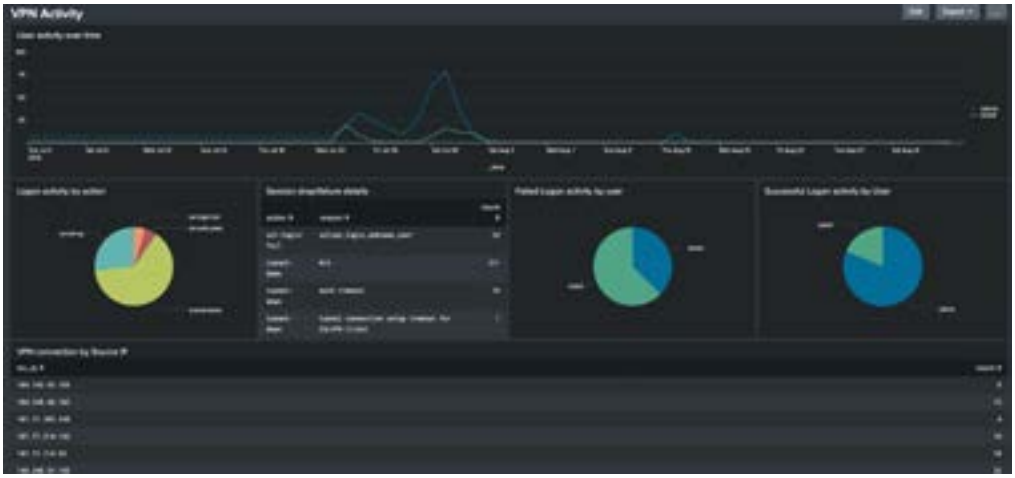
Remote Work Insights ist ein Programm, das:

- Ihre Herausforderungen im Unternehmen versteht und quantifiziert
- wichtige, für Ihr Unternehmen relevante Anwendungsfälle identifiziert
- Splunkbase-Apps und -Add-Ons pflegt, die zur Erfüllung der ausgewählten Use Cases notwendig sind

Use Cases, die Remote Work Insights unterstützt

Monitoring von Remote Access VPNs

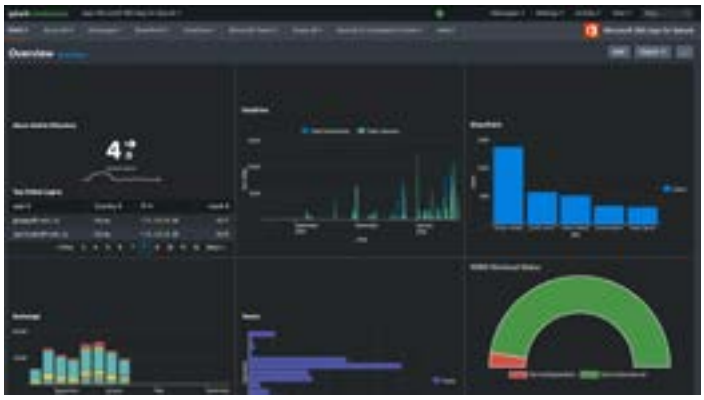
Da immer mehr Mitarbeiter im Home-Office arbeiten, sehen sich Unternehmen mit steigenden Performance-Anforderungen konfrontiert. Das Monitoring von Remote Access VPNs versetzt Benutzer in die Lage, ihre Arbeitsumgebungen besser zu überwachen, zu schützen und Fehler zu beheben, da sie Erkenntnisse gewinnen, die von Performance-Problemen bis zur Anwendungsnutzung reichen.



Beispiel-Dashboard für Echtzeiteinblicke in VPN-Aktivitäten

Remote-Zugriff: Monitoring der Microsoft 365-Zusammenarbeit

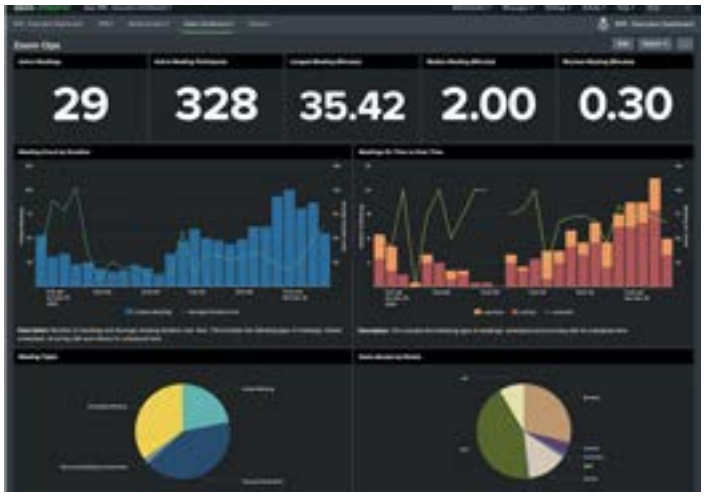
Da mehr Mitarbeiter von zu Hause aus arbeiten, beobachten Unternehmen eine zunehmende Belastung und sogar Ausfälle bei ihren Tools für Remote-Zugriff und Zusammenarbeit. Und mit der wachsenden Abhängigkeit von Kommunikations- und Kollaborationslösungen wie Microsoft 365 wirken sich die gefürchteten Ausfälle stärker denn je aus. Unternehmen, die Produktivität und konsistente Service Delivery im Rahmen verbindlicher SLAs aufrechterhalten wollen, müssen in der Lage sein, die Service-Performance zu überwachen, Incidents zu untersuchen und diese Daten mit Cloud-Servicedaten zu korrelieren. Remote Work Insights macht dies mit Monitoring-Features für Microsoft 365 möglich.



Beispiel-Dashboard für Echtzeiteinblicke in Microsoft 365-Aktivitäten

Videokonferenzen

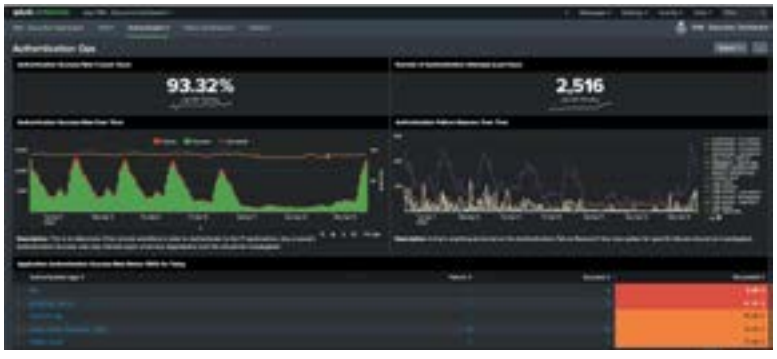
Durch die derzeitige Zunahme von Remote-Arbeit ist die Nutzung von Videokonferenzlösungen extrem in die Höhe geschnellt – was die Belastung bereits ausgelasteter IT Operations-Teams nur noch weiter verstärkt. IT-Teams müssen daher nun zunehmend Probleme im Zusammenhang mit Videokonferenzlösungen von Drittanbietern beheben. Remote Work Insights bietet Transparenz bei Problemen, die sich auf die Audio- und Videoleistung sowie -qualität von Zoom-Meetings, -Webinaren und Zoom Rooms auswirken.



Beispiel-Dashboard für Echtzeiteinblicke in Video Conferencing-Aktivitäten mit Zoom

Authentifizierung

Ähnlich wie beim Monitoring von Remote Access VPNs kann die Anzeige von Authentifizierungsdaten Einblicke in wichtige IT Operations-Probleme bieten, wie etwa gleichzeitige Verbindungen oder Benutzerzahlen, aktive Benutzer im System, Bandbreitennutzung und Service-Probleme, die sich in fehlgeschlagenen oder abgebrochenen Anmeldungen und Sitzungen widerspiegeln. Zu den von Remote Work Insights unterstützten Authentifizierungsservices zählen Okta, Duo, Sailpoint und Windows.



Beispiel-Dashboard für Echtzeiteinblicke in Authentifizierung-Aktivitäten

Splunk hat eine Liste wichtiger Prozesse und Security Use Cases erstellt. Bitte kreuzen Sie die Punkte an, die für Sie und Ihr Unternehmen besonders interessant sind. Unternehmen können mehr als einen Anwendungsfall auswählen, die Zahl ist zu Anfang jedoch auf drei Use Cases beschränkt. Sie werden dann zusammen mit Ihrem Account-Team die am besten geeignete, weitere Vorgehensweise bestimmen.

Use Case 1
Monitoring von Remote Access VPNs

Zielgeräte	Datenquellen (wählen Sie max. 2)
VPN-Gateways oder -Clients	☐ Cisco AnyConnect ☐ Palo Alto Networks GlobalProtect ☐ Fortinet Forticlient ☐ Check Point SecuRemote, SecuClient, Endpoint Security, SSL VPN ☐ Zscaler ZPA, ZPI
Technische Erfolgskriterien	☐ Wie viele Personen sind mit dem VPN verbunden? Verteilung über die Zeit? Gesamtbenutzerzahl? ☐ Standort – von wo aus verbinden sich die Benutzer? ☐ Fehler ☐ Gleichzeitige Benutzer zu einem beliebigen Zeitpunkt ☐ Mit dem VPN verbundene Gerätetypen ☐ Wer kann sich nicht mit dem VPN verbinden? (d. h. fehlgeschlagene oder nicht durchgeführte Versuche) ☐ Brechen Verbindungen ab? ☐ Auf welche Anwendungen wird zugegriffen?

Use Case 2
Sicherheitsniveau von Remote Access VPNs

Zielgeräte	Datenquellen (wählen Sie max. 2)
VPN-Gateways oder -Clients	☐ Cisco AnyConnect ☐ Palo Alto Networks GlobalProtect ☐ Fortinet Forticlient ☐ Check Point SecuRemote, SecuClient, Endpoint Security, SSL VPN ☐ Zscaler ZPA, ZPI
Security Detection und Response Use Case	☐ Erfolgreiche Anmeldungen aus ungewöhnlichen/unerwarteten Ländern ☐ Geografisch unwahrscheinlicher Zugriff ☐ Password Spraying ☐ Mehrere gleichzeitige Anmeldungen ☐ VPN-Verbindung von nicht unterstütztem Gerät ☐ Authentifizierung von TOR oder einer verdächtigen Domäne ☐ Sichtbarkeit/Verfügbarkeit von SMB/UPnP/Bonjour-Geräten im VPN-Subnetz

Use Case 3

Remote-Zugriff: Monitoring von Microsoft 365

Die Microsoft 365 App bietet mehrere out-of-the-box Dashboards. Bitte wählen Sie für Sie interessante Optionen aus.	
☐ Azure Active Directory ☐ User Audit-Dashboard ☐ Exchange ☐ SharePoint ☐ OneDrive ☐ Microsoft Teams ☐ Power BI	Die Datenquelle für diesen Use Case wird durch die Bereitstellung des Microsoft 365 Technology Add-On unterstützt. Dies beinhaltet auch eine umfassende, schrittweise Anleitung für die Datenintegration.

Use Case 4

Remote-Zugriff: Monitoring des Sicherheitsniveaus für Microsoft 365-Umgebungen

Microsoft 365-Zieldatenquellen	Security Detection und Response Use Case
Managementdaten	☐ BCC-Regeln für neu hinzugefügte Organisationen ☐ Erstellung einer Regel für die E-Mail-Weiterleitung ☐ Export von PSTs ☐ Hinzufügen von Berechtigungen für Postfächer ☐ Erstellung eines neuen Administratorkontos ☐ Freigabe von OneDrive-Dateien ☐ Downloads von OneDrive
Azure Active Directory	☐ Erfolgreiche Anmeldungen aus ungewöhnlichen/unerwarteten Ländern ☐ Geografisch unwahrscheinlicher Zugriff ☐ Password Spraying ☐ Mehrere gleichzeitige Anmeldungen ☐ Anmeldungen von Benutzern aus externen Organisationen ☐ Anmeldeversuche von abgelaufenem/deaktiviertem Account
Message Trace Logs	☐ Anomaler Anstieg bei E-Mails zur Passwortrücksetzung ☐ E-Mails mit Pandemie-bezogenem Betreff ☐ E-Mails von bekanntermaßen böswilligen Domänen ☐ E-Mails von Doppelgänger-Domänen ☐ E-Mail von außerhalb des Unternehmens mit Unternehmensdomänen

Use Case 5
Security Monitoring und Response für Authentifizierungsprotokolle

Ziel: Authentifizierungs-datenquelle	Security Detection und Response Use Case
Beliebige Datenquelle mit geografischer Zuordnung (IP-Adresse oder Ähnliches)	☐ Geografisch unwahrscheinlicher Zugriff erkannt ☐ Anmeldungen aus ungewöhnlichen Ländern/Regionen ☐ Mehrere Anmeldungen von einem Standort/einer IP ☐ Anmeldeversuche bei mehreren Konten von einem einzelnen Ursprung (Password Spraying)
Beliebige Datenquelle (zu den gängigen gehören Okta, Duo, Ping, Windows Security, Azure AD, klassisches AD)	☐ Neue interaktive Anmeldung von einem Service-Account ☐ Nicht autorisierter Benutzer ist bei Compliance-relevantem ☐ System angemeldet ☐ Übermäßig hohe Zahl an Benutzeraccount-Sperren ☐ Aktivität unter einer abgelaufenen Benutzeridentität ☐ Aktivität unter einer lange inaktiven Identität ☐ Neuer Benutzer, der Handlungen durchführt, für die spezielle ☐ Berechtigungen notwendig sind ☐ Erstellung/Änderung/Hinzufügen von Benutzern zu privilegierter ☐ Gruppe prüfen ☐ Standardmäßige Accountaktivität erkannt ☐ Ungewöhnlicher Anwendungszugriff für Benutzer/Rolle ☐ Ungewöhnlich viele fehlgeschlagene Anmeldungen ☐ Gleichzeitige Anmeldeversuche erkannt ☐ Erfolgreiche Anmeldungen von neuem Gerät ☐ Erstmalige Anmeldung bei neuem Server ☐ Erstmalige Anmeldung bei Jump-Server ☐ Anstieg der Host-Zahlen, bei denen die Anmeldung über Benutzer erfolgte
Beliebige Datenquelle (zu den gängigen gehören Okta, Duo, Ping, Windows Security, Azure AD, klassisches AD) + Endpunkte/Malware-Daten	☐ Anmeldung von Benutzer auf Überwachungs-/Prioritätsliste bei infiziertem System

Use Case 6
Security Monitoring und Response für Zoom

Ziel: Zoom-Datenquelle	Use Case zu Sicherheitserkennung und -reaktion
Zoom-Events über TCP Webhook	☐ Wiederverwendung persönlicher IDs/Meeting-IDs ☐ Client-Versionen prüfen ☐ Profileinstellungen zu Passwörtern und Meeting-IDs prüfen ☐ Neue Benutzeraccounts und andere Änderungen prüfen ☐ Anormale Dauer von Zoom-Meeting
Zoom-Events über TCP Webhook + REST API-Aufrufe	☐ Zoom-Anmeldungen aus ungewöhnlichen Ländern/Regionen ☐ Vorbeugung gegen Zoombombing[2]

2. Die erforderliche Phantom-Lizenz ist nicht im Remote Work Insights-Angebot enthalten, kann aber vom Kunden selbst organisiert werden. Weitere Einzelheiten über die Verfügbarkeit von Phantom und die ersten Schritte zur Nutzung der kostenlosen Community Edition von Phantom finden Sie **hier**.

Use Case 7
Monitoring von Service-Performance und -Qualität bei Zoom

Ziel: Zoom-Datenquelle	Use Case zu Sicherheitserkennung und -reaktion
„Meeting Alerts“ von Zoom über TCP Webhook	☐ Audio- oder Videoqualität schwankt (Meeting) ☐ Schlechte Qualität bei Bildschirmfreigabe (Meeting) ☐ Hohe CPU-Nutzung (Meeting) ☐ Probleme bei erneutem Verbindungsaufbau (Meeting)
„Webinar Alert“ von Zoom über TCP Webhook	☐ Audio- oder Videoqualität schwankt (Webinar) ☐ Schlechte Qualität bei Bildschirmfreigabe (Webinar) ☐ Hohe CPU-Nutzung (Webinar) ☐ Probleme bei erneutem Verbindungsaufbau (Webinar)

Use Case 8
Messen der Zoom-Nutzung

Ziel: Zoom-Datenquelle	Service-Nutzung
Zoom-Meldungen „Meeting Created“, „Meeting Started“ und „Participant Joined“ über TCP Webhook	☐ Zoom-Meldung „Meeting Created“ ☐ Zoom-Meldung „Meeting Started“ ☐ Zoom-Meldung „Participant Joined“
Zoom-Meldungen „Webinar Created“, „Webinar Started“ und „Participant Joined“ über TCP Webhook	☐ Zoom-Meldung „Meeting Created“ ☐ Zoom-Meldung „Meeting Started“ ☐ Zoom-Meldung „Participant Joined“

Use Case 9
Monitoring von Zoom Cloud-Aufzeichnung

Ziel: Zoom-Datenquelle	Service-Nutzung
Zoom-Meldung „Recording Completed“ über TCP Webhook	☐ Zoom-Meldung „Recording Completed“

Use Case 10
Monitoring von Zoom Room-Meldungen

Ziel: Zoom-Datenquelle	Service-Nutzung
Zoom-Meldung „Zoom Room Alert“ über TCP Webhook	☐ Hohe CPU-Nutzung ☐ Probleme wegen niedrigem Batteriestand, Ladevorgang und/oder Verbindung bei einem Zoom Room-Gerät (Computer, Controller oder Planungsanzeige) ☐ Verbindungsfehler/erneuter Verbindungsaufbau bei Room Controller ☐ Verbindungsfehler/erneuter Verbindungsaufbau bei Kamera ☐ Kamera/Mikrofon fehlt ☐ Verbindungsfehler/erneuter Verbindungsaufbau bei Lautsprecher

Insights for Success – Helfen Sie uns, Ihnen zu helfen

Wir möchten Sie unterstützen und Ihnen mit Remote Work Insights Möglichkeiten für erfolgreiches Arbeiten bieten. Bitte füllen Sie noch die untenstehenden Felder aus und leiten Sie sie an Ihr Splunk Account-Team weiter. Wir vereinbaren dann einen Telefontermin, um die gewünschten Ergebnisse durchzusprechen und zu klären, was für das Onboarding Ihrer Daten erforderlich ist. Außerdem informieren wir Sie über die Datentypen, die für eine erfolgreiche Durchführung benötigt werden und beraten Sie in Bezug auf Best Practices für diese grundlegende Bereitstellung.

Kontakte

Ansprechpartner für das Splunk-Team:

Hauptkontakt: Name, E-Mail, Telefonnummer

Technische Leitung: Name, E-Mail, Telefonnummer

Endbenutzer 1: Name, E-Mail, Telefonnummer

Endbenutzer 2: Name, E-Mail, Telefonnummer

Empfohlene Schulungsmaßnahmen und Testversionen

Falls Sie aktuell noch kein Benutzer sind, registrieren Sie sich bitte für einen Account auf splunk.de und das KOSTENLOSE Splunk eLearning unter splunk.com/training, um sich erste Grundkenntnisse zu verschaffen.

20-13222-Splunk-RET-Remote Work Insights-A4-107-SG