Die 6 Säulen einer erfolgreichen **DevSecOps-Strategie**

splunk>
turn data into doing®

Die rasante Verbreitung von DevOps ist alles andere als überraschend. Schließlich ermöglicht DevOps Unternehmen unter anderem eine Verkürzung des Softwareentwicklungszyklus und die kontinuierliche Bereitstellung von hochwertiger Software. Beim Wechsel zur Cloud hilft DevOps den Unternehmen, schneller zu wachsen und sich zu entwickeln, ihre Produkte rascher auf den Markt zu bringen und die Time-to-Value für Kunden drastisch zu verkürzen.

Dank der unkomplizierten Verfügbarkeit von Computing-Ressourcen in der Cloud und der weiten Verbreitung von Open-Source-Software/Code Repositorys haben sich viele Unternehmen zu produktiven Softwareherstellern entwickelt. Dadurch ist DevOps für eine größere Anzahl und Bandbreite von Projekten attraktiv geworden und hat sich von einem relativ unbekannten Verfahren zu einer weithin akzeptieren und gängigen Methode entwickelt. Laut einer 2021 vom unabhängigen Strategieberatungs- und Meinungsforschungsunternehmen ClearPath Strategies durchgeführten Umfrage unter Entscheidungsträgern im Bereich Cloud-Beschaffungen in den USA und Großbritannien wenden 62 % der Unternehmen Standard-DevOps-Praktiken an – entweder unternehmensweit oder in einzelnen Teams. Bei weiteren 28 % kommen DevOps-Lösungen in bestimmten Teams zum Einsatz.

Allerdings hat DevOps durch eine größere und sich rasch entwickelnde Angriffsfläche auch zusätzliche Sicherheitsherausforderungen geschaffen – einschließlich einer wesentlich größeren Anzahl potenzieller Angriffspunkte. Unternehmen müssen Sicherheitsaspekte früher und umfassender in den DevOps-Prozess einbinden, um diese Probleme in den Griff zu bekommen. Herkömmliche Sicherheitsansätze lassen sich mit DevOps nicht vereinbaren. Aufgrund dieses Dilemmas ist das Interesse an Sicherheit als integralem Bestandteil der DevOps-Strategie gewachsen – was zur Entwicklung einer neuen Disziplin geführt hat, nämlich Development Security Operations (DevSecOps).

DevSecOps steht für eine sichere Softwarebereitstellung in DevOps-Geschwindigkeit. Da es sich um eine relativ neue Disziplin handelt, herrscht allerdings bei vielen Unternehmen noch Unsicherheit hinsichtlich der Bedeutung, der Anforderungen und der effektiven Umsetzung. In diesem Leitfaden erörtern wir, wie Unternehmen aller Größenordnungen strategisch und taktisch vorgehen können, um DevSecOps in der Praxis nachhaltig umzusetzen. Die sechs nachfolgend skizzierten Säulen bilden das Fundament einer erfolgreichen DevSecOps-Strategie, die schneller wirkungsvolle Ergebnisse liefert.

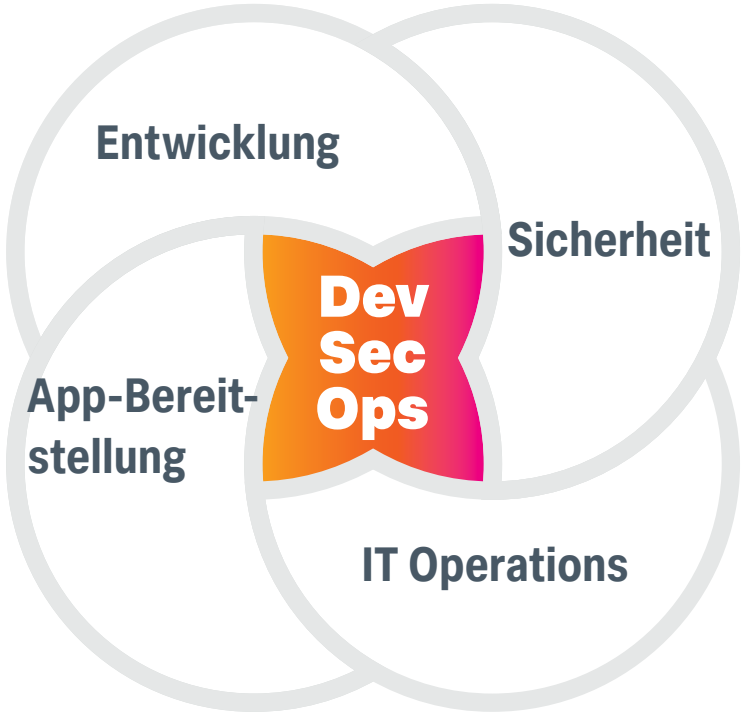
DevSecOps:
Sicherheit im Ablauf früher implementieren

In der Vergangenheit war eine Gruppe von Spezialisten für die Sicherheit verantwortlich, die Anwendungen zu Beginn und/oder am Ende des Entwicklungszyklus untersuchten und Stresstests durchführten. Angesichts des derzeitigen Tempos der DevOps-Verfahren sind herkömmliche Ansätze, bei denen die Sicherheit eine nachrangige Rolle spielt, allerdings nicht zukunftsfähig.

Im Kern geht es bei DevSecOps darum, die Sicherheit in jede Phase des DevOps-Entwicklungszyklus einzubinden – vom ersten Entwurf über das Codieren und Testen bis hin zur Bereitstellung und zum Betrieb. So können Fachkräfte Sicherheitsschwachstellen zu einem viel früheren Zeitpunkt des DevOps-Zyklus erkennen und beheben, besseren Code schreiben und sie müssen sich in späteren Stadien weniger häufig mit plötzlichen Notsituationen befassen.

Eine effektive DevSecOps-Strategie ist außerdem nur möglich, wenn alle Teams gemeinsam Verantwortung für die Sicherheit einer Anwendung und ihrer Umgebung übernehmen und Security-, Entwicklungs- und Operations-Teams Hand in Hand auf gemeinsame Ziele hinarbeiten. Das ist mitunter leichter gesagt als getan, weil jedes Team sich von anderen Prioritäten leiten lässt: Entwicklungsteams geht es normalerweise vor allem um Schnelligkeit und die Codequalität, Operations-Teams um Stabilität und Resilienz der Architektur und Security-Teams um Sorgfalt, eine breite Abdeckung und Absicherung gegen Schwachstellen und Sicherheitslücken. Ein erfolgreiches DevSecOps-Programm bringt all diese Ziele in Einklang und ermöglicht es Unternehmen, Anwendungen ebenso schnell oder noch schneller zu erstellen – mit einem Extra an integrierter Sicherheit.

Um wettbewerbsfähig zu bleiben, müssen Unternehmen auch schneller und flexibler agieren. Vor diesem Hintergrund stehen Entwickler der Einführung anfangs vielleicht zögerlich gegenüber, weil sie befürchten, DevOps-Prozesse auszubremsen oder keine Erfahrung mit sicheren Entwicklungspraktiken zu haben. Doch bei richtiger Umsetzung kommt DevSecOps nicht nur dem Sicherheitsteam zugute, sondern trägt auch zur Steigerung der Entwicklerproduktivität und zur zeitgerechten Fertigstellung qualitativ hochwertigerer Produkte bei. Für das Unternehmen kann DevSecOps Risiken senken, ein besseres Sicherheitsniveau schaffen und gleichzeitig ein hohes Entwicklungstempo unterstützen.



6 Säulen des DevSecOps-Erfolgs

Die Vorteile von DevSecOps sind unbestreitbar, doch die Implementierung ist kein einfacher Prozess. Im Wesentlichen ist DevSecOps eine Methode, kein einzelnes Produkt, und erfordert daher nicht nur neue technologische Ansätze und Toolsets im Unternehmen, sondern auch ein Umdenken und einen Kulturwandel. Dazu müssen Brücken zwischen Teams geschlagen werden, die in der Vergangenheit unabhängig voneinander gearbeitet haben, mit eigenen Tools und Workflows und oftmals auch unterschiedlichen KPIs.

Eine wirksame DevSecOps-Strategie muss auf bestehenden Systemen aufbauen, veraltete Prozesse oder Technologien eliminieren und bei Bedarf neue hinzufügen. Darüber hinaus sollte sie die Anforderungen der Entwicklungs-, Operations- und Security-Teams erfüllen und alle Ebenen des Technologie-Stacks und der Anwendung selbst in allen Phasen des Softwareentwicklungszyklus abdecken.

Nachfolgend werden sechs Säulen für die Entwicklung und nachhaltige Einführung einer erfolgreichen DevSecOps-Strategie und Splunks Beitrag zur einfacheren und schnelleren Umsetzung dieser Strategie erläutert.

1 **Überwinden von Silogrenzen im Unternehmen:** Für eine wirksame Implementierung von DevSecOps müssen Unternehmen zunächst die Barrieren zwischen Entwicklungs-, Operations-, SRE (Site Reliability Engineering)- und Security-Teams abbauen und die Sicherheit zu einer gemeinsamen Aufgabe machen. Die Teams sollten sich auf gemeinsame Ziele und KPIs einigen. Auch wenn dies für alle Beteiligten unweigerlich mit Kompromissen verbunden ist, fördert die Festlegung gemeinsamer Prioritäten und wichtiger Ziele, die nicht zu Lasten der Sicherheit gehen, die Akzeptanz. Tools, die es den Benutzern ermöglichen, mit einer gemeinsamen Source of Truth zu arbeiten, sind entscheidend für eine gute Zusammenarbeit.

Der Ansatz von Splunk: Splunk hilft, Silogrenzen im Unternehmen zu überwinden und unterstützt die Zusammenarbeit durch eine gemeinsame Plattform und Speziallösungen für Security-, IT- und DevOps-Teams. Splunk führt Daten aus der gesamten Technologielandschaft und den zugehörigen Tools zusammen, und zwar in jeder Größenordnung und bei voller Datentreue. Dank der gemeinsamen Daten- und Berichtsgrundlage lassen sich im gesamten DevOps-Lebenszyklus leichter wichtige Aufgaben bestimmen und priorisieren, gemeinsame KPIs erstellen, Fortschritte verfolgen und nach Bedarf Iterationen vornehmen.

2 **Einführen neuer Sicherheitstools und -prozesse, die Reibungsverluste für DevOps- und Sicherheitsteams reduzieren:** Bei der Einführung von DevSecOps müssen Unternehmen eventuell ihre bestehenden Tools und Prozesse ergänzen, und alle Ergänzungen müssen in die bestehenden Workflows integrierbar sein. Entwickler sind keine Sicherheitsexperten. Damit sie das hohe Entwicklungstempo beibehalten können, müssen Sicherheitstools und -prozesse sich nahtlos in die bestehende DevOps-Toolchain integrieren lassen, sodass sie weiterhin in der vertrauten integrierten Entwicklungsumgebung arbeiten können. Gleichzeitig müssen die Tools und Prozesse in bestehende Security- und SOC-Workflows integrierbar sein, damit die Sicherheitsteams wirklich effektiv mit ihren Kollegen aus dem DevOps-Bereich zusammenarbeiten können.

Der Ansatz von Splunk: Splunk führt Daten aus jeder Quelle und in jeder Größenordnung aus dem gesamten Technologie-Stack zusammen und bietet Entwicklungs-, Security- und Operations-Teams innerhalb ihrer bestehenden Prozesse und Workflows Transparenz mit Kontextbezug. Neben einzelnen, speziell auf die Teams zugeschnittenen Datenansichten ermöglicht Splunk auch die Erstellung kombinierter, teamübergreifender Dashboards, die Führungskräften einen umfassenden Überblick über wichtige Metriken geben.

3 **Fokus auf Automatisierung:** Herkömmliche Ansätze für Anwendungssicherheit sind in der Regel schwerfällig und Gate-gestützt und müssen oftmals von Sicherheitsexperten umgesetzt werden. Diese Ansätze bieten keine Skalierung für DevSecOps-Prozesse, die agil sind und kontinuierlich Feedback benötigen. Automatisierung spielt für das Tempo und die Genauigkeit bei DevSecOps ebenso wie bei DevOps eine wichtige Rolle, und trägt dazu bei, dass die Teams vereinbarten Protokollen und Best Practices folgen. Falls es zu Incidents kommt, ist Automatisierung auch für die Schaffung von Transparenz und eine einfachere Problemlösung unerlässlich. Allerdings gilt es, bei der Automatisierung mit Bedacht vorzugehen, eine unnötige Überlastung von Systemen oder eine Flut von Fehlalarmen zu vermeiden und den Schwerpunkt stattdessen auf genaue, belastbare Ergebnisse zu legen.

Für Aufgaben, die „außer der Reihe" ausgeführt werden müssen und nicht automatisiert werden können, muss ein iterativer, im Vorfeld festgelegter Zeitplan erstellt und ein System entwickelt werden, über das die Ergebnisse in den DevSecOps-Prozess eingebunden werden.

Der Ansatz von Splunk: Splunk bietet zwei Arten der Automatisierung. Zum einen werden Daten aus den unterschiedlichen Tools des Softwareentwicklungszyklus nahtlos verknüpft. Dieser Vorgang wird durch vordefinierte Integrationen für eine breite Palette branchenführender Tools und die API-gestützte Architektur von Splunk, die Konnektivität für Nischen- und unternehmensspezifische Tools bietet, erheblich vereinfacht. Diese Automatisierung trägt letztendlich zu einer Reduzierung manueller Eingriffe bei und ermöglicht es den Teams, sich von monotonen Routineaufgaben zu befreien, damit sie sich auf neue, innovative Use Cases konzentrieren können.

Zum anderen unterstützt Splunk auch größer angelegte Automatisierungsinitiativen im DevSecOps-Bereich. Durch transparente Einblicke in den Zustand und die Funktionalität dieser Automatisierungen trägt Splunk dazu bei, durch Black-Box-Prozesse hervorgerufene Herausforderungen zu mindern. Dabei kann durch Predictive Analytics vor möglichen Problemen gewarnt werden, bevor diese auftreten.

4 **Durchgängige, teamübergreifende Transparenz:** Transparenz und Feedback müssen kontextbezogen und durchgängig sein – von der Definition eines Features bis zu dessen Einsatz in der Produktionsumgebung – und im gleichen Tempo bereitgestellt werden wie der Code, der das System durchläuft. Entwicklungs- und Operations-Teams brauchen diese Transparenz in ihrer Toolchain und in ihren bestehenden Prozessen wie Ticket-Systemen oder Slack-Benachrichtigungen. Security-Teams sollten ebenfalls Einblick in alle wichtigen Metriken ihrer eigenen Prozesse und Toolchains haben, um mit ihren Kollegen aus den Entwicklungs- und Operations-Abteilungen zusammenarbeiten und auf alle Informationen zugreifen zu können, die zur Behandlung von Sicherheitsproblemen in der Produktionsumgebung erforderlich sind.

Der Ansatz von Splunk: Da Splunk Daten aller Tools und Technologie-Stacks erfasst, bietet die Plattform kontextuelle Einblicke in Anwendungen und die Infrastruktur, auf der sie ausgeführt werden, sowie einen Überblick über die Verbindungen zwischen den einzelnen Prozessphasen in der gesamten Pipeline. Darüber hinaus extrahiert Splunk mithilfe von KI/ML aussagekräftige und belastbare Erkenntnisse und optimiert die Workflows für Entwicklungs-, Operations- und Security-Teams. Funktionen wie risikobasierte Benachrichtigungen priorisieren Incidents, dämmen Over-Alerting ein und erleichtern Entwicklern die Sicherheitsbemühungen.

5 Behandeln aller Sicherheitsschwachstellen als Qualitätsmängel: Unternehmen erfassen ihre Analyseergebnisse oft in zwei unterschiedlichen Kategorien – Sicherheit und Qualität – an zwei unterschiedlichen Stellen. Diese Methode wirkt sich negativ auf die Transparenz aus und führt häufig dazu, dass Entwickler Sicherheitsmängeln eine niedrigere Priorität einräumen. Unternehmen können gegensteuern, indem sie Sicherheits- und Qualitätsergebnisse an einer Stelle zusammenführen, damit sich alle Parteien ein genaues Bild von der Sicherheitslage machen können und das Entwicklungsteam Qualitäts- und Sicherheitsproblemen die gleiche Bedeutung beimessen kann.

Der Ansatz von Splunk: Da Splunk Daten aus den gesamten DevOps- und Sicherheits-Toolchains abrufen und konsolidierte, gemeinsam genutzte Dashboards bereitstellen kann, können die Teams auf ein gemeinsames Repository zugreifen und erhalten in Echtzeit einen genauen Überblick über Sicherheits- und Qualitätsmängel. Diese gemeinsame Sicht auf die Daten kann dazu beitragen, dass beträchtliche Sicherheitsmängel zu einem frühen Zeitpunkt und unter Beteiligung aller Teams behoben werden, um kostenintensive Nacharbeit in der Produktion zu vermeiden.

6 Ausweiten/Stärken der Strategie zur Incident Response: Das Auftreten von Sicherheitsproblemen in der Produktionsumgebung lässt sich nicht gänzlich vermeiden. Umfassende kontextuelle Transparenz ab der Definition eines Features hilft den Teams jedoch beim raschen Erkennen dieser Probleme. Angesichts der Kurzlebigkeit von Cloud-Architektur kommt auch der Full-Fidelity-Nachverfolgung jeder einzelnen Interaktion große Bedeutung zu. Selbst nach der Zuweisung eines Incidents müssen Security-Response- und Resolution-Teams bisweilen noch zusammenarbeiten. Gemeinsame Tools und übergreifende Transparenz tragen zu einer besseren und schnelleren Lösung bei.

Der Ansatz von Splunk: Über die Entwicklung hinaus bietet Splunk eine Sicht auf alle Incident-Daten sowie integrierte Tools für eine wirksame Incident Response. Damit haben SREs, die in der Regel an vorderster Front tätig sind, Zugriff auf alle Daten, die sie für die Analyse von Sicherheits-Incidents brauchen. Mit Splunk können sie Warnmeldungen an die richtigen Mitarbeiter weiterleiten, eine Reaktion zuweisen und den Ticketstatus und Fortschritt überwachen. Wenn ein Ticket einem Sicherheitsexperten zugewiesen wird, sorgt Splunk dafür, dass ihm alle forensischen Untersuchungsdaten des SRE zur Verfügung stehen, um doppelten Aufwand zu vermeiden. Darüber hinaus bietet Splunk End-to-End-Transparenz ab der Definition der Features, sodass Sicherheitsexperten sich ein Bild von einem Incident machen können, ohne den Entwickler zu behelligen. Entwickler haben Einblick in den Lösungsprozess, auch wenn sie selbst nicht eingreifen müssen, und können sich so ein Bild von den Sicherheitsauswirkungen ihres Codes in der Produktion machen und Schlüsse für die Definition und Priorisierung von Sicherheitsanforderungen bei zukünftigen Projekten ziehen.

DevSecOps anwenden

In zahlreichen Branchen gibt es potenziell Tausende von Einsatzmöglichkeiten für DevSecOps. Fast alle sind jedoch drei Hauptkategorien zuzuordnen: Sicherheit in der Entwicklungsumgebung, Entwicklung sicherer Apps und Sicherheit von Apps in der Produktion.

1 **Sicherheit in der Entwicklungsumgebung:** Entwickler brauchen eine sichere und resiliente Umgebung, um in der DevOps-Toolchain erfolgreich arbeiten zu können. Die DevOps-Toolchain umfasst jedoch eine Vielzahl von Punktlösungen für unterschiedliche Einzelfunktionen. Noch komplexer wird das Ganze durch die zunehmende Abhängigkeit von Open-Source-Software für die Entwicklung von Apps und die Einführung entkoppelter und kurzlebiger Architekturmuster.

Wie Splunk helfen kann: Splunk verknüpft die Telemetrie über diese zahlreichen Tools hinweg, analysiert Datenmuster mithilfe von KI/ML und erstellt lesbare, risikobasierte Benachrichtigungen. Auf diese Weise können Unternehmen sicherstellen, dass ihre Mitarbeiter unabhängig von den verwendeten Tools die Sicherheitsrichtlinien einhalten und gleichzeitig störende Fehlalarme auf ein Minimum reduzieren. Darüber hinaus unterstützt Splunk die automatisierte Incident Response zur Vereinfachung der Fehlerbehebung.

2 **Entwicklung sicherer Apps:** Um sichere Apps zu entwickeln, muss die Sicherheit auf jeder Ebene der App einbezogen werden – bei App-Komponenten, Cloud-Services und OSS-Bibliotheken, auf die Apps angewiesen sind. Das Einbeziehen von Sicherheitsaspekten in jeder Phase umfasst auch den Custom Code der App, API-Interaktionen zwischen unterschiedlichen Services, entwickelte und bereitgestellte Images sowie die Infrastruktur – zunehmend in der Cloud und in Containern –, auf der der Code ausgeführt wird.

Wie Splunk helfen kann: Splunk kann in Echtzeit Logs von all diesen Ebenen abrufen und die Nachverfolgung der Aktivitäten-Pipeline von der Feature-Definition bis zum Release und zu Sicherheits-Incidents in der Produktion unterstützen. Diese tiefgreifenden kontextuellen Einblicke werden über gemeinsam genutzte Dashboards und innerhalb der bestehenden Tool-Konstellation in Echtzeit bereitgestellt.

Dadurch können Entwickler die Sicherheit des Codes erhöhen und gleichzeitig Richtlinien- und Sicherheitsverstöße korrigieren. Diese teamübergreifenden Erkenntnisse sind auch wertvoll für die Bestimmung, Nachverfolgung und Messung optimaler Codierungspraktiken im gesamten Softwareentwicklungszyklus.

3 **Sicherheit von Apps in der Produktion:** Wenn es nach der Bereitstellung zu einem Sicherheits-Incident kommt, sind in der Regel der SRE und das Security-Team für Abhilfemaßnahmen zuständig. Tatsächlich ist die Behebung von Problemen aber oftmals kompliziert, und zwar einerseits wegen des hohen Entwicklungstempos und andererseits weil Entwickler sich ein Bild von den frühen Phasen des Entwicklungszyklus und auch von den späteren Phasen des Nutzungszyklus machen müssen.

Wie Splunk helfen kann: Splunk zeichnet die gesamte Pipeline der Aktivitäten auf, beschleunigt dadurch Sicherheitsuntersuchungen und die Incident Resolution und steigert die Effizienz dieser Prozesse durch eine wirkungsvolle Reduzierung des ständigen Hin und Hers zwischen Entwicklern, SREs und Security-Teams.

DevSecOps ist fundamental für den Erfolg im Datenzeitalter

Angesichts von immer neuen Bedrohungen ist Sicherheit für Unternehmen wichtiger denn je. Gleichzeitig steigt der Druck und Unternehmen, die nicht riskieren wollen, ihren Wettbewerbsvorteil an schnellere und agilere Akteure zu verlieren, müssen die Produktion und Entwicklung von Apps beschleunigen.

Durch die Integration von Sicherheitstests in den Softwareentwicklungszyklus ohne das DevOps-Tempo zu verringern, bietet DevSecOps die Lösung für beide Probleme. Da DevSecOps Sicherheitsrisiken und -schwachstellen von Beginn an entgegenwirkt, können Unternehmen schädliche oder kostspielige Überraschungen, die andernfalls möglicherweise erst in späteren Phasen zutage treten würden, rasch eindämmen oder gänzlich verhindern. Die Einführung von DevSecOps ermöglicht auch die Implementierung kontinuierlicher Sicherheit, d. h., die Assets der entsprechenden Unternehmen sind 365 Tage im Jahr rund um die Uhr geschützt.

Mit Splunk lassen sich diese neuen DevSecOps-Strategien leichter umsetzen und skalieren – dank End-to-End-Transparenz, der Integration der richtigen Daten in die entsprechenden Arbeitsabläufe und dem reibungslosen Funktionieren neuer Tools und Prozesse bei Sicherheits- und DevOps-Teams. Mit einem ganzheitlichen Ansatz stellt Splunk sicher, dass die Lösungen funktionieren, und zwar nicht nur für bestehende DevOps-Prozesse, sondern auch für die Security-Teams und deren Verfahren innerhalb des SOC.

Zukünftig dürfte DevSecOps eine noch größere Rolle im Entwicklungsprozess, aber auch für den Gesamterfolg der Unternehmen und deren Wettbewerbsfähigkeit im Datenzeitalter spielen. Der Aufbau und Erhalt einer DevSecOps-Kultur ist nicht von heute auf morgen realisierbar, doch ein neuer Denkansatz mit DevSecOps-Fokus in der Entwicklungspipeline hilft Unternehmen dabei, die Produktivität zu steigern, das Risiko zu senken und von Beginn an ein höheres Sicherheitsniveau zu kultivieren.

Kontaktieren Sie Ihren Splunk-Vertriebsexperten, um zu erfahren, wie Splunk Ihre DevSecOps-Initiative unterstützen kann.

Erfahren Sie mehr

splunk> turn data into doing®

21-21001-Splunk-6 Pillars_GER