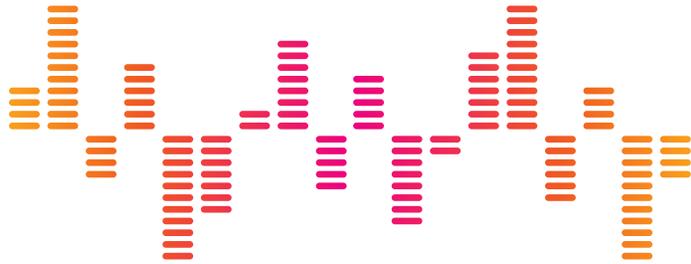




Pioniere des Datenzeitalters

Wie führende Unternehmen das volle Potenzial
ihrer Daten nutzen

splunk>



Inhalt

TEIL I: Ein prägendes Zeitalter

Einleitung	3
Neue Wege einschlagen	5
Data-to-Everything – Mit Daten wird alles besser	6
Unternehmerische Erkenntnisse: Domino's, Porsche	7
DevOps: Arlo, PSCU	9
IT Operations: U.S. Census Bureau, Global Emancipation Network	11
Security: Mars Inc., Intel	13

TEIL II: Von den Besten lernen

Bildungswesen

● ● University of Arizona	17
● ● University of Illinois	18
● ● Jefferson Co. Public Schools	19
● ● Arizona State University	20

Finanzdienstleister

● ● au Kabucom Securities	22
● Die Bank of England	23
● ● Keystart	24
● Aflac	25
● ● PSCU	26

Gesundheitswesen

● NewYork-Presbyterian	28
● ● Imprivata	29
● Molina Healthcare	30

Fertigung

● ● Porsche	32
● ● Mars Inc.	33
● Nikko Chemicals	34
● Zeppelin	35
● ● Shaw Floors	36

Gemeinnützige Organisationen

● ● ● Compassion International	38
● Global Emancipation Network ...	39
● Rise Against Hunger	40
● ● NetHope	41

Öffentlicher Sektor

● ● ● U.S. Census Bureau	43
● ● Derbyshire Fire and Rescue	44
● Michigan Department of Health and Human Services	45
● ● National Ignition Facility	46
● Gold Coast in Australien	47

Einzelhandel

● ● ● Domino's	49
● REI	50
● ASICS	51

Technologie

● ● Intel	53
● Lenovo China	54
● ● Arlo	55
● ● Acquia	56
● Square Enix	57

Telekommunikations- und Versorgungsunternehmen

● ● TalkTalk	59
● Belong	60
● Puget Sound Energy	61

Reise und Verkehr

● ● ● Hyatt Hotels	63
● Gatwick Airport	64
● ● Dubai Airports	65
● Sapura	66

LEGENDE

- Security
- IT Operations
- DevOps
- Unternehmerische Erkenntnisse

Ein prägendes Zeitalter

Unternehmen stehen stärker unter Druck als je zuvor.

Von der COVID-19-Pandemie über Naturkatastrophen bis hin zu regulatorischen Änderungen und politischen Auseinandersetzungen – Unternehmen und öffentliche Einrichtungen sehen sich mit beispiellosen Veränderungen und Herausforderungen konfrontiert. Doch es eröffnen sich auch Chancen.

Nachdem die Digitalisierung in den letzten Jahren immer schneller vorangeschritten ist, sind wir nun vollends im Datenzeitalter angekommen. Es ist ein Zeitalter, in dem allgegenwärtige und vernetzte digitale Technologien Daten nutzen, die in Unternehmen, im täglichen Leben und in der Gesellschaft als fundierte Grundlage für jede Entscheidung herangezogen werden. Diese neue Realität bringt Drucksituationen und Potenziale mit sich, die die Wettbewerbslandschaft neu definieren, die Kundenerwartungen steigern und in beispiellosem Tempo umwälzende Innovationen antreiben.

Und alles dreht sich um Daten.

In den letzten Jahren hat angesichts der ungeheuren Datenmenge und des enormen Werts dieser Daten in allen Branchen ein Wandel stattgefunden – und die Möglichkeiten wachsen weiter. Im Bericht „[Das Datenzeitalter hat begonnen. Sind Sie bereit?](#)“ geben zwei Drittel der befragten Unternehmen an, die Menge ihrer Daten werde sich bis 2025 nahezu verfünffachen. Laut dem von TRUE Global Intelligence Research im Auftrag von Splunk erstellten Bericht geben nur 14 % der Führungskräfte aus Business und IT an, ihr Unternehmen sei auf eine neue Datenwelle vorbereitet.

Bei Splunk haben wir die Erfahrung gemacht, dass erfolgreiche Unternehmen Daten als Grundlage für jede Frage, Entscheidung und Handlung nutzen und sich wandelnden Erwartungen anpassen, um neue Geschäftschancen zu erschließen und überzeugende Ergebnisse zu erzielen. Diese Datenpioniere treffen Entscheidungen in Echtzeit, antizipieren Trends und steigern ihre Effizienz, um Kunden und Endbenutzern einen Mehrwert zu bieten.

Das Datenzeitalter könnte für viele Führungskräfte und Unternehmen die prägende Ära sein.

Zwei Drittel der befragten Unternehmen erwarten bis 2025 einen fast fünffachen Anstieg ihrer Datenmenge

5 x

Neue Wege einschlagen

Splunk-Kunden haben in diesem prägenden Zeitalter die Nase vorn. Sie setzen die Data-to-Everything™ Plattform ein, um ihre Unternehmen und Kunden besser zu verstehen, Vertrauen bei den Konsumenten aufzubauen und sich an die verändernden Umstände anzupassen.

Von Porsche über Intel bis hin zu ASICS – Splunk-Kunden setzen auf agile Cloud-Umgebungen und integrieren Technologien wie Machine Learning und IoT. Gleichzeitig investieren sie weiterhin in wichtige Eckpfeiler wie IT Operations und Security. Dank dieses integrierten Ansatzes können Teams unternehmensweit ihre Silos aufbrechen und ihr gesamtes Handeln auf Daten gründen. Die Bandbreite reicht von einem DevSecOps-Ansatz über die Entwicklung und Vermarktung neuer digitaler Produkte bis hin zu einer personalisierten Omnichannel-Erfahrung für jeden Benutzer.

Diese Datenpioniere liefern den Beweis dafür, dass einfach alles möglich wird, wenn Sie das volle Potenzial Ihrer Daten nutzen.

Über Branchen und Landesgrenzen hinweg entfernen Unternehmen und Organisationen die Barrieren zwischen Daten und Maßnahmen und erzielen damit beeindruckende Ergebnisse.



Compassion International, eine seit fast 70 Jahren bestehende gemeinnützige Organisation, setzt Machine Learning und Datenverarbeitung ein, um jedes Jahr über zwei Millionen Kinder aus Armut und Menschenhandel zu befreien.



Der Spitzenreiter auf dem weltweiten Pizzamarkt versorgt 16.300 Filialen auf der ganzen Welt und 16 digitale Bestellkanäle mit Daten und bietet seinen Kunden damit ein komfortables und erstklassiges Erlebnis.



Nach dem COVID-19-Ausbruch gelang es einer staatlichen Universität, in nur zwei Wochen mit 60.000 Studierenden, Dozenten und Mitarbeitern auf eine Remote-Lernumgebung umzusteigen und dabei jederzeit zuverlässige und sichere virtuelle Systeme bereitzustellen.

Data-to-Everything – Mit Daten wird alles besser

„Alles“ ist ein weiter Begriff – lassen Sie uns also konkreter werden. Die zukunftsorientierten Unternehmen auf den folgenden Seiten nutzen Daten in ihren Business-, Security-, IT- und DevOps-Teams und haben so Erfolg – mit einem vernetzten, ganzheitlichen Ansatz. Sie investieren in unternehmerische Eckpfeiler und erweitern gleichzeitig ihre Use Cases, um neue Geschäftschancen zu erschließen.

Dabei sichern sie ihre Infrastruktur ab und binden gleichzeitig ihren Kundenstamm. Sie gewährleisten eine maximale Verfügbarkeit und generieren so Umsatzsteigerungen. Sie automatisieren Prozesse und verbessern dabei automatisch ihre Organisation.

Unternehmerische Erkenntnisse

Daten sind von grundlegender Bedeutung für erfolgreiche Unternehmen, sei es bei der Akquise neuer Kunden, beim Entwickeln einer fundierten Produktstrategie, beim Bewerten von Marketinginitiativen oder beim Prognostizieren von Verkaufstrends. Splunk-Kunden wissen um den Wert dieser Erkenntnisse und verwandeln Daten in konkrete Handlungen, um Betriebsabläufe zu optimieren, den Umsatz zu steigern und ihren Kundenservice zu verbessern.

Domino's bietet eine überzeugende Omnichannel-Erfahrung

Pizza und Daten sind eine eher ungewöhnliche Kombination. So dachte man zumindest noch vor einem Jahrzehnt, als Pizzeriaunternehmen noch nicht in die Digitalisierung investierten. Außer Domino's.

Die weltweit agierende Pizzakette stellte sich als „E-Commerce-Unternehmen, das nebenbei auch noch Pizza verkauft“ neu auf und verlagerte ihren Schwerpunkt auf digitale Kanäle und neue Technologien. Heute ist Domino's weltweit die umsatzstärkste Pizzakette. Mit den Erkenntnissen, die die Splunk-Plattform liefert, trifft das Unternehmen fundierte Entscheidungen, fördert Innovation und wird dem Kundenbedürfnis nach Schnelligkeit, Qualität und Benutzerfreundlichkeit gerecht.

Domino's verfügt mittlerweile über 16 unterschiedliche digitale Bestellkanäle – von Smart-TV-Geräten und Smartwatches über Mobiltelefon-Apps bis hin zu Slack und sozialen Medien. In Kombination generiert das Unternehmen damit 65 % der Umsätze auf dem US-amerikanischen Markt. „Splunk hilft uns mit jeder Echtzeittransaktion“, so Mike Cox, Operational Intelligence Architect bei Domino's. „Wir verstehen, was mit unseren Bestellungen, Services, Websites und Anwendungen passiert. Wenn wir all diese Daten sammeln, können wir unsere Prozesse sowohl auf internationaler als auch auf nationaler Ebene verbessern.“

In den USA generiert Domino's mehr als 65 % des Umsatzes über 16 digitale Bestellkanäle.

Bei Domino's werden die von Splunk bereitgestellten Daten unternehmensweit von allen Teams genutzt. Die Bandbreite reicht von E-Commerce und digitaler Infrastruktur bis hin zu Marketing und zur In-Store-Kundenerfahrung. „Domino's nutzt Daten auf jede nur erdenkliche Weise“, sagt Alex Padilla, Vice President of Information Security bei Domino's. „Wir nutzen Daten als Grundlage für Investitions-, Budget- und Technologie-Entscheidungen und zum Messen der Effizienz von Tools und Prozessen. Wir stützen uns auf Daten, um neue Technologien zu entwickeln und unseren Kunden einen neuen Ansatz zu bieten.“

Wenn alle dieselben Daten im selben Tool betrachten, können Teams besser zusammenarbeiten und Erkenntnisse problemlos mit Führungskräften austauschen. So konnte das Unternehmen weiter wachsen und seine Position als Spitzenreiter verteidigen, ohne Kompromisse bei der Qualität einzugehen.



Porsche startet in die Zukunft durch

„Das letzte Auto, das jemals gebaut wird, wird ein Sportwagen sein.“ Das ist die Philosophie, die Porsche antreibt, ein Unternehmen, das mit Performance, Design, Technologie und Innovation auf Weltklasseniveau bereits seit Jahrzehnten eine Führungsrolle übernimmt. Um auch weiterhin immer einen Schritt voraus zu sein, musste Porsche sich an neue Kundenansprüche anpassen und nutzt Daten, um das zukunftsweisende, luxuriöse Erlebnis zu liefern, das die Marke ausmacht.

„Wie bei fast allen anderen Unternehmen sind auch bei uns Daten plötzlich das Herzstück unseres Geschäfts“, erklärt Tim Klapper, IT Service Manager bei Porsche. „Wir nutzen Daten, um unsere Performance zu steigern, mehr Erkenntnisse zu gewinnen und bessere und intelligentere Entscheidungen zu treffen.“ Stefan Arnold, Head of Technology Acceleration and Management, sagt: „Intelligente Performance ohne Daten ist nicht möglich.“

Porsche verwendet die Splunk-Plattform für einen Leistungsschub auf der Straße und auch abseits davon. Dies geschieht im Rahmen von Projekten wie Porsche Connect, einer App, die Fahrern den Remote-Zugriff auf ihr Fahrzeug ermöglicht. Dabei können sie unter anderem den Kilometerstand überprüfen, die Klimaanlage steuern und die Autotüren ver- und entriegeln. „Heute basiert unser digitaler Support auf Splunk“, so Klapper. „Wir haben unsere Eventprotokoll- und Customer Journey-Analyse verbessert und nutzen Splunk, um Probleme zu beheben, bevor sie sich irgendwo



Intelligente Performance ohne Daten ist nicht möglich.“

— Stefan Arnold, Head of Technology Acceleration and Management bei Porsche

im Verlauf der digitalen Journey auf unsere Kunden auswirken. Nachdem wir uns mit der Software vertraut gemacht hatten, haben wir die Business-Anwendungsfälle ausgeweitet. Splunk hilft uns nun, das Potenzial der Daten in allen Prozessen auszuschöpfen.“

Eine der jüngsten Innovationen ist der Porsche Taycan, das erste Elektrofahrzeug des Unternehmens. Um digitale Technologie nahtlos mit physischen Kontaktpunkten zu kombinieren, setzt Porsche für den digitalen Kundensupport an mehr als 2.000 Ladestationen auf der ganzen Welt auf die Splunk-Plattform und nutzt Daten, um Fahrer zur optimalen Ladestation zu leiten. Arnold dazu: „Mit Splunk verwandeln wir Daten in Taten – ganz nach Porsche-Art.“



DevOps

Wir befinden uns in der „Now Economy“. Die Verbraucher erwarten intuitive Apps und Services, die effizient, zuverlässig und jederzeit und überall verfügbar sind. Um diese Erwartungen zu erfüllen, brauchen DevOps-Teams Transparenz im gesamten Technologie-Stack – von der lokalen Infrastruktur bis zu Cloud-Umgebungen. Nur so ist es möglich, eine gute Performance sicherzustellen, Ausfälle zu verhindern und Incidents rasch zu beheben, bevor sie sich auf das Unternehmen oder Kunden auswirken.

Arlo erfüllt die Kundenerwartungen

Mit seinen preisgekrönten IoT-Geräten hilft Arlo seinen Kunden, mit geliebten Menschen und Orten in Verbindung zu bleiben und sie zu schützen. Arlo muss in 3,4 Millionen registrierten Haushalten in 100 Ländern dafür sorgen, dass alle Geräte, von drahtlosen Sicherheitskameras bis hin zu fortschrittlichen Babyfonen, sicher sind und zuverlässig funktionieren – eine Aufgabe, die einen einfachen Zugriff auf Daten und End-to-End-Observability erforderlich macht.

Das Unternehmen setzt zur mühelosen Untersuchung und Überwachung seiner Systeme auf Splunk Cloud. So kann sich das Team auf Innovationen und die strategische Ausrichtung, statt auf die Wartung der IT-Infrastruktur konzentrieren. Splunks positiver Einfluss auf die täglichen Arbeitsabläufe erstrecken sich mittlerweile auf alle Teams. Mit vorherigen Tools konnte die MTTI (Mean-Time-To-Investigate) eines einzigen Produktions-Incidents Tage betragen, was frustrierte Teammitglieder und kostspielige Produktivitätsverluste zur Folge hatte. Doch dank Splunk ist es Arlo gelungen, die MTTI von Tagen auf Stunden zu reduzieren – in vielen Fällen sogar auf Minuten.



Bisher hat uns die fehlende Transparenz immer ausgebremst. Doch Splunk unterstützt die Geschwindigkeit des Teams, sodass wir Produkte und Funktionen schneller entwickeln und früher zuverlässige Releases veröffentlichen können.“

— Jishnu Kinwar, Vice President Cloud Platform Engineering bei Arlo

Mit optimierten internen Prozessen haben die DevOps- und QS-Teams von Arlo die Produktivität gesteigert und Innovationen beschleunigt, sodass Probleme nun schneller gelöst und neue Produkte und Funktionen schneller auf den Markt gebracht werden können. „Bisher hat uns die fehlende Transparenz immer ausgebremst“, erklärt Jishnu Kinwar, VP Cloud Platform Engineering bei Arlo. „Doch Splunk unterstützt die Geschwindigkeit des Teams, sodass wir Produkte und Funktionen schneller entwickeln und früher zuverlässige Releases veröffentlichen können.“

Arlo fügt weiterhin neue Anwendungsfälle in den Bereichen Infrastruktur-Monitoring und Predictive Analytics hinzu. Das Team setzt die Machine Learning-Funktion der Splunk-Plattform bereits zur Erkennung von Ausreißern ein, wird sie aber in Kürze auch für Zeitreihenprognosen und zum automatischen Skalieren von Modellen nutzen, um künftige Trends zu prognostizieren und eine proaktive Kapazitätsplanung zu ermöglichen.



PSCU investiert in Agilität

PSCU ermöglicht mehr als 1.500 Kreditgenossenschaften die Durchführung von fast 4 Milliarden Transaktionen pro Jahr und stellt White-Label-Anwendungen für Online-Rechnungszahlungen, Online-Kredite und andere Finanzdienstleistungen zur Verfügung. Um den Kreditgenossenschaften im Wettbewerb mit den Banken eine bessere Position zu verschaffen, kümmerte sich PSCU vor allem um die Verbesserung wichtiger IT-Performance-Metriken, z. B. der MTTA (Mean-Time-To-Acknowledge), die angibt, wie viel Zeit zwischen dem Eingang einer Warnmeldung und der Reaktion vergeht. Die MTTA ist eine wichtige Metrik für die Verminderung von Ausfallzeiten, da durch ein schnelleres Auslösen der Incident Response auch die MTTR (Mean-Time-To-Repair) verkürzt werden kann.

Um dieses Ziel zu erreichen, entschied sich die PSCU für die Splunk-Plattform, die ein nahtloses Security-Monitoring und PCI-Compliance (Payment Card Industry) ermöglicht. Die PSCU löste ihre Probleme im Bereich der Verantwortlichkeit mit der Incident Management-Software Splunk On-Call (ehemals VictorOps). Sie versetzt Bereitschaftsteams in die Lage, Probleme durch automatisierte und informationsreiche Incident Management-Weiterleitung, Zusammenarbeit und Überprüfungen schneller zu erkennen und zu lösen. Dank dieser neuen Funktionen konnte das PSCU-Team die MTTA von vier Stunden auf weniger als zwei Minuten verkürzen.

Heute nutzen die Qualitätssicherungs- und DevOps-Teams der PSCU die Splunk-Plattform, um Performance-Einbußen proaktiv zu erkennen, bevor sie sich zu Ausfällen entwickeln. Den Ausgangspunkt bildeten IT-Anwendungsfälle. Mittlerweile kombiniert die PSCU die Maschinendatenanalyse von Splunk mit der Incident Response von Splunk On-Call zu einer übergreifenden Plattform, mit der die DevOps-Teams schneller innovative Lösungen finden, agiler werden und die Kundenerfahrung



Mit der Splunk-Plattform
konnte die MTTA
**von 4 Stunden
auf weniger
als 2 Minuten
verkürzt werden.**

IT Operations

Miteinander verflochtene Infrastrukturen werden immer komplexer und IT-Teams stehen immer stärker unter Druck. Sie sollen Probleme vorhersagen und gleichzeitig eine hohe Servicequalität für Mitarbeiter und Kunden gewährleisten. Splunk-Kunden haben die Herausforderung angenommen und begreifen das Datenzeitalter als Chance, sich durch die Einführung neuer Technologien und die Automatisierung und effektivere Gestaltung von Prozessen zu einer effizienten, vernetzten Organisation zu entwickeln.

Das U.S. Census Bureau schreibt Geschichte

Das U.S. Census Bureau, also die für die Volkszählung zuständige US-amerikanische Behörde, hat eine überraschend komplexe Zielsetzung: Die Behörde möchte die landesweit führende Quelle für Qualitätsdaten über Bürger und Wirtschaft sein.

Alle zehn Jahre führt das Census Bureau eine umfassende, genaue Zählung der Bevölkerung und des Wohnraums in den gesamten Vereinigten Staaten durch. Das heißt, jede Person in jedem Winkel des Landes wird gezählt. Da die Volkszählung 2020 zum ersten Mal digital durchgeführt wird, nutzt die Behörde die Splunk-Plattform, um ihre Aufgabe effektiver und effizienter zu erfüllen.

Die Volkszählung von 2020 umfasst 35 Prozesse und 52 Systeme, von der Personal- und Lohnbuchhaltung bis hin zur Koordinierung einer landesweiten Zählung, bei der jeder Haushalt in jedem Bundesstaat und im gesamten Hoheitsgebiet der USA erfasst werden muss. Doch dank der Digitalisierung und der verbesserten Datenverarbeitung umfasst die diesjährige Zählung weniger Systeme als 2010, was sich positiv auf die Leistung, die Genauigkeit und die Effizienz auswirken und die Nutzung von Steuergeldern optimieren wird.

Splunk leistet einen vielfältigen Beitrag zu diesem riesigen Datenprojekt. Zunächst einmal unterstützt Splunk die Behörde bei der Koordinierung von Adressenlisten aus verschiedenen Quellen, beim Einsatz von Satellitendaten zur Reduzierung des manuellen Erfassungsaufwands an der Haustür und bei der effizienteren und genaueren Konsolidierung erhobener Daten. Außerdem macht Splunk die Rekrutierung, Einstellung und Bezahlung von Mitarbeitern durch Automatisierung und digitale Workflows effizienter. Dies ist ein riesiger Vorteil für eine Behörde, die 6.000 Helfer zur Datenerhebung an der Haustür einstellen und koordinieren muss.



Die Volkszählung in den USA hat Einfluss auf die öffentliche Politik und die Verteilung von Finanzmitteln in Höhe von mehr als 675 Milliarden Dollar . Sie zeichnet die politische Landkarte des nächsten Jahrzehnts neu.

2020 ist das erste Jahr, in dem die Amerikaner die Möglichkeit haben, die Volkszählungsfragen online zu beantworten. Inmitten der COVID-19-Pandemie ist diese digitale Option für das Census Bureau ein Eckpfeiler des Erfolgs. In Partnerschaft mit Splunk hat die Behörde IT-Systeme und Infrastruktur mit inhärenter Redundanz eingerichtet und war dank ihres vielschichtigen Cybersicherheitsprogramms in der Lage, angemessen auf die aktuelle Krise zu reagieren. Das Census Bureau setzt seine Mission fort und nutzt Splunk für das Monitoring des digitalen Datenverkehrs und die Echtzeitprüfung der IT-Systeme. Damit wird es den Verantwortlichen ermöglicht, in einer turbulenten Welt fundierte Entscheidungen zu treffen.

Global Emancipation Network sagt Menschenhandel den Kampf an

Mit schätzungsweise 45 Millionen Opfern pro Jahr ist der Menschenhandel die Ursache einer schweren Menschenrechtskrise. Global Emancipation Network (GEN) ist ein Teil der Lösung.

„Menschenhandel ist eine menschliche Tragödie. Gleichzeitig ist er aber auch ein illegaler Wirtschaftszweig, bei dem jemand ein Produkt kauft, um einen Bedarf zu decken, zum Beispiel nach sexueller oder häuslicher Knechtschaft“, erklärt Sherrie Caltagirone, Gründerin und Executive Director von GEN. „Diese Transaktion hinterlässt oftmals einen digitalen Fußabdruck. Der Menschenhandel ist also ein Datenproblem. Bei 99,9 % unseres alltäglichen Kampfes geht es darum, Zugriff auf Daten zu bekommen, um den Menschenhandel zu stoppen.“

Doch der Zugriff auf diese traditionell in verteilten Silos gespeicherten Daten erwies sich als extrem schwierig und GEN suchte nach einer effizienten Möglichkeit, Daten zu sammeln und Systeme zu optimieren, um seine Analyse- und Handlungsfähigkeit zu verbessern. GEN entschied sich bei seiner Gründung im Jahr 2016 für Splunk als Datenplattform und seitdem bildet Splunk das Fundament, auf dem die Organisation ihre Mission aufbaut.



Bei 99,9 % unseres alltäglichen Kampfes geht es darum, Zugriff auf Daten zu bekommen, um den Menschenhandel zu stoppen.“

— Sherrie Caltagirone, Founder and Executive Director bei Global Emancipation Network



Mithilfe von Splunk hat GEN Minerva entwickelt, eine mandantenfähige Datenanalyseplattform, die einen sicheren, individualisierten Datenaustausch und intelligente Analysen ermöglicht. Die leistungsstarke Plattform nutzt Splunk, um in ungeordneten, unstrukturierten Daten aus Hunderten von Quellen Verbindungen zwischen Benutzernamen, E-Mail-Adressen, Telefonnummern, Texten und Bildern herzustellen, die manuell nicht oder nur schwer herstellbar wären.

GEN nutzt Daten zur Lösung eines der größten Probleme, mit denen die Welt konfrontiert ist, und hat damit schon Beachtliches erreicht. Beispielsweise hat die Organisation bei sieben Razzien im Bereich des Menschenhandels Unterstützung geleistet, bei denen allein im letzten Jahr Dutzende von Opfern gerettet wurden. Darüber hinaus wurde durch die Identifizierung von mehr als 10.000 Fällen von Menschenhandel in 22.000 Massageunternehmen die Eindämmung der illegalen Massagebranche gefördert. In Zukunft sind weitere vielversprechende Ergebnisse zu erwarten. Über GEN und Splunk for Good steht Minerva nationalen und internationalen Strafverfolgungsbehörden, Nichtregierungsorganisationen, wissenschaftlichen Institutionen und dem privaten Sektor für das weltweite Aufspüren und Stoppen von Menschenhandel kostenlos zur Verfügung.

Security

Ein einziger Sicherheitsverstoß kann jedes Unternehmen lahmlegen, Ressourcen binden, das Vertrauen der Kunden erschüttern und die Reputation der Marke beschädigen. Clevere Unternehmen verstärken ihre Schutzmaßnahmen, indem Sie Echtzeitdaten zur schnelleren Erkennung, Untersuchung und Behebung von Bedrohungen nutzen.

Mars gewinnt die richtigen Erkenntnisse

Mars Inc. wurde bereits 1911 gegründet und das Unternehmen kennt sich daher bestens mit Anpassungen an unterschiedliche Zeiten aus. Mars ist eines der größten privat geführten Unternehmen der USA und machte sich ursprünglich mit Süßigkeiten wie den Mars- und Milky Way-Riegeln, M&Ms und Snickers einen Namen. Im Laufe der Jahre hat das Unternehmen jedoch durch eine diskrete und aggressive Akquisitionsstrategie und die Übernahme von Unternehmen wie dem Kaugummigiganten Wrigley Jr. Company oder der Tierklinikette VCA Inc. massiv expandiert.

Eine ehrgeizige Akquisitionsstrategie erfordert die Fähigkeit, neue Akteure zu integrieren und gleichzeitig die Security- und IT-Monitoring-Services rasch und bedarfsgerecht auszubauen. Wenn neue Niederlassungen und Tochtergesellschaften eine eigene Infrastruktur und Cloud-Instanzen mitbringen, kann die Verwaltung der Umgebung schnell zur Herausforderung werden, insbesondere mit Blick auf die Sicherheit. Mithilfe von Splunk Data Stream Processor (DSP) kann das Security-Team aus zahlreichen, über das gesamte Portfolio der Mars-Niederlassungen und Tochtergesellschaften und deren SOC (Security Operation Centers) verteilten Tools ein einziges Repository mit sicherheitsrelevanten Daten erstellen. Durch das Zusammenführen der Daten an einem Ort, können Probleme schneller behoben und das allgemeine Sicherheitsniveau erhöht werden.

Angesichts unterschiedlicher, auf verschiedenen Plattformen gespeicherter Datenquellen brauchte Mars eine geeignete Plattform, um seinen Datenhunger zu stillen. „Mit DSP kann Mars die Anforderungen einer breiteren Gruppe von Akteuren erfüllen, die für das Monitoring unterschiedlicher Systeme und Plattformen auf

reaktionsschnelle, gut zugängliche Dashboards und Metriken angewiesen sind“, sagt Greg Poniatowski, Area Leader of Information Security bei Mars.

Anfangs wurde Splunk bei Mars im Kern der Security und IT Operations eingesetzt. Die Plattform entwickelte sich jedoch schon bald zum Standard-Analysetool aller Geschäftsbereiche des Konzerns und leistet weltweit einen Beitrag zur Förderung von Innovationen und Stärkung des Wettbewerbsvorteils. „Wir reifen mit dem System, und es hat sich gezeigt, dass Splunk auch die Lösung für unsere umfassenderen Probleme ist“, so Antonio Guedes, Security Analytics Senior Lead bei Mars. „Inzwischen haben wir mehr als 300 Benutzer, die mit Splunk alle per Self-Service eigene Erkenntnisse gewinnen.“



[Splunk Data Stream Processor] ermöglicht Mars die Anforderungen einer breiteren Gruppe von Akteuren zu erfüllen, die für das Monitoring unterschiedlicher Systeme und Plattformen auf reaktionsschnelle, gut zugängliche Dashboards und Metriken angewiesen sind.“

— Greg Poniatowski, Area Leader of Information Security bei Mars Inc.



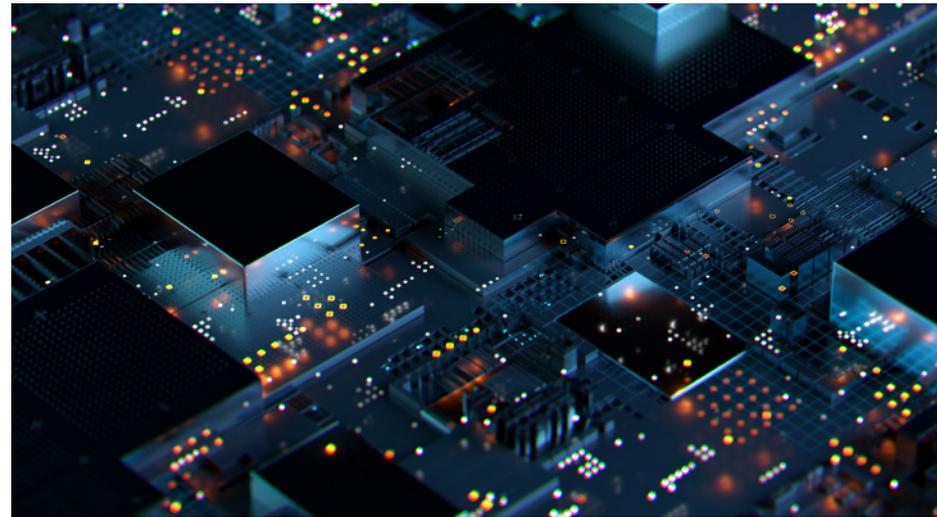
Intel revolutioniert die Bedrohungssuche

Intel hat sich im Laufe der Zeit von einem PC-orientierten zu einem datenorientierten Unternehmen gewandelt, das neue Produkte entwickelt, neue Märkte erschließt und auf innovative Weise neue Kunden gewinnt. Aufgrund dieser stärkeren Ausrichtung auf Daten musste Intels Abteilung für Informationssicherheit (InfoSec) eine umfassende „Defense-in-Depth“-Strategie entwickeln und verfolgen. Das Team automatisierte Präventions- und Erkennungstools auf vielen Ebenen und konnte damit 99 % der Bedrohungen für Intels Umgebung abdecken. Doch da blieb noch dieses eine Prozent.

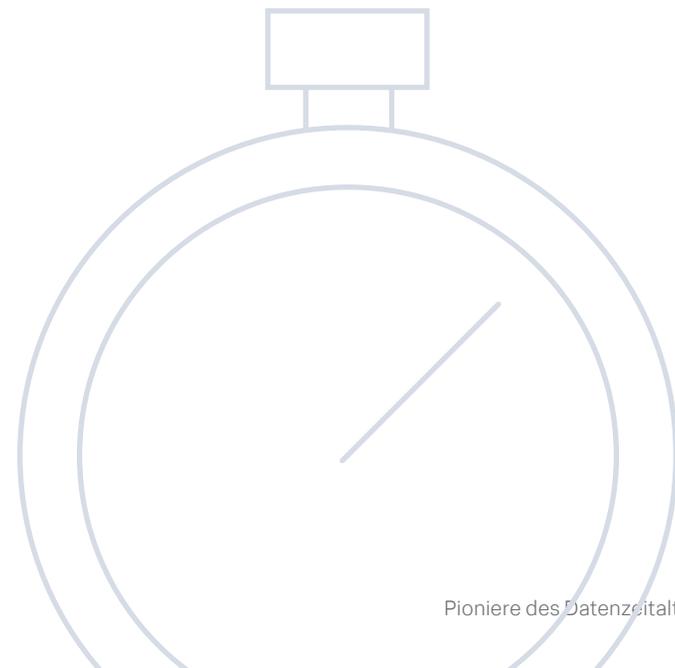
Bei Intel InfoSec mühte man sich mit einer veralteten SIEM-Lösung (Security Information and Event Management), die nicht mehr auf die stetig steigende Anzahl neuer Datentypen skalierbar war. Das Team brauchte eine Strategie zur Erkennung von hochkomplexen Bedrohungen für die Umgebung des Unternehmens – bei Intel InfoSec die „Jagd nach dem einen Prozent“ genannt. Aus dieser Strategie entsprang die Entwicklung der Cyber Intelligence-Plattform (CIP) von Intel, die auf Spitzentechnologien wie der Splunk-Plattform und Apache Kafka basiert.

Mit der Splunk Data-to-Everything Plattform und Hunderten von Drittanbieter-Tools verfügt Intel InfoSec nun über umfassende Transparenz, aussagekräftige Informationen und eine gemeinsame Arbeitsoberfläche und konnte die Effektivität in der gesamten Organisation steigern. Das Team ist nun in der Lage, Bedrohungen innerhalb von Stunden oder Minuten anstelle von Wochen oder Stunden zu erkennen und abzuwehren.

Das InfoSec-Team von Intel ist dabei, die Nutzung von Splunk und Kafka auszuweiten. Die Analysten und Datenwissenschaftler befassen sich mit dem Transformieren, Anreichern, Verknüpfen, Filtern und Bearbeiten von Daten im Datenstrom. Darüber hinaus fügt das Team weitere Machine Learning-Tools für unterschiedlichste Anwendungsfälle hinzu – von Incident Response, Betriebs- und Systemintegrität bis hin zur Workflow-Orchestrierung und Warnmeldungen.



Die Abteilung für Informationssicherheit bei Intel ist nun in der Lage, Bedrohungen innerhalb von Stunden bzw. Minuten anstelle von Wochen bzw. Stunden zu erkennen und abzuwehren.



Von den Besten lernen

Splunk hilft Unternehmen auf der ganzen Welt, u. a. 91 der Fortune 100, Barrieren zwischen Daten und Handlungen zu überwinden.

Auf den folgenden Seiten erhalten Sie mehr Informationen darüber, wie Datenpioniere aus verschiedenen Branchen die Data-to-Everything Plattform nutzen, um Systeme zu schützen, Prozesse zu straffen und Innovationen zu beschleunigen.

The background features a light blue topographic map with contour lines. A solid magenta line starts from the bottom left and curves upwards. A dashed orange line starts from the middle left and curves upwards, crossing the solid magenta line. A dotted grey line follows a path across the map.

Bildungswesen

Branche
Bildungswesen

Lösungen
IT Operations
Security
Splunk Remote Work Insights

Die University of Arizona stellt sich der Herausforderung der Pandemie und wahrt die Integrität ihres Netzwerks

Zentrale Herausforderungen

Als fast alle 60.000 Studenten, Dozenten und Mitarbeiter der University of Arizona (UArizona) plötzlich nicht mehr auf dem Campus arbeiten konnten, nutzte die Bildungsstätte Splunk Remote Work Insights (RWI), um die neuen Herausforderungen zu verstehen und zu meistern.

Wichtige Ergebnisse

Mit Splunk RWI gewann die UArizona einen vollständigen Überblick über ihr Netzwerk und Erkenntnisse darüber, ob Benutzer die Remote-Tools nutzten. So konnte die Universität ihre Funktion auch während des Lockdowns erfüllen.

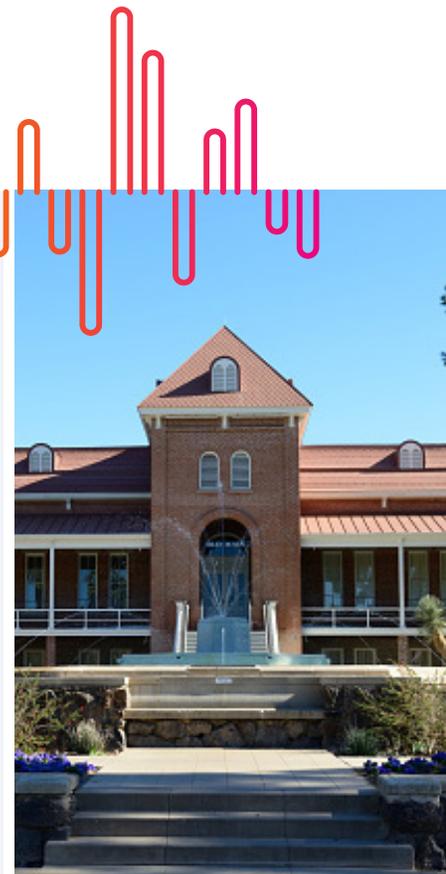
Nach dem COVID-19-Ausbruch musste die UArizona innerhalb von nur zwei Wochen auf Remote-Teaching, Remote-Learning und Remote-Work umstellen. Netzwerk-Traffic-Muster bewegten sich plötzlich außerhalb der Firewall, wodurch die Sicht auf die Servicenutzung eingeschränkt war, während die Anzahl der Studierenden, Mitarbeiter und Dozenten, die unsichere Verbindungen nutzten, anstieg. Dies brachte eine verschärfte Bedrohungslage für das Netzwerk der UArizona mit sich. Die Abteilung für IT-Sicherheit setzte Splunk RWI ein, um wieder einen Überblick über ihre Services zu bekommen und zu verstehen, wie Studierende und Mitarbeiter die Tools für die Remote-Arbeit nutzten.

Datengestützte Ergebnisse

Zusammenführung der Daten aus den VPN-, SSO- und MFA-Systemen der Bildungseinrichtung, WLAN-Nutzung und Zoom-Datenverkehr für **mehr Sicherheit und bessere Performance**

Entscheidungen und **Handlungen des Teams gründen sich jetzt auf reale Daten** statt auf bloße Annahmen

Mehr Effizienz und Sicherheit bei gleichzeitiger Erschließung neuer Datenquellen und Erkenntnisse, die als Entscheidungsgrundlage für IT, Netzwerkplanung und Marketing dienen



Mit der RWI-App hat es nur etwa fünf Stunden gedauert, all unsere Datenquellen einzubinden und alle Panels mit Daten aufzufüllen. Hätte ich das selbst machen müssen, dann hätte es Tage gedauert.“

— Paul Reeves, Principal Security Engineer an der University of Arizona

Branche
Bildungswesen

Lösungen
Datenmaskierung
Security
IT Operations
Unternehmerische Erkenntnisse



Datengestützte Ergebnisse

Gesundheits- und Leistungsoptimierung bei Sportlern durch die Nachverfolgung von Erschöpfungsgraden und weiteren wichtigen Gesundheitsdaten

Studierende können sich auf das Lernen konzentrieren statt auf Sicherheitsverstöße, da kompromittierte Konten schnell erkannt werden (Anzahl erkannter Konten verdoppelt)

Kostensenkung durch Datenmigration in Splunk Cloud

Die University of Illinois nutzt Daten, um Studierenden zum Erfolg zu verhelfen

Zentrale Herausforderungen

Die Daten befanden sich in isolierten Datensilos und waren für die meisten Mitarbeiter nicht zugänglich. Dadurch verzögerte sich die Lösung von Problemen und Mitarbeiter waren nicht in der Lage, Schwachpunkte der Studierenden auszumachen und den Erfolg zu messen.

Wichtige Ergebnisse

Dank des erweiterten Datenzugriffs konnte die Universität das Lernerlebnis und die Studierendenzufriedenheit durch eine genauere Einschätzung der Leistung und des Erfolgs der Studierenden verbessern.

An der University of Illinois sind Daten ein integraler Bestandteil jeder Entscheidung. Dank der „Student Success Initiative“ können die Mitarbeiter besser beurteilen, was die Studierenden brauchen, um erfolgreich zu sein. Anhand von Daten wird ermittelt, welche Studierenden Schwierigkeiten haben könnten. Mit diesen Erkenntnissen kann das Team gefährdeten Studierenden in Zusammenarbeit mit Beratern persönliche Betreuung und akademische Hilfe zukommen lassen. Das Frauenfußballteam trägt beim Training auf dem Spielfeld biometrische Sensoren und die Spielerinnen beantworten regelmäßig Umfragen, über die der Erschöpfungsgrad nachverfolgt wird. Die Daten werden mit Splunk analysiert und das IT-Team teilt den Trainern mit, wie sich die einzelnen Übungen auf die Spielerinnen auswirken.



Wir nutzen Splunk, um Erkenntnisse über unsere Studierenden, Mitarbeiter, Dozenten und Forscher umzusetzen. So können wir den Studierenden zu einer besseren Erfahrung verhelfen und Forschern und Dozenten die richtigen Tools zur Verfügung stellen.“

— Nick Vance, Manager of Data and Technology Innovation an der University of Illinois

Jefferson County Public Schools ermöglicht sicheres Lernen im 21. Jahrhundert

Zentrale Herausforderungen

Im Rahmen der Modernisierung des Lernumfelds sollten Computerressourcen für Schüler jederzeit und überall verfügbar sein. Dies erforderte wiederum eine längere Uptime und der Schulbezirk sah sich mit neuen Sicherheitsschwachstellen konfrontiert.

Wichtige Ergebnisse

Jefferson County Public Schools (Jeffco) bietet nun ein geschütztes, innovatives Lernumfeld mit optimierter Sicherheit, höherer Zuverlässigkeit und einem besseren Schutz vor Cybermobbing.

Als Jeffco ein WLAN-Netzwerk einrichtete, um den Schülern Computerressourcen zur Verfügung zu stellen, wurde die Organisation damit auch anfällig für Diebstähle von Kontozugangsdaten und unberechtigte Zugriffe. Vor der Bereitstellung von Splunk mussten Untersuchungsteams zahlreiche Systemprotokolle durchforsten, um die Quelle von Malware oder Phishing-Angriffen zu ermitteln. Mit der Splunk-Plattform können die Mitarbeiter von Support Center und Service Desk nun schnell handeln, wenn ein Benutzer auf einen Phishing-Link klickt, Zugangsdaten stiehlt oder ein Konto kompromittiert. Die Splunk-Plattform unterstützt Jeffco auch bei der Bekämpfung von Cybermobbing, da das Team die Systemnutzung, Benutzer und Geräte nachverfolgen kann.



Unsere größte Herausforderung bestand darin, unseren Lehrern und Schülern die Flexibilität zu bieten, Inhalte zu erstellen und innovativ zusammenzuarbeiten und dabei gleichzeitig die Datensicherheit in unserer verteilten, komplexen Umgebung zu gewährleisten.“

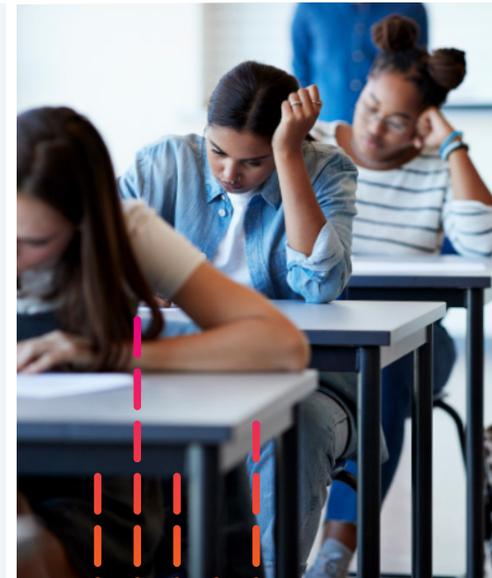
— Chris Paschke, Director of Data Privacy and Security,
Jefferson County School District (Colorado)

Datengestützte Ergebnisse

86 Tsd. Schüler und 15 Tsd. Mitarbeiter an 156 Standorten profitieren von zuverlässigen IT-Services

99,99 % WLAN-Verfügbarkeit ermöglicht Schülern ein Lernen ohne IT-Unterbrechungen

100 Tsd. Geräte auf einer Fläche von etwa 1.800 Quadratkilometern mit verbesserter Sicherheit



Branche
Bildungswesen

Lösungen
Security
Betrugsbekämpfung
Unternehmerische Erkenntnisse



Datengestützte Ergebnisse

780 Tsd. USD Einsparung durch Betrugsbekämpfung bei Gehaltsabrechnungen und Direktüberweisungen für mehr als 14.600 Mitarbeiter

30 Tsd. USD Einsparung alle zwei Wochen durch den Schutz der jährlichen Lohnsumme der ASU in Höhe von von 889 Mio. USD

150 Tsd. Studierende, Dozenten und Mitarbeiter profitieren von einer verbesserten Erfahrung auf dem Campus



Wir haben bei der ASU über 150.000 Studierende, Dozenten und Mitarbeiter. Aus verschiedensten Quellen erreichen uns kontinuierlich neue Daten. Mit Splunk haben wir jetzt Einblicke in die Erfahrungen der Studenten. Wir können Daten erfassen, zusammenführen und Berichte erstellen. So können wir schneller denn je geschäftliche Entscheidungen treffen.“

— Nate Plamondon, Splunk Architect an der Arizona State University

Arizona State University erhält Echtzeiteinblicke in die Studierendenerfahrung

Zentrale Herausforderungen

Ursprünglich ging es für die Arizona State University (ASU) darum, Splunk für mehrere Security-Anwendungsfälle einzusetzen und Studierende und Dozenten vor Betrug zu schützen.

Wichtige Ergebnisse

Mit Splunk konnte die ASU Betrug bei Gehaltsabrechnungen und Direktüberweisungen für ihre mehr als 14.600 Mitarbeiter mit einer jährlichen Lohnsumme von 889 Millionen USD beträchtlich reduzieren. Nun werden Daten auch genutzt, um die Erfahrungen der Studierenden umfassend zu verbessern.

Nach dem beeindruckenden Erfolg mit Splunks fortschrittlichen Monitoring- und Benachrichtigungslösungen weitete die ASU die Nutzung der Splunk-Plattform aus und konsolidiert nun wichtige Daten, um die Erfahrung der Studierenden auf dem gesamten Campus besser zu verstehen. Mitarbeiter der Universität können jetzt Probleme der Studierenden schneller beheben, wichtige geschäftliche Fragen beantworten und die Studierendenerfahrung durch eine bessere WLAN-Verfügbarkeit, Kursvorschläge und vieles mehr verbessern. Dank zuverlässigerer Daten kann die ASU ihre Mission vorantreiben und ein sicheres Bildungsumfeld für Studierende und Dozenten bereitstellen.

The background features a topographic map with light blue contour lines. A path is drawn across the map, starting as a solid magenta line on the left, transitioning to a solid orange line in the middle, and ending as a dashed orange line on the right. The path appears to rise and then level out towards the right side of the image.

Finanzdienstleister

Branche
Finanzdienstleister

Lösungen
Log-Management
IT Operations
Security
Betrugsbekämpfung

au **Kabucom Securities** erhöht die Cybersicherheit und erhält Zugriff auf neue, wertvolle Datenquellen

Zentrale Herausforderungen

Nach einem DDoS-Ausbruch im Jahr 2017 entschied sich au Kabucom Securities für einen automatisierten DevSecOps-Ansatz, um die Cybersicherheit zu erhöhen und alle Daten zu visualisieren und zu analysieren – auch möglicherweise wertvolle Dark Data.

Wichtige Ergebnisse

Durch das Erkennen verdächtigen Verhaltens, das Auslösen von Warnmeldungen und das Analysieren von Logs ermöglichte Splunk au Kabucom Securities die vollständige Automatisierung von DevSecOps.

au Kabucom Securities gehört zur Mitsubishi UFJ Financial Group und bietet Online-Brokerage-Services für mehr als 1,1 Millionen Kunden in ganz Japan an. Dank Splunk führt au Kabucom Securities nun Protokolle aus mehreren Cloud-Services in einer einzigen Konsole zusammen. Das Team wertet diese wertvollen Daten aus und analysiert sie, um Muster vorherzusagen, die Berichterstellung zu zentralisieren und in Echtzeit Einblick in das Sicherheitsniveau des Unternehmens zu gewinnen. Die Benutzerfreundlichkeit und Skalierbarkeit der Splunk-Plattform ermöglichen es dem Unternehmen, sein großes Datenvolumen kostengünstig zu verwalten. Gleichzeitig können Bedrohungen dank Korrelationsanalyse mit externer Threat Intelligence wirkungsvoll abgewehrt werden.

INHALT



Splunk hilft uns dabei, aus ungenutzten Datenbeständen maximalen Wert zu schöpfen und steigert damit stetig unsere Wettbewerbsfähigkeit.“

— Yoichi Ishikawa, Assistant Executive des General Managing Officer of System, System Development Department und Deputy General Manager, IT Strategy Group bei au Kabucom Securities Co., Ltd.



Datengestützte Ergebnisse

Automatisierung zeitintensiver Aufgaben ermöglicht Stressabbau im Team und Fokussierung auf strategische Programme

Optimierte Kundenerfahrung durch schnellere Untersuchung und Behebung kritischer Probleme

Verfügbarmachung weiterer wertvoller Daten – strukturierter und unstrukturierter – als Grundlage für Analysen und Entscheidungen

Datengestützte Ergebnisse

1 Billion USD an Transaktionsvolumen wird täglich von sicherer Infrastruktur geschützt

10 Tsd. Endpunkte, bestehend aus Servern und Benutzergeräten, sind dank Analysen zur schnellen Erkennung potenzieller Angriffe sicher

1/3 des BIP mit proaktiver Verteidigungsstrategie geschützt



Bank of England

schützt tagtäglich 1 Billion US-Dollar

Zentrale Herausforderungen

Die Bank of England musste ihr SOC von einem eher reaktiven auf einen proaktiven Ansatz umzustellen und erkannte, dass sie ein neues Betriebsmodell brauchte, und zwar eines, bei dem die Technologie zum Modell passte und nicht umgekehrt.

Wichtige Ergebnisse

Die Splunk-Plattform trägt entscheidend dazu bei, dass die Bank of England nun großangelegtes Data Mining, Log-Analysen, den Abgleich von Bedrohungsinformationen und präventive Kontrollen durchführen kann.

Die 1694 gegründete Bank ist die Zentralbank des Vereinigten Königreichs und ermöglicht täglich Transaktionen, die sich auf ein Drittel des BIP des Landes belaufen. Das SOC der Bank ist mit seinem Team von zehn Sicherheitsanalysten für den Schutz der Infrastruktur verantwortlich, die diesen Transaktionen zugrunde liegt. Da sich mit Splunk schnell iterative Suchen erstellen lassen, können Analysten jetzt eine breite Palette von Analysen entwickeln, die mehr Flexibilität und Effizienz bei der Erkennung von Angriffen bieten. Durch die Implementierung von Splunk konnte das SOC zudem seine Verteidigungsstrategie ändern und sich auf die Abwehr feindlicher Operationen innerhalb des MITRE ATT&CK-Frameworks der Bank anstatt auf den eigentlichen Angriff konzentrieren. Damit verzeichnet das Institut deutlich mehr Erfolg bei der Abwehr von Bedrohungen.

Keystart steigert die Produktivität und räumt der Compliance höchste Priorität ein

Zentrale Herausforderungen

Vor dem Einsatz von Splunk hatte Keystart keine formalisierten Sicherheitsprogramme oder -systeme und rechnete bei der Verwaltung seiner umfangreichen Security-Datasets mit hohen Implementierungskosten und vielen Ressourcenstunden.

Wichtige Ergebnisse

Mit Splunk als SIEM konnte das Unternehmen die Reaktionszeit bei Incidents verkürzen, Kosten senken und die Einhaltung staatlicher Normen vereinfachen.

Als privat geführter, staatseigener Hypothekengeber mit Sitz in Westaustralien kam es für Keystart vor allem auf die Datensicherheit und Einhaltung gesetzlicher Anforderungen an. Gleichzeitig galt es, Wohnraum in Perth und im gesamten Bundesstaat erschwinglich zu machen. Mit Splunk stand Keystart eine flexible, kostengünstige Lösung zur Verfügung, dank derer Altsysteme ad acta gelegt und ersetzt und Daten an einem zentralen Ort zusammengeführt werden konnten. Da die aktuell eingesetzten Splunk-Anwendungen unmittelbare Erfolge brachten, prüft Keystart nun im gesamten Unternehmen weitere Use Cases, beispielsweise die Nutzung von Splunk für Business Analytics und als Business Intelligence-Tool.



Bevor wir Splunk eingesetzt haben, musste ich intern mehrere Anwendungen programmieren, um einen umfassenden Überblick über unser in Silos organisiertes System zu bekommen. Mit den Warnmeldungen von Splunk und einer einheitlichen, zentralen Sicht auf unsere Systeme konnten wir die Reaktionszeit bei Incidents um 75 % verkürzen und unsere Produktivität mindestens vervierfachen.“

— Sean Smart, Information Security Officer bei Keystart

Datengestützte Ergebnisse

75 % kürzere Reaktionszeiten bei Incidents

4-fache Produktivitätssteigerung durch Splunk-Benachrichtigungen und eine zentrale Sicht auf die Systeme

Über 2 Mio. Events werden täglich geprüft

Aflac setzt auf die Splunk-Plattform für analysegestützte Cyber Security

Zentrale Herausforderungen

Angesichts eines rapiden Wandels der Bedrohungslandschaft benötigte Aflac eine zuverlässige Sicherheitsplattform, um seine Kunden, 10.000 Mitarbeiter und die Markenreputation zu schützen.

Wichtige Ergebnisse

Aflac hat Bedrohungsinformationen aus 20 Sicherheitstechnologien orchestriert und einen analysegestützten Sicherheitsansatz mit sofortigem Return-on-Investment konzipiert.

Aflac ist der führende Anbieter von freiwilligen Versicherungen in den USA. Angesichts einer Flut von Sicherheitsbedrohungen setzte Aflac die Splunk-Plattform ein, um die Bedrohungsinformationen aus 20 Sicherheitstechnologien in seinem internen Threat Intelligence-System zu orchestrieren. Splunk bildet nun das Kernstück des SOC von Aflac. Sechs Teams mit ca. 40 Mitarbeitern verlassen sich auf die Splunk-Plattform, um eine breite Palette von sicherheitsbezogenen Anwendungsfällen zu verwalten – von der Bedrohungssuche und Reaktion auf Incidents bis hin zur Anwendungssicherheit, Sicherheitsverwaltung und Betrugsbekämpfung. Das System bietet taktische und strategische Funktionen und jetzt auch eine Automatisierung, durch die der tägliche Bedrohungsdaten-Feed effizienter wird, die Fehlerrate sinkt und Daten für jede Entscheidung verwendet werden können.

[Video ansehen](#)

INHALT



Als Versicherungsnehmer möchte ich gern davon überzeugt sein, dass die Versicherung alles tut, damit meine Daten geschützt bleiben. Wir achten sehr auf die Verwaltung unserer eigenen Daten und auch auf den Datenschutz unserer Versicherungsnehmer. Mit Splunk ist das ganz einfach.“

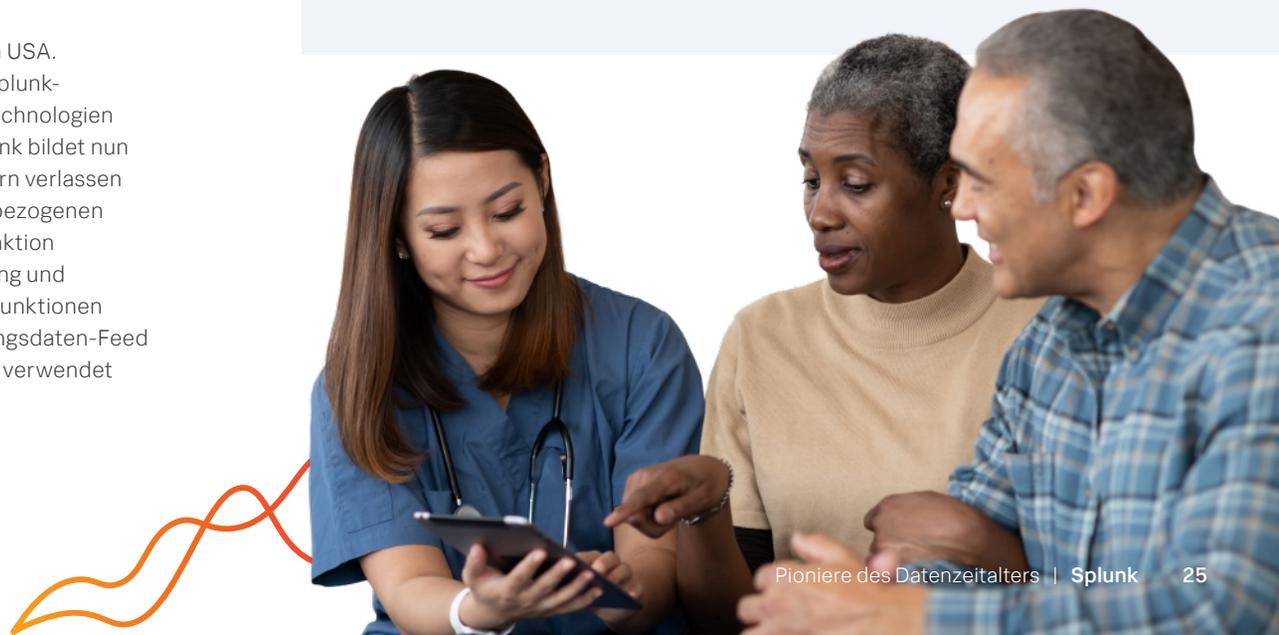
— Ben Murphy, Vice President of Information Security bei Aflac Incorporated

Datengestützte Ergebnisse

2 Wo. bis zur unternehmensfertigen Implementierung

2 Mio. Sicherheitsbedrohungen in sechs Monaten blockiert

40 Std. pro Monat durch Ersetzen manueller Prozesse eingespart



Branche
Finanzdienstleister

Lösungen
IT Operations
Infrastruktur-Monitoring
Security



Datengestützte Ergebnisse

< 2 Min. MTTA mit Splunk und Splunk On-Call (ehemals VictorOps) im Vergleich zu 4 Stunden vor dem Einsatz von Splunk

3,8 Mrd. Transaktionen durch optimierte Zusammenarbeit und Enterprise-Funktionen ermöglicht

Mehr als 1.500 Kreditgenossenschaften mit mobilem Monitoring und Echtzeit-Benachrichtigungen unterstützt



Jede IT-Abteilung bei der PSCU verwaltet einen Bereitschaftsplan. VictorOps bringt alle Manager mit einem Tool zusammen. Wir wissen, was wir tun und verwenden alle denselben Eskalationsplan. So wird das Verantwortungsgefühl gestärkt.“

— Earl Diem, IT Operations Manager bei PSCU

PSCU verkürzt die MTTA und sorgt für mehr Sicherheit

Zentrale Herausforderungen

Um die Produkt- und Service-Verfügbarkeit für mehr als 1.500 Kreditgenossenschaften zu verbessern, musste die PSCU die MTTA und MTTR verkürzen und gleichzeitig das Verantwortungsgefühl der Bereitschaftsteams stärken.

Wichtige Ergebnisse

Mit der Data-to-Everything Plattform verkürzte die PSCU die MTTA und MTTR und ermöglichte den Mitarbeitern Monitoring-Zugriff über Mobilgeräte, damit sie von überall aus Unterstützung bieten können.

Als größte Dienstleistungsgesellschaft für Kreditgenossenschaften in den USA ist es die Aufgabe der PSCU, den Kreditgenossenschaften im Wettbewerb mit den Banken eine bessere Position zu verschaffen. Zu diesem Zweck setzt die PSCU auf Splunk, um Fehler zu ermitteln und Incidents rascher zu beheben. Splunk On-Call (ehemals VictorOps) ist Teil der Splunk-Plattform und bietet den Bereitschaftsteams eine automatisierte Incident Management-Weiterleitung, durch die sich die MTTA von vier Stunden auf weniger als zwei Minuten senken ließ. Nun entschied sich die PSCU, Splunk auch noch in weiteren Anwendungsfällen einzusetzen, u. a. zum Gewinnen vorausschauender Erkenntnisse und zur schnelleren Fehlererkennung bei neuen Software-Versionen. Dank der einheitlichen Plattform von Splunk kann die PSCU jetzt schneller innovative Lösungen finden, die Zusammenarbeit optimieren und die Bedürfnisse der Kunden zufriedenstellen.

[Video ansehen](#)

The background features a topographic map with light blue contour lines. A path is drawn across the map, starting as a solid magenta line on the left, transitioning to a solid orange line, and ending as a dashed orange line on the right. A faint dotted line also traces a path across the map.

Gesundheitswesen

NewYork-Presbyterian bekämpft Opioid-Problematik mit Daten

Zentrale Herausforderungen

NewYork-Presbyterian musste Daten aus elektronischen Gesundheitsakten, Apothekensystemen und anderen Quellen nachverfolgen, um herauszufinden, ob Medikamente für möglicherweise illegale Zwecke entwendet wurden.

Wichtige Ergebnisse

In Partnerschaft mit Splunk baute NewYork-Presbyterian eine Plattform auf, die eine enge Überwachung von Betäubungsmitteln und anderen Medikamenten erlaubt und das Entwenden von Opioiden eindämmt.

Das NewYork-Presbyterian Hospital ist einer der größten Gesundheitsversorger mit Universitätsangliederung der USA. Anfangs nutzte das Krankenhaus Splunk für eine Reihe von Sicherheitsanwendungsfällen von der Abwehr von Phishing-Angriffen bis hin zur Automatisierung wichtiger Security-Workflows. Beim Aufbau des SOC stießen die Verantwortlichen des NewYork-Presbyterian dann auf weitere nützliche Splunk-Funktionen und entwickelten in Zusammenarbeit mit Splunk eine angepasste Plattform, die unbefugte Zugriffe auf Patientenakten und die Entwendung von Opioiden verhindert. Die Korrelations- und Machine Learning-Funktionen von Splunk, die für die Patientenplattform von grundlegender Bedeutung waren, versetzen das Krankenhaus nun in die Lage, die Opioid-Problematik auf globaler Ebene zu bekämpfen.



Datengestützte Ergebnisse

Schutz vor der Entwendung von Opioiden und hochpreisigen Medikamenten wie z. B. bestimmten Krebsmedikamenten, die mehrere Zehntausend US-Dollar kosten können

Monitoring der IT-Sicherheitsprozesse, um dafür zu sorgen, dass Betäubungsmittel und andere Medikamente nicht illegal eingesetzt oder verschrieben werden

Möglichkeiten für vergleichbare Institutionen, in ihren Krankenhäusern dieselben Monitoring-Methoden anzuwenden



Mit Splunk haben wir nahezu unbegrenzte Möglichkeiten zur Nutzung von Daten im Krankenhaus. Wir wollen den Einsatz von Splunk weiter ausbauen und diese Partnerschaft vorantreiben, und zwar nicht nur für uns, sondern für das Gesundheitswesen im ganzen Land.“

— Jennings Aske, Senior Vice President und Chief Information Security Officer

Branche
Gesundheitswesen

Lösungen
IT Operations
DevOps
Container-Monitoring
Security
Compliance



Datengestützte Ergebnisse

150-500 GB Daten pro Tag von Splunk abgefragt

100 % der Produktions-Incidents mit Automatisierung und Runbooks abgewickelt

Mehr Zeit für wertschöpfende Aufgaben und Kernursachenanalysen im DevOps-Team

Imprivata verwaltet und schützt die Container-Umgebung mit Splunk Cloud

Zentrale Herausforderungen

Imprivata benötigte in einer stark verteilten, containerisierten Produktions- und Entwicklungs-Umgebung eine sichere, zentrale Protokollierung und Ad-hoc-Abfragefunktionen.

Wichtige Ergebnisse

Dank Splunk Cloud können sich die DevOps-Teams von Imprivata nun auf Geschäftsanforderungen mit hoher Priorität konzentrieren und die Sicherheits-Compliance wurde optimiert. Die hohen Kosten einer lokalen Speicherung konnten vermieden werden.

Der Umstieg auf Splunk Cloud ermöglicht Imprivata, wichtige Erkenntnisse aus Maschinendaten zu gewinnen, ohne eine Infrastruktur verwalten zu müssen. Mit Splunk Cloud wird die Compliance mit HIPAA (Health Insurance Portability and Accountability Act) und weiteren gesetzlichen Vorgaben zum Kinderspiel, darunter SOC 2 Typ II und die DSGVO (Datenschutz-Grundverordnung). Darüber hinaus ermöglicht Splunk Cloud den Mitarbeitern des NOC (Network Operations Center) die Abwicklung aller Incidents in der Produktionsumgebung mit Automatisierung und Runbooks. Dadurch wird eine weitere Eskalation zu DevOps verhindert und die MTTR (Mean-Time-To-Repair) erheblich gesenkt. Durch die proaktive Problembehebung werden Auswirkungen auf den Service vermieden.



Dank Splunk Cloud kann ich meinen Schwerpunkt von administrativen Aufgaben auf die Unterstützung meines Teams und anderer Personen im gesamten Unternehmen verlagern, Analysen des Geschäfts und von Kernursachen durchführen und konkrete Ergebnisse anvisieren.“

— Manager, Cloud Platform Team bei Imprivata



Molina Healthcare verschafft sich einen gesunden Vorteil

Zentrale Herausforderungen

Molina Healthcare musste die Verfügbarkeit seiner umsatzgenerierenden Anspruchs-Engine sicherstellen und eine schnellere Möglichkeit finden, Sicherheits- und IT-Incidents zu erkennen und zu beheben.

Wichtige Ergebnisse

Das Molina-Team nutzt Splunk, um Probleme innerhalb von Minuten zu lösen, IT-Incidents zu reduzieren, die Verfügbarkeit der Anspruchs-Engine zu erhöhen und den Zeitaufwand für die Abstimmung mit mehreren funktionsübergreifenden Teams und Tools zu senken.

Molina Healthcare sorgt für die Bereitstellung von Managed Care-Leistungen im Rahmen der Medicaid- und Medicare-Programme und nutzt Splunk, um operative Daten in umsetzbare Erkenntnisse zu verwandeln und die Patientenversorgung zu optimieren. Mit Splunk Enterprise und Splunk ITSI erhält Molina eine Echtzeitübersicht über die Daten im gesamten Unternehmen. Früher hatten Ausfälle der Anspruchs-Engine negative Auswirkungen auf den Umsatz. Durch die neue Transparenz der IT-Systeme kann das Team die Verfügbarkeit der Anspruchs-Engine – das Herzstück des Unternehmens – nun kontinuierlich sicherstellen. Manuelle Prozesse werden reduziert und alles besser mit den Betriebsabläufen abgestimmt.

Datengestützte Ergebnisse

63 % geringere MTTR bei Molina

Reduzierung der IT-Incidents auf **1/5** der ursprünglichen Anzahl seit Einsatz von Splunk

4,2 Mio. Personen profitieren dank Data Mining und der Vorhersagbarkeit von Trends von besseren Gesundheitsdiensten



Der Versuch, eine ähnliche Lösung mit den vorhandenen Tools zu implementieren, hätte unzählige Arbeitsstunden und Millionen Dollar für Professional Services und Upgrades verschlungen.“

— Ben Gordon, Vice President Enterprise Infrastructure Services bei Molina Healthcare

The background is a topographic map with light blue contour lines. A path is drawn across the map, starting as a solid magenta line on the left, transitioning to a solid orange line, and ending as a dashed orange line on the right. The word 'Fertigung' is written in a bold, sans-serif font, with 'Fert' in orange and 'igung' in magenta.

Fertigung

Branche
Fertigung

Lösungen
IT Operations
AIOps
IoT und Industrie 4.0
Predictive Analytics
Business Analytics



Datengestützte Ergebnisse

Umsetzung der Nachhaltigkeitsziele durch erfolgreiche Markteinführung des ersten elektrischen Sportwagens Porsche Taycan

Performance-Optimierung für 2.000 Taycan-Ladestationen weltweit

Verbesserung der digitalen Kundenerfahrung durch proaktives Monitoring und bessere Analyse der Customer Journey

Porsche treibt intelligente Performance und Nachhaltigkeit an

Zentrale Herausforderungen

Porsche musste innovative, zukunftsorientiert Software entwickeln und eine auf die Kunden zugeschnittene digitale Premiererfahrung liefern, um in puncto Innovation und Performance weiterhin ganz vorn dabei zu bleiben.

Wichtige Ergebnisse

Porsche nutzt die Splunk-Plattform, um in allen Bereichen intelligente Performance zu bieten, von der Porsche Connect-App über die digitale Customer Journey bis hin zum Porsche Taycan, dem ersten elektrischen Sportwagen des Unternehmens.

Porsches Partnerschaft mit Splunk entstand 2015 mit Porsche Connect, einer App, mit der Fahrer Remote-Zugriff auf ihr Fahrzeug erhalten. Heute basiert auch Porsches digitaler Support auf Splunk. Die Plattform wird genutzt, um Einblicke in die Customer Journey zu bekommen und Probleme proaktiv zu verhindern, bevor sie sich auf die Kunden auswirken. Porsche nutzt Splunk darüber hinaus, um bei seinem ersten elektrischen Sportwagen – dem Porsche Taycan – und mehr als 2.000 Ladestationen auf der ganzen Welt intelligente Performance und Nachhaltigkeit verschmelzen zu lassen.

[Video ansehen](#)



Daten stehen bei uns im Mittelpunkt und Splunk ist ein großartiger Partner, der uns wirklich hilft, Daten in Taten zu verwandeln.“

— Stefan Arnold, Head of Technology Acceleration & Management bei Porsche

Branche
Fertigung

Lösungen
Security
Unternehmerische Erkenntnisse
IT Operations



Mars macht eine Punktlandung und baut Datenfunktionen aus

Zentrale Herausforderungen

Angesichts einer aggressiven Akquisitionsstrategie und immer datenhungrigeren Teams musste Mars die Anforderungen von IT-, Security- und Business-Bereichen in sehr unterschiedlichen Niederlassungen und Tochtergesellschaften erfassen.

Wichtige Ergebnisse

Dank der Splunk-Plattform verfügt Mars nun über eine einzige, umfassende Sicht auf alle Datenquellen und profitiert von umgehenden Benachrichtigungen, proaktiver Optimierung und verbesserter Entscheidungsfindung im gesamten Unternehmen.

Mit Splunk kann Mars den unterschiedlichen Akteuren gezielte Rückmeldungen zu Problemen in ihren Prozessen geben. Wo früher nur ganz allgemein auf Probleme hingewiesen werden konnte, kann das Mars-Team jetzt fast in Echtzeit verbindliche Anweisungen geben, um die Problembehebung zu beschleunigen. Die Streaming-Analyse-Funktionen von Splunk Data Stream Processor (DSP) helfen bei der Optimierung von Infrastruktur und Ressourcen. Mit DSP kann das Security-Team aus zahlreichen, über das gesamte Portfolio der Mars-Niederlassungen und -Tochtergesellschaften und deren SOCs (Security Operation Centers) verteilten Tools ein einziges Repository mit sicherheitsrelevanten Daten erstellen. So lässt sich die Problembehebung beschleunigen und das allgemeine Sicherheitsniveau erhöhen.

Datengestützte Ergebnisse

Erweiterung des Datenzugriffs für mehr als **300 Mitarbeiter** weltweit und Austausch von Erkenntnissen mit SOCs und NOCs unterschiedlicher Niederlassungen und Tochtergesellschaften

Weltweite Optimierung der Cloud-Performance durch zentrale Kontrolle und Optimierung

Filtern und Normalisieren von Daten **zur optimalen Nutzung der Rechenleistung** und Infrastruktur



Wir reifen mit dem System und es hat sich gezeigt, dass Splunk die Lösung für unsere übergeordneten Probleme ist. Inzwischen haben wir mehr als 300 User, die mit Splunk alle per Self-Service eigene Erkenntnisse gewinnen.“

— Antonio Guedes, Security Analytics Senior Lead bei Mars Inc.

Branche
Fertigung

Lösungen
Log-Management
Security
Betrugsbekämpfung

Nikko Chemicals schafft die sichere Cloud-Migration

Zentrale Herausforderungen

Nach dem starken Erdbeben vor der japanischen Küste und den darauffolgenden Tsunamis im Jahr 2011 startete Nikko Chemicals eine Initiative zur Migration in die Cloud, um die Business Continuity-Planung zu verbessern.

Wichtige Ergebnisse

Mit Splunk gelingt es Nikko Chemicals problemlos, sicherheitsrelevante Logs aus einer breiten Palette von Anwendungen zu sammeln, Transparenz zu schaffen und einen zentralen Überblick über alle SaaS-Bereitstellungen zu gewinnen.

Dank Splunk Cloud führt Nikko Chemicals Logs nun in einer einheitlichen Plattform zusammen und zentralisiert das SOC-Monitoring in einem einzigen Knoten. So werden die Kosten auf ein Minimum reduziert und Korrelationsanalysen von SaaS-Anwendungen ermöglicht, sodass das Team die Sicherheit erhöhen und mehr Entscheidungen im gesamten Unternehmen auf eine solide Datengrundlage stellen kann. Das Log-Monitoring erfolgt jetzt rund um die Uhr, Log-Analysen werden über einen externen SOC-Service abgewickelt. Dank dieser Verbesserungen kann Nikko Chemicals seine Daten in Taten verwandeln, unvorhergesehene Ausreißer automatisch erkennen und in Echtzeit auf Events reagieren.



Splunk ist jeden Penny wert und bietet für Unternehmen wie das unsere, mit personell schwach besetzten Operations-Teams, beispiellosen Mehrwert und ungeahnte Möglichkeiten.“

— Yuichi Higashihara, Security Management Division bei Nikko Chemicals Co., Ltd.



Datengestützte Ergebnisse

Automatisierter Cloud-Betrieb mit einem ganzheitlichen Blick auf zahlreiche SaaS-Anwendungen

Maximierte Unternehmenssicherheit durch zentralisierten und proaktiven Schutz vor Bedrohungen

Effizienzsteigerung durch vereinfachte Prozesse und mühelose Systemwartung

Branche
Fertigung

Lösungen
IT Operations
Industrie 4.0 und IoT



Datengestützte Ergebnisse

Tiefgreifende Einblicke in historische und Echtzeit-Betriebsdaten von Tausenden IoT-Geräten

Anstieg der Kundenzufriedenheit und besserer Service mit höheren Anlagenbetriebszeiten

Vorausschauende Instandhaltung für schnellere Fehlerbehebung und bessere Ressourcenzuweisungen

Zeppelin setzt neue Maßstäbe bei der vorausschauenden Instandhaltung

Zentrale Herausforderungen

Das deutsche Industrieunternehmen musste Ausfallzeiten senken und benötigte zudem eine skalierbare Lösung für den Servicebereich mit Monitoring-Möglichkeiten aus der Ferne für vermietetes Equipment durch die Analyse von Sensordaten.

Wichtige Ergebnisse

Mit Splunk konnte Zeppelin seine IT-Systeme optimieren, die Fehlerbehebung mit vorausschauender Instandhaltung und Analysen beschleunigen und die Anlagenbetriebszeiten für die Kunden erhöhen.

Zeppelin stellt Maschinen und Geräte für Branchen wie den Bausektor, Bergbau und Landwirtschaft her und ist darüber hinaus wachstumsorientiert. Das Unternehmen ist dabei, seinen Servicebereich auszuweiten und neue digitale Modelle für den Bausektor zu entwickeln. Auch die IT-Infrastruktur von Zeppelin ist größer und komplexer geworden. Durch die Nutzung der Splunk-Plattform für seine IT Operations und IoT-Geräte verfügt Zeppelin nun über eine einheitliche, verschlankte Lösung, kann Maschinenausfälle vorhersagen und Probleme im Ansatz unterbinden, die Betriebszeit von Maschinen und Geräten maximieren, den Kundenservice verbessern und maximalen Wert aus seinen Daten schöpfen.

[Video ansehen](#)



Mit Splunk haben wir einen innovativen Partner, der uns dabei unterstützt, Herausforderungen mit Daten anzugehen. Für uns ist das die Zukunft.“

— Andreas Zientek, Systems Engineer bei Zeppelin

Branche
Fertigung

Lösungen
Industrie 4.0 und IoT
IT Operations
Unternehmerische Erkenntnisse

Der führende Anbieter von Bodenbelagslösungen, **Shaw Industries**, bricht Produktionsrekord mit Splunk IoT

Zentrale Herausforderungen

Die Shaw Industries Group brauchte in ihrer Fertigung Zugriff auf Echtzeitdaten, um die Produktionsleistung zu erhöhen und ihre Wettbewerbsposition zu verteidigen.

Wichtige Ergebnisse

Seit Shaw Industries die Splunk-Plattform einsetzt, konnten die Durchlaufzeiten für Arbeitsaufträge verbessert, der Output von Produktmustern erhöht und das Gewinnen unternehmerischer Erkenntnisse beschleunigt werden.

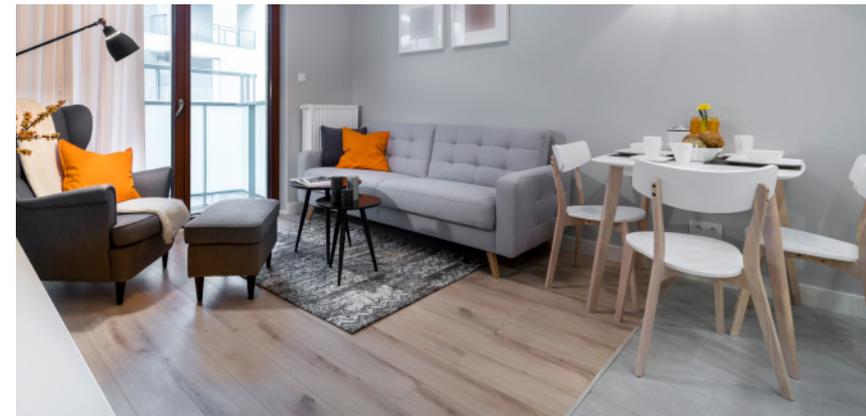
Ursprünglich hat Shaw Industries die Splunk-Plattform eingeführt, um einen Einblick in eine neue Post-Consumer-Recyclinganlage zu ermöglichen. Heute sind annähernd 300 Führungskräfte und Techniker im Erstellen von Splunk-Suchen für ihre Maschinen- und Unternehmensdaten ausgebildet. Werksleiter und Produktionsleiter nutzen Splunk-Dashboards für wichtige unternehmerische Erkenntnisse. Dank eines Splunk-Dashboards für Effizienzdaten, das die Produktion in Echtzeit abbildet, konnte das Werk seine Produktionsleistung durch gezielte Prozessverbesserungen mehr als verdoppeln. Insgesamt hat Shaw durch das Erfassen und Analysieren von Fertigungs- und industriellen Sensordaten in Echtzeit mehr Transparenz geschaffen und Einblicke in geschäftskritische Aspekte wie Qualität und Performance gewonnen.

[Video ansehen](#)



In der vergangenen Woche haben wir den Rekord für produzierte Paneele gebrochen, also trägt Splunk zum Wandel unseres unternehmerischen Handelns bei.“

— Gabriel Gerges, Department Manager, Samples Division bei Shaw Industries Group, Inc.



Datengestützte Ergebnisse

Verbesserte Durchlaufzeiten für Arbeitsaufträge, sodass Kunden schnell bedient werden können

Signifikant **erhöhter Produktionsoutput der Musterproduktion**

Verringerter Energieverbrauch an einem Standort, was zu **erheblichen Kosteneinsparungen führt**



Gemeinnützige Organisationen

Branche
Gemeinnützige
Organisationen

Lösungen
IT Operations
Security
Unternehmerische Erkenntnisse



Datengestützte Ergebnisse

Mehr als 2 Mio. Kinder pro Jahr werden unterstützt

< 5 Min. für die Überprüfung von Sponsoren mit Splunk anstelle von einer Woche

~120 Splunk-Dashboards liefern Business-Teams die Daten, die sie für intelligente Entscheidungen benötigen

Compassion International

nutzt Daten zum Schutz und zur Betreuung von Kindern in Armut

Zentrale Herausforderungen

Compassion International kümmert sich um den Schutz von fast zwei Millionen Kindern auf der ganzen Welt. Die Organisation musste für eine hohe Systemverfügbarkeit und die Sicherheit von Finanzdaten sorgen und Sponsoren schneller und effektiver überprüfen.

Wichtige Ergebnisse

Mit der Splunk-Plattform verwandelt Compassion International Rohdaten in umsetzbare Erkenntnisse, um Spender zu schützen, Ausbeutung einzudämmen, die Wirkung der finanziellen Förderung zu messen und mehr Kinder aus Armut und Menschenhandel zu befreien.

Um den Schutz von Kindern und Sponsoren zu gewährleisten, muss das Team von Compassion International die unterschiedlichsten Daten verwalten und schützen – von Finanzdaten über die Daten von Sponsoren und Kindern bis hin zu Informationen zu Systemzustand und Netzwerkverbindungen auf der ganzen Welt. Compassion nutzte Splunk zunächst für herkömmliche IT- und Sicherheitsanwendungsfälle. Doch bald machten sich weitere Teams, von Führungskräften und der Abteilung für Risikomanagement bis hin zu Marketing und Fundraising, die leistungsstarken Funktionen der Plattform zunutze. Die Initiative PATCH (Protect All the Children) setzt beispielsweise die Machine Learning- und Datenverarbeitungsfunktionen von Splunk ein, um Sponsoren zu überprüfen und automatisch jeden zu kennzeichnen, der mit einer Datenbank für Sexualstraftäter in Verbindung gebracht wird.



In diesen schweren Zeiten müssen wir noch mehr Kinder erreichen und unterstützen als zuvor. Die Splunk-Plattform ermöglicht uns Entscheidungen auf der Grundlage von Daten zu treffen. Sie wird in Zukunft eine noch wichtigere Rolle beim Schutz und bei der Betreuung der bedürftigsten Kinder spielen.“

— John Edom, Principal of Monitoring and Automation bei Compassion International

Global Emancipation Network bekämpft Menschenhandel mit Daten

Zentrale Herausforderungen

Geschätzt 45 Millionen Menschen pro Jahr sind von Menschenhandel betroffen, doch die Daten, die für das Aufspüren der Täter dieses Verbrechens benötigt werden, sind schlecht definiert, in isolierten Datensilos gespeichert und schwer zugänglich.

Wichtige Ergebnisse

Splunk bildet das Fundament, auf dem Global Emancipation Network (GEN) seine Mission aufbaut. Über das Splunk for Good-Programm werden Softwarelizenzen, Schulungen, Support und Ausbildungsmöglichkeiten bereitgestellt.

GEN und Splunk haben gemeinsam eine Analyseplattform namens Minerva entwickelt, die unstrukturierte, in Silos gespeicherte Daten analysiert, um aufzudecken, wer hinter den weltweiten Menschenhandelsoperationen steckt. Mithilfe von Splunk lassen sich Daten aus Hunderten von Quellen durchkämmen, um Verbindungen zwischen Benutzernamen, E-Mail-Adressen, Telefonnummern, Text und Bildern herzustellen, die manuell nicht oder nur schwer herstellbar wären. Über GEN und Splunk for Good steht Minerva nationalen und internationalen Strafverfolgungsbehörden, Nichtregierungsorganisationen, wissenschaftlichen Institutionen und dem privaten Sektor für das Aufspüren und Stoppen von Menschenhandel kostenlos zur Verfügung.



Ohne Splunk wäre GEN nicht da, wo es heute ist. Das Support-Team ist einfach fantastisch, das Produkt ist wundervoll. Splunk war in gleichem Maße für den Erfolg von GEN verantwortlich wie wir selbst.“

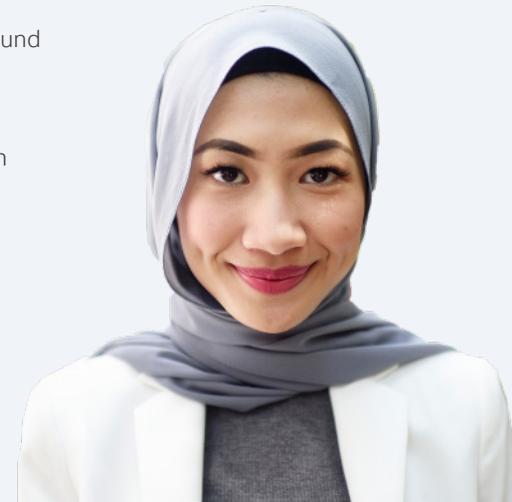
— Sherrie Caltagirone, Gründerin und Executive Director von Global Emancipation Network

Datengestützte Ergebnisse

Tage statt Jahre für die Verarbeitung und Analyse enormer Datenmengen

Millionen von Datenpunkten von mehr als 22.000 Messageunternehmen analysiert

Mehr als 55 Tsd. Schulen in Nordirland, England und Wales zur Beschleunigung der Untersuchung von Kindesmissbrauch untersucht



Branche

Gemeinnützige Organisationen

Lösungen

Business- und IT Service-Monitoring
Compliance
Industrie 4.0 und IoT

Rise Against Hunger – Daten zügeln und sich mit Splunk auf die Mission fokussieren

Zentrale Herausforderungen

Rise Against Hunger hat sich das Ziel gesteckt, den Hunger auf der Welt bis 2030 auszuradieren. Dazu war es erforderlich, Daten besser zu verwalten und zu schützen und Essenspakete und Mahlzeiten auf globaler Ebene nachzuverfolgen.

Wichtige Ergebnisse

Dank Splunk for Good profitiert die gemeinnützige Organisation nun von der Transparenz über unterschiedliche Systeme und die gesamte Lieferkette hinweg und gewinnt Erkenntnisse über die weltweite Lieferung und Verteilung von Mahlzeiten.

Rise Against Hunger ist eine internationale humanitäre Organisation, die jährlich fast 800.000 Menschen in 31 Ländern mit Nahrungsmitteln versorgt. Die Organisation war mit Herausforderungen konfrontiert, die ihre lebenswichtige Mission in Gefahr brachten, und setzt die Splunk-Plattform für einen besseren Datenschutz, mehr Sicherheit und die Einhaltung internationaler Datenstandards ein. Vor allem gewinnt Rise Against Hunger Erkenntnisse aus den Daten, aufgrund derer die Organisation die Hilfeempfänger mit dem größten und unmittelbarsten Bedarf ermitteln kann.

INHALT



Splunk hilft uns dabei, einen kompletten ‚Fahrplan‘ zu erstellen, mit dem wir Transparenz in Bezug auf die gesamte Lieferkette erhalten. Die Technologie und unsere Partnerschaft wird dazu beitragen, die Organisation voranzubringen.“

— Sheryl Gustafson, Director of Technology Solutions and Services



Datengestützte Ergebnisse

Rationalisierung und Priorisierung von über **180 unterschiedlichen Systemen** in der IT-Umgebung

Transparenz bei der weltweiten Lieferung und Verteilung von Mahlzeiten

Klares, effizientes Verfahren zur **Verbesserung des Datenschutzes** und für den Compliance-Nachweis

Branche
Gemeinnützige
Organisationen

Lösungen
IT Operations
Unternehmerische Erkenntnisse



Datengestützte Ergebnisse

~60 NGOs erhalten Erkenntnisse in Bezug auf Netzwerke und die von NetHope verwendeten Geräte, sodass das Team die Ausrüstung am Einsatzort besser verwalten und warten kann.

300 verteilte Netzwerke werden in einem integrierten NOC verwaltet, was eine datengestützte Planung für die Skalierung von Netzwerken ermöglicht.

60 % aller internationalen, nicht-staatlichen Hilfsprogramme werden jedes Jahr von NetHope erfolgreich abgewickelt.

NetHope nutzt Daten zur Bewältigung globaler Katastrophen und Flüchtlingskrisen

Zentrale Herausforderungen

NetHope wollte die Krisenreaktion bei globalen Katastrophen und Flüchtlingskrisen verbessern und suchte nach einer Möglichkeit, Erkenntnisse aus der Krisenkommunikation und Direkthilfemaßnahmen zu sammeln.

Wichtige Ergebnisse

Dank Splunk for Good erstellte NetHope ein erstes integriertes NOC und war damit in der Lage, Daten besser zu verwalten, Analysen zum Netzwerkzustand durchzuführen, die Nutzung zu verfolgen und in Krisenzeiten für noch mehr Menschen da zu sein.

NetHope ist ein weltweites Konsortium von fast 60 führenden Nichtregierungsorganisationen (NGOs) und koordiniert die Krisenreaktion für hilfsbedürftige Länder mit den Hilfsorganisationen, die Informationen benötigen, um handeln zu können. Splunk for Good stellt NetHope die Technologie zur Verfügung, mit der es gelingt, unterschiedliche Daten besser zu verwalten und zu interpretieren, und hat der gemeinnützigen Organisation beim Aufbau eines integrierten NOC für ihre fast 300 verteilten Netzwerke geholfen. Die Mitarbeiter können diese Netzwerke nun besser verwalten und den Partnern Informationen zu deren Nutzung liefern. Durch die neue Möglichkeit zur Analyse des Netzwerkzustands kann NetHope proaktiv Netzwerke planen und nicht nur die Wartung übernehmen.

[Video ansehen](#)



Durch die Möglichkeit, die Wirkung eines bestimmten Einsatzes an einem bestimmten Ort im Rahmen unserer Konnektivitäts- und Netzwerkinitiativen gezielt zu kommunizieren, profitieren wir von einem Vorteil, über den meines Wissens niemand sonst in der Branche verfügt.“

— John Crowley, Director of Information Management and Crisis Informatics bei NetHope

The background features a light blue topographic map with contour lines. Overlaid on the map are three distinct paths: a solid magenta line starting from the bottom left and curving upwards; a solid orange line starting from the middle left and curving upwards; and a dashed orange line starting from the middle right and curving upwards. A faint dotted grey line also traces a path across the map.

Öffentlicher Sektor

Branche
Öffentlicher Sektor

Lösungen
IT Operations
Security
Unternehmerische Erkenntnisse

Das **U.S. Census Bureau** setzt auf Digitalisierung für die größte Volkszählung in der Geschichte der USA

Zentrale Herausforderungen

Für die Verteilung von Finanzmitteln in Höhe von 675 Milliarden US-Dollar muss das U.S. Census Bureau im Rahmen des United States Census 2020, der ersten digitalen Volkszählung des Landes, eine vollständige und genaue Zählung aller in den USA lebenden Personen durchführen.

Wichtige Ergebnisse

Das Census Bureau nutzt Splunk, um bei der größten Volkszählung in der Geschichte der USA Daten zu schützen, Systeme zu konsolidieren, den manuellen Erfassungsaufwand an der Haustür zu reduzieren und Daten als Grundlage für jede Handlung zu nutzen.

Seit 1790 übernimmt das U.S. Census Bureau (USCB) alle zehn Jahre die Mammutaufgabe, eine genaue Zählung sämtlicher in den USA und ihrem Hoheitsgebiet lebenden Personen durchzuführen. 2020 wird die Volkszählung zum ersten Mal digital durchgeführt und die Amerikaner bekommen die Möglichkeit, nicht nur telefonisch oder per Post, sondern auch online zu antworten.

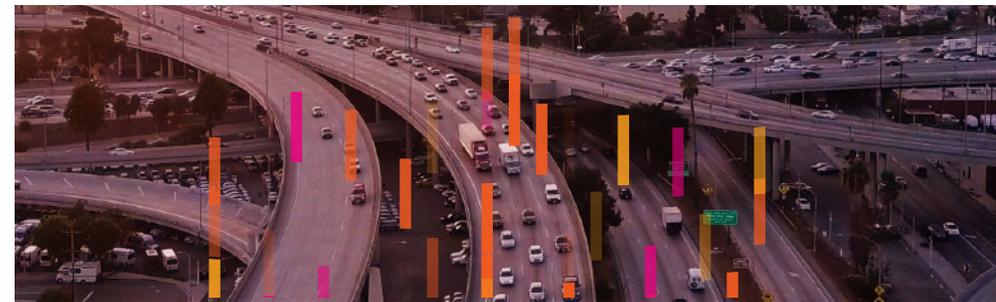
Die Datenvisualisierungen von Splunk sind zu einem wichtigen Bestandteil der täglichen Workflows des Census Bureau geworden und liefern Echtzeiterkenntnisse, aufgrund derer Führungskräfte und Teams für Sicherheit, IT und Anwendungen Fragestellungen angehen, Entscheidungen treffen und Maßnahmen ergreifen können. Mit Splunk als Kern seines SOC und NOC konnte das Census Bureau die Betriebszeit steigern und ist in der Lage, Schwachstellen proaktiv zu identifizieren und Probleme schneller zu beheben. Dies macht das gesamte Nutzungserlebnis sicherer und zuverlässiger.

INHALT



Die Dashboards und Berichte von Splunk bilden den Kern [unseres funktionsübergreifenden Hubs]. Unsere Führungskräfte nutzen sie als Informationsquelle und Grundlage für bessere Entscheidungen.“

— Atri Kalluri, Senior Advocate, Decennial Census Response Security and Data Integrity beim U.S. Census Bureau



Datengestützte Ergebnisse

Vereinfachte erfolgreiche Volkszählung, die 2020 **zum ersten Mal digital durchgeführt wurde**

Führungskräfte können dank standardisierten Dashboards und Echtzeiteinblicken **bessere und fundiertere Entscheidungen treffen**

Gewährleistung der Integrität, Verfügbarkeit und Sicherheits-Compliance der komplexen Infrastruktur der Behörde mit ihren **52 Systemen und 35 Prozessen**



Derbyshire Fire and Rescue

spart Kosten und rettet Leben durch optimale Datennutzung

Zentrale Herausforderungen

Ohne eine zentrale Lösung für das Log-Monitoring klagte das kleine IT-Team des Feuerwehr- und Rettungsdienstes über mangelnde Transparenz bei der Systemverwaltung, bei Software-Updates und bei Sicherheitsbedrohungen.

Wichtige Ergebnisse

Mit Splunk gelang es dem IT-Team dank besserer Erkenntnisse zum Sicherheitsniveau, rascherer Problembehebung und optimierter Zusammenarbeit die Sicherheitsreaktion zu verbessern und die Cyberrisiken einzudämmen.

Derbyshire Fire and Rescue Service (DFRS) hat die Aufgabe, mehr als eine Million Menschen zu schützen. Doch um für die Sicherheit der Bürger sorgen zu können, musste der Feuerwehr- und Rettungsdienst zunächst seine 31 Feuerwehrstationen und seine beiden Rechenzentren schützen, die dem Risiko von Cyberangriffen ausgesetzt waren. Mit Splunk-Dashboards kann sich das vielbeschäftigte DFRS-Team problemlos einen visuellen Überblick über den Systemzustand verschaffen. Zuvor blieben Security-Incidents manchmal unentdeckt und die zuständigen Mitarbeiter mussten sich mühsam manuell durch Logdateien arbeiten, um nach Anomalien zu suchen, wenn ihnen etwas verdächtig vorkam. Mit Splunk konnte DFRS die Mitarbeiterproduktivität steigern und gleichzeitig katastrophale Sicherheitsverstöße verhindern, da Angriffe bereits abgewehrt werden können, bevor Schaden entsteht.

Datengestützte Ergebnisse

Angriffe werden blockiert, bevor Schaden entstanden ist

Probleme der Systemwartung schnell entdeckt und repariert

Kosteneinsparung durch Nachverfolgung und Behebung von missbräuchlicher Druckernutzung



Dank Splunk haben wir wichtige Informationen sofort im Blick. Das hat uns geholfen, bessere, fundiertere Entscheidungen zu treffen.“

— Pete Garyga, ICT Security and Project Team Manager bei Derbyshire Fire and Rescue Service

Branche
Öffentlicher
Sektor

Lösungen
Anwendungsbereitstellung
Security
Compliance



Datengestützte Ergebnisse

20% Verbesserung bei der Behebung von Problemen, bevor sie sich auf die Benutzer auswirken

35% kürzere MTTR und damit bessere SLA-Erfüllung

50% weniger manueller Compliance-Aufwand und daher effizientere und erfolgreichere Audits

Michigan Department of Health and Human Services bietet erstklassige Bürgerservices

Zentrale Herausforderungen

Das Michigan Department of Health and Human Services (MDHHS) brauchte Transparenz in seinem integrierten Portal BRIDGES, um den 1,7 Millionen Bürgern des Bundesstaates seine Dienste effektiv zur Verfügung stellen zu können.

Wichtige Ergebnisse

Mit Splunk konnte das MDHHS mehr Transparenz in BRIDGES schaffen, das 52 Behörden verbindet und über 12.000 Transaktionen pro Minute verarbeitet, um damit letztlich den Service für die Bürger zu verbessern.

Das MDHHS ist für Dienstleistungen in den Bereichen Gesundheitsversorgung, Nahrungsmittelhilfe, Förderung und Betreuung von Kindern, finanzielle Beihilfen und staatliche Nothilfe zuständig. Nach der Einführung der Data-to-Everything Plattform steigerte das MDHHS seine Effizienz in allen Bereichen dank Transparenz bis ins kleinste Detail innerhalb der Infrastruktur seiner BRIDGES-Anwendung. Durch die Möglichkeit, die Nutzung zu beziffern und die Leistung zu analysieren, in Kombination mit Prognosefunktionen und den Möglichkeiten künstlicher Intelligenz, gewinnt die Behörde nun Erkenntnisse zu Problemen, lange bevor die Nutzer davon betroffen sind und kann so das Dienstangebot für die Bürger verbessern.



Unser manueller Arbeitsaufwand zur Erfüllung und Erfassung der PCI- und Audit-Compliance konnte dank Splunk um 50 % gesenkt werden. Dies hilft uns, bei Compliance-Audits erfolgreich abzuschneiden.“

— Sanjay Srivastava, Division Director, Eligibility Area DTMB, State of Michigan

Branche
Öffentlicher
Sektor

Lösungen
Anwendungs-Monitoring
Infrastruktur-Monitoring
Industrie 4.0 und IoT
IT Operations
Predictive Analytics
Security-Monitoring

National Ignition Facility

setzt das Potenzial sauberer Energie frei und schützt den Kernwaffenbestand der USA

Zentrale Herausforderungen

Die National Ignition Facility (NIF) suchte nach einer sicheren Möglichkeit, Daten zu schützen und Anlagenausfälle zu verhindern, um die Verfügbarkeit der Anlage für wissenschaftliche Experimente sicherzustellen.

Wichtige Ergebnisse

Nachdem Netzwerk-, Authentifizierungs- und Hostdaten in Splunk integriert wurden, um Herausforderungen im Bereich Security zu meistern, kombinierten die Mitarbeiter diese Daten mit verschiedenen anderen Quellen, um Echtzeitsichtbarkeit über die gesamte Einrichtung hinweg zu erhalten.

Die NIF hat ihren Sitz im Lawrence Livermore National Laboratory in Kalifornien und verfügt über den weltweit größten Laser. Damit die NIF ihre Hauptziele erfüllen kann, zu denen unter anderem die Verwaltung des Kernwaffenbestands und wissenschaftliche Forschungen zählen, benötigen die Wissenschaftler und Ingenieure eine sichere und zuverlässige IT-Infrastruktur. Splunk Enterprise und Splunk IT Service Intelligence bilden jetzt das Kernstück des NIF-Steuersystems, mit dem mehr als 66.000 Steuerpunkte für den Betrieb der riesigen NIF-Laseranlage verwaltet werden. Die Ingenieure des Labors können bei Ereignissen jetzt auf eine fundierte Datenbasis von Anwendungsdaten bis hin zu Sensordaten wie Laserspannung, Temperatur und Druck zurückgreifen und entsprechend handeln.

[Video ansehen](#)

INHALT



Daten sind absolut entscheidend für unsere Lernkurve und die Fortschritte, die wir bei den komplexen Fragestellungen machen, die wir bei NIF untersuchen.“

— Bruno Van Wonterghem, Operations Manager bei der National Ignition Facility



Datengestützte Ergebnisse

Mehr als 66 Tsd. IoT-Geräte zusätzlich zur IT-Infrastruktur werden von Splunk überwacht

Verdopplung der Laserschussexperimente auf 400 pro Jahr ohne Einschränkung der Uptime oder Datenintegrität

192 Laserstrahlen werden unter anderem dank Echtzeiterkenntnissen erfolgreich auf ein winziges Ziel fokussiert, das kleiner ist als eine menschliche Haarsträhne



Datengestützte Ergebnisse

Tausende von Sportlern, Mitarbeitern und Zuschauern der Commonwealth Games werden vor Cyberangriffen und Unterbrechungen geschützt

4 unterschiedliche Umgebungen und Systeme erhalten Echtzeittransparenz und operative Erkenntnisse

Verbesserung der Erkennung, Nachverfolgung und Abwehr von Bedrohungen während einer internationalen Sportveranstaltung mit erhöhtem Bedrohungsprofil

City of Gold Coast profitiert von Echtzeitsichtbarkeit bei den Commonwealth Games

Zentrale Herausforderungen

Die Ausrichtung der Commonwealth Games 2018 war ein wichtiger Impuls für die Stadt, ihre Sicherheitsprozesse und die Sichtbarkeit innerhalb der Organisation zu verbessern.

Wichtige Ergebnisse

Dank der Splunk-Plattform erlangte die City of Gold Coast (CoGC) Echtzeitsichtbarkeit in zahlreichen Umgebungen und konnte die Risiken in einer Umgebung mit erhöhter Bedrohungslage erheblich eindämmen.

Mit Splunk erreichte CoGC ein optimales Sicherheitsergebnis für die Commonwealth Games, und zwar ohne Betriebsbeeinträchtigungen. Splunk stellte für CoGC eine vollständige Plattform für vier unterschiedliche Umgebungen bereit, von den Industrieanlagen von Gold Coast Water bis hin zu herkömmlichen IT-Kernsystemen. Damit konnten unterschiedliche Organisationsbereiche mit ganz verschiedenen Anforderungen effektiv überwacht werden. Während der Spiele erreichte CoGC dank der Flexibilität von Splunk Cloud und Splunk Enterprise Security Echtzeittransparenz in der operativen Sicherheit und erweiterte den Beitrag seines Security-Teams auf den Austausch von Bedrohungsinformationen mit Bundesbehörden, Sponsoren und Partnern.



Mit Splunk konnten wir die Reife unseres Security-Service enorm verbessern. Da der Service jetzt stabil läuft und die Betriebsabläufe etabliert sind, können wir uns neuen Anwendungsfällen und Datenquellen in anderen Bereichen der Organisation zuwenden.“

— Matthew Walker, Information Technology Security Advisor, Gold Coast, Australien

Einzelhandel

The image features a topographic map background with light blue contour lines. A prominent wavy line starts as a solid red line on the left, transitions to a solid orange line in the middle, and ends as a dashed orange line on the right. A faint dashed grey line also follows a similar path across the map.

Branche
Einzelhandel

Lösungen
Unternehmerische Erkenntnisse
IT Operations
Security



Datengestützte Ergebnisse

Die Nummer 1 unter den Pizzeriaunternehmen mit dem höchsten Einzelhandelsumsatz weltweit

16 digitale Bestellkanäle, über die 65 % des Umsatzes in den USA generiert werden – alle mit Splunk überwacht, geschützt und optimiert

3 Mio. Pizzen werden täglich an 1 Million Kunden auf der ganzen Welt verkauft



Fast alle Teams bei Domino's nutzen Splunk auf die eine oder andere Art. Sie wollen nicht wissen, ob eine einzelne Komponente fehlerfrei ist, sondern sich ein Bild vom großen Ganzen machen, einschließlich Vertriebsdaten, Umsatz und mehr. Auf diese Weise können sie sehen, welche Auswirkungen ihre Entscheidungen auf das gesamte Unternehmen haben.“

— Mike Cox, Operational Intelligence Architect bei Domino's

Domino's verrät: Daten sind ihr Geheimrezept

Zentrale Herausforderungen

Domino's wollte neuen Bedürfnissen seiner Kunden nach einem schnellen, qualitativ hochwertigen und benutzerfreundlichen Service gerecht werden und eine zuverlässige, moderne Digitalerfahrung bieten.

Wichtige Ergebnisse

Domino's nutzt Splunk, um alle Transaktionen zu überwachen, Daten zu schützen, die Systemverfügbarkeit proaktiv sicherzustellen und fundierte Investitions-, Budget- und Effizienz-Entscheidungen zu treffen und bietet seinen Kunden eine maßgeschneiderte Omnichannel-Erfahrung.

Domino's ist die weltweit umsatzstärkste Pizzakette, und zwar vor allem aufgrund eines datenzentrierten Ansatzes in allen Bereichen, von Hintergrundprozessen im IT- und Securitybereich bis hin zu alltäglichen Kundeninteraktionen wie Bestellvorgängen und Lieferungen. Mit Splunk steht der Pizzakette eine zuverlässige Technologie zur Verfügung, die Erkenntnisse zu allen Echtzeittransaktionen auf der Website, Anwendungen und 16.300 Niederlassungen auf der ganzen Welt bietet. Mithilfe der Echtzeiterkenntnisse von Splunk gelingt es Domino's, seine Systeme, Kundendaten und den Ruf der Marke zu schützen. Gleichzeitig wurden wiederkehrende Workflows automatisiert, sodass sich die Sicherheitsanalysten nun nicht mehr mit monotonen Routineaufgaben beschäftigen müssen und mehr Zeit für analytische Tätigkeiten haben. Vor der Einführung neuer Features oder Services lässt Domino's die Funktionalität von Splunk optimieren und sicherstellen, dass die Technologie für den Kundeneinsatz bereit ist. Nicht zuletzt deshalb bleibt das Unternehmen innovativ und marktführend.

[Video ansehen](#)

REI erhält Edge-Schutz mit Splunk Cloud und AWS

Zentrale Herausforderungen

Bei der Migration seiner Anwendungen zu Amazon Web Services (AWS) benötigte der Outdoor-Fachhändler eine Plattform, die Edge-Schutz für die Amazon Virtual Private Clouds (VPCs) anbieten würde.

Wichtige Ergebnisse

Dank Splunk Cloud und Amazon GuardDuty können die Teams von REI jetzt analysegestützte Entscheidungen treffen. Sie haben genügend Informationen, um das Risiko zu minimieren und gleichzeitig die Verfügbarkeit für die Kunden sicherzustellen.

Als Unternehmen, das für seinen Kundenservice und die Markenreputation bekannt ist, wollte REI sein Sicherheitsniveau erhöhen, damit nach der Migration seiner Anwendungen zu Amazon Web Services (AWS) auch der Edge-Schutz seiner Amazon Virtual Private Clouds sichergestellt ist. Bisher fehlte es im Unternehmen an einem Untersuchungs-Workflow, der AWS miteinbezog. Die Mitarbeiter mussten die relevanten Daten also zeitaufwändig manuell extrahieren und analysieren. Da REI alle sicherheitsrelevanten Daten in der Splunk Cloud zusammenführt, liefert die Technologieorganisation Analyseerkenntnisse für immer mehr Fragen und Entscheidungen, was im gesamten Unternehmen zu besseren Ergebnissen führt.



Wir möchten die Daten von REI schützen. Dafür setzen wir unsere Ressourcen ein und investieren Zeit. Die Anschaffung von Splunk Cloud war eine wirklich gute Investition – nicht nur aufgrund der gebotenen Funktionen, sondern auch wegen der Zeiteinsparungen.“

— David Bell, Manager, Infrastructure and Cloud Services bei REI



Datengestützte Ergebnisse

**End-to-End-Sicherheits-
transparenz** während der
AWS-Cloud-Migration

Sicherheitsorientierter
Ansatz durch
die **DevSecOps-
Transformation**

Echtzeiterkenntnisse
zu potenziellen
Bedrohungen

Branche
Einzelhandel/
Fertigung

Lösungen
Security
Betrugsbekämpfung

ASICS automatisiert Management und Behebung von Incidents mit Echtzeit- Log-Analysen

Zentrale Herausforderungen

ASICS wollte Cyberbedrohungen bekämpfen und Incidents sofort lösen und benötigte daher eine zentrale Plattform zur Verwaltung, Korrelierung und Analyse von Logs aus mehreren Systemen.

Wichtige Ergebnisse

ASICS verwendet die Splunk-Plattform, um Log-Daten aus allen Systemen in einer einzigen Plattform zu konsolidieren und zu analysieren und profitiert von Erkenntnissen und Echtzeittransparenz aller Abläufe.

Dank Automatisierung kann ASICS sein Rechenzentrum mit minimalen manuellen Eingriffen rund um die Uhr überwachen, Sicherheitsbedrohungen und Incidents im Betriebsablauf erkennen und schnell Maßnahmen ergreifen. Durch automatisiertes Log-Management spart ASICS wertvolle Arbeitsstunden ein und ermöglicht seinem Team gleichzeitig, sich auf wertschöpfende Aktivitäten zu konzentrieren. ASICS verfolgt die Mission, mit intelligenter Sporttechnologie einen gesunden Lebensstil zu fördern und nutzt dazu mit Begeisterung die Intelligenz von Splunks Data-to-Everything Plattform.

INHALT

Datengestützte Ergebnisse

Echtzeitsichtbarkeit von Incidents und Bedrohungen durch automatisierte Log-Analysen

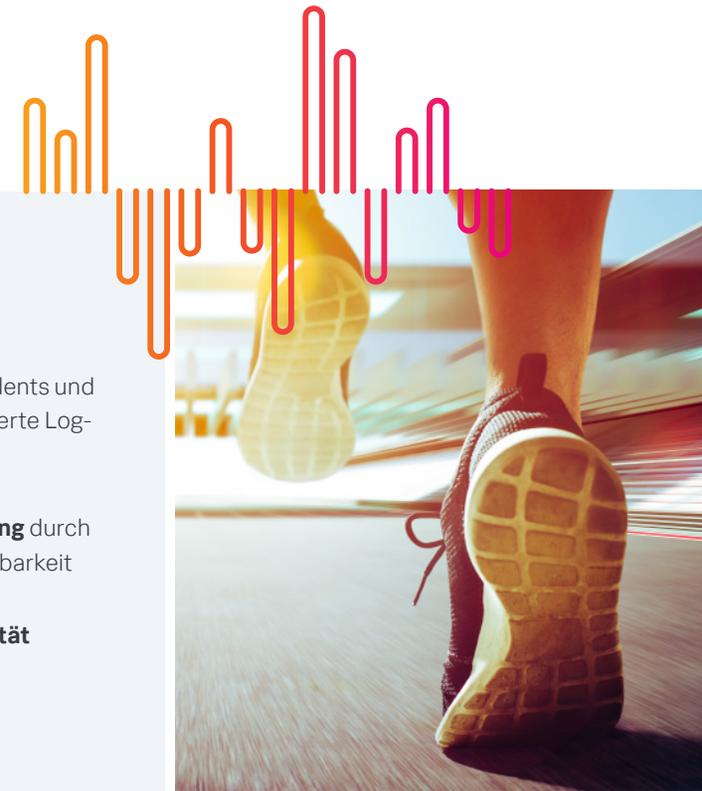
Stärkere soziale Verantwortung durch optimierte Sicherheit und Sichtbarkeit

Mehr Effizienz und Produktivität aufgrund von optimierten Geschäftsabläufen



Als Allround-Analysetool unterstützt Splunk Enterprise effizient unsere Geschäftsabläufe und bietet uns große Vorteile. Wir glauben, dass Splunk eine Art ‚Energizer‘ für die Sportbranche sein könnte.“

— Shigekazu Tanimoto, Global Security Lead bei ASICS Corporation 51



Technologie

The image features a background of a topographic map with light blue contour lines. A thick, wavy line with a color gradient from red to orange flows across the lower half of the frame. A dashed orange line follows a path across the map, starting from the right side and moving towards the left, crossing the wavy line.

Intel erhöht Sicherheitsniveau mit innovativer Data Intelligence

Zentrale Herausforderungen

Intel war auf der Suche nach einem datenzentrierten Geschäftsmodell, das den Wert der Daten erhöht und gleichzeitig deren Verwundbarkeit senkt.

Wichtige Ergebnisse

Mit Splunk und Apache Kafka als Grundlage bietet die Cyber Intelligence Plattform (CIP) lückenlose Transparenz für Intels InfoSec-Organisation, welche das Management der Informationssicherheit verändert hat.

Intels Abteilung für Informationssicherheit musste eine umfassende „Defense-in-Depth“-Strategie entwickeln und verfolgen und automatisierte im Zuge dessen Präventions- und Erkennungstools auf vielen Ebenen. Dadurch konnten 99 % der Bedrohungen in Intels gesamter Umgebung abgewickelt werden. Doch das InfoSec-Team musste trotzdem noch hochkomplexe Bedrohungen erkennen und bezeichnete dieses Unterfangen als „die Jagd nach dem einen Prozent“. Dies war ausschlaggebend für die Entwicklung der Cyber Intelligence-Plattform (CIP), die auf Spitzentechnologien wie Splunk und Apache Kafka basiert. Mit der CIP verfügt das InfoSec-Team jetzt über umfassende Transparenz, aussagekräftige Informationen und eine gemeinsame Arbeitsoberfläche, womit die Effektivität gesteigert und die MTTR (Mean-Time-To-Repair) verkürzt werden konnte.

[Video ansehen](#)



Daten sind alles, Daten sind Trumpf ... Sie transformieren traditionelle Branchen und solche, die in der Cloud zu Hause sind. Die Fähigkeit, Erkenntnisse aus Daten zu gewinnen, unterscheidet erfolgreiche Unternehmen von Unternehmen, die den Anschluss verlieren.“

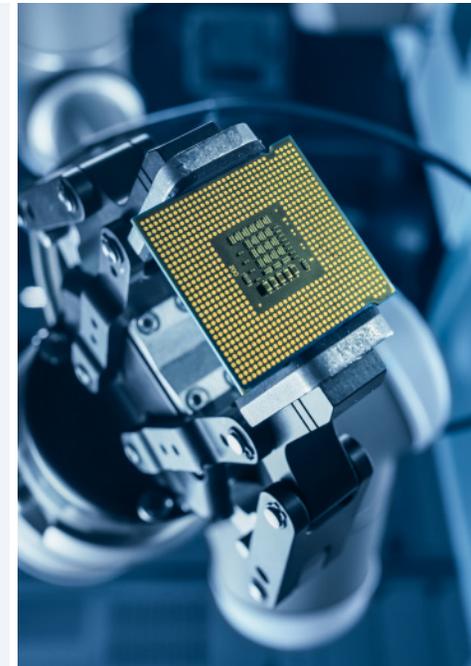
— Brent Conran, Chief Information Security Officer bei Intel

Datengestützte Ergebnisse

Beschleunigung der Datenanalyse und Erkennung hochkomplexer Bedrohungen innerhalb von **Minuten bzw. Stunden statt Tagen bzw. Wochen**

Gemeinsamer, einheitlicher Ansatz für die Steuerung der Cybersicherheit

Stream-Processing- und Machine Learning-Tools sind auch in zusätzlichen Bereichen wie Sicherheitsprozessen und dem Systemzustand wertschöpfend



Branche
Technologie

Lösungen
Log-Management
Security
Betrugsbekämpfung

Lenovo China optimiert Security Operations und gewinnt umsetzbare Erkenntnisse

Zentrale Herausforderungen

Lenovo generiert jeden Tag ein Datenvolumen von zwei Terabyte und suchte nach einer zuverlässigen Sicherheitslösung, um Bedrohungen schnell zu erkennen und bedarfsgerecht zu reagieren.

Wichtige Ergebnisse

Dank der Splunk-Plattform kann Lenovo seine Daten jetzt optimal nutzen und verbessert die Schnelligkeit, Zuverlässigkeit und Effizienz seiner Sicherheitsprozesse.

Der global agierende Technologiegigant Lenovo beschäftigt mehr als 57.000 Mitarbeiter in 180 Ländern und muss seinen Betrieb ständig entsprechend des Unternehmenswachstums skalieren. Vor der Einführung von Splunk mussten die Sicherheitsingenieure Informationen aus unterschiedlichen Systemprotokollen abrufen und korrelieren und anschließend die Ergebnisse zusammenführen und in einem visuellen Format präsentieren. Dieser arbeitsintensive Prozess kostete die Ingenieure viel Zeit und sorgte für eine langsame und komplizierte Fehlerbehebung. Dank Splunk konnte Lenovo seine Workflows optimieren und die Produktivität steigern. Durch die Integration unterschiedlicher Datenquellen wurden präzise Datenabrufe in Echtzeit sowie zentrales Monitoring und Analysen möglich. Darüber hinaus hat Splunk einen Beitrag zur Lösung von Bereitstellungsproblemen geleistet und Lenovos Migration in die Cloud vorangetrieben.



Datengestützte Ergebnisse

Maximierte Unternehmensagilität
durch Log-Management in Echtzeit

Beschleunigte Incident Response mit
verbessertem Security-Monitoring

Höhere Prozesseffizienz



Dank der intelligenten und zuverlässigen Performance der Splunk-Lösung können wir in Echtzeit operative Erkenntnisse gewinnen, indem wir verwertbare Informationen aus Rohdaten extrahieren, eingehend analysieren und für ein effektives Security-Monitoring verwenden. Wir sind froh, dass wir uns für Splunk entschieden haben und freuen uns wirklich darauf, die Partnerschaft mit Splunk in Zukunft noch zu vertiefen.“

— Yu Sheng Li, IT Security Director bei Lenovo China

Branche
Technologie

Lösungen
Security
DevOps
IT Operations



Datengestützte Ergebnisse

Mehr Sicherheit für Systeme und Kundendaten durch Echtzeit-Monitoring und -Troubleshooting

Bessere Kundenerfahrung durch schnellere Problembehebung und zuverlässige Produkt-Performance

Schnellere Markteinführung für neue Produkte und Funktionen

Arlo optimiert interne Prozesse zum Schutz von Kundendaten

Zentrale Herausforderungen

Mit den selbst entwickelten Tools von Arlo war weder funktionales Monitoring noch das Debuggen von Incidents in der Produktionsumgebung möglich, was negative Auswirkungen auf die Sicherheit und die Kundenerfahrung hatte.

Wichtige Ergebnisse

Dank schnellerer Fehlerbehebung, höherer Verfügbarkeit und optimierter Sicherheit konnte Arlo die Kundenzufriedenheit erhöhen und durch den Umstieg in die Cloud gleichzeitig die Kosten senken.

Um sicherzustellen, dass Arlos 13,3 Millionen IoT-Geräte bei den Kunden sicher und zuverlässig funktionieren, setzt das Unternehmen Splunk für das System-Monitoring und -Troubleshooting in Echtzeit ein. Damit ist es möglich, Bedrohungen proaktiv zu erkennen und einzudämmen, bevor es zu einem Sicherheitsverstoß kommt. Mit vorherigen Tools konnte die MTTI (Mean-Time-To-Investigate) eines einzigen Produktions-Incidents Tage betragen, was frustrierte Teammitglieder und kostspielige Produktivitätsverluste zur Folge hatte. Doch dank Splunk ist es Arlo gelungen, die MTTI von Tagen auf Stunden zu reduzieren – in vielen Fällen sogar auf Minuten. Mit optimierten internen Prozessen haben die DevOps- und QS-Teams von Arlo die Produktivität gesteigert und Innovationen beschleunigt.

[Video ansehen](#)



Splunk trägt entscheidend dazu bei, dass unsere Sicherheitsprozesse dauerhaft zuverlässig sind und unsere Kunden auf unsere Rund-um-die-Uhr-Services in der Cloud vertrauen.“

— Tejas Shah, SVP & Chief Information Officer bei Arlo

Branche
Technologie

Lösungen
IT Operations
Anwendungs-Monitoring
Infrastruktur-Monitoring
DevOps

Acquia revolutioniert die Customer Experience mit Problemlösungen in Echtzeit

Zentrale Herausforderungen

Im Zuge seiner Skalierung musste Acquia das Wachstum seiner Infrastruktur bewältigen, die Komplexität des Technologie-Stacks reduzieren und vielbeschäftigte Teams entlasten.

Wichtige Ergebnisse

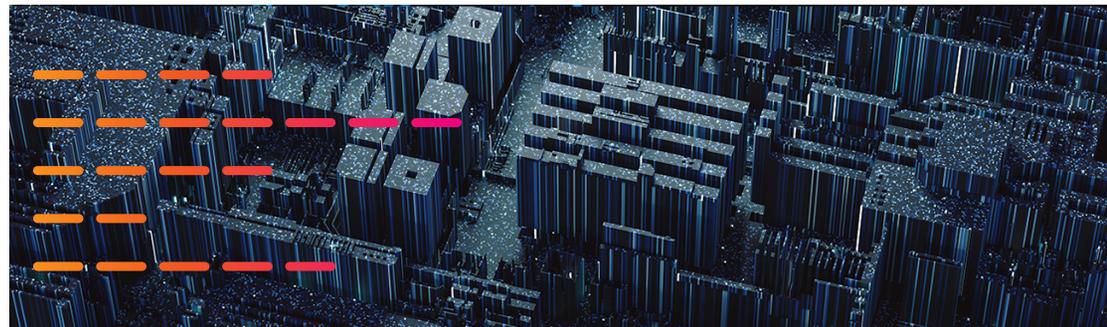
Mit Splunk hat Acquia seine Ziele sogar übertroffen. Die Support-Zeiten wurden verkürzt, Probleme werden schneller gelöst und das Leben ist für Kunden und das Acquia-Team leichter geworden.

Als der Kundenstamm des Unternehmens wuchs, brauchte Acquia einen besseren Einblick in die Instanzen der Kunden und schnelleren Zugriff auf zuverlässige Daten. Acquia entschied sich für Splunk, um eine konsolidierte Plattform für das Echtzeit-Monitoring seiner wachsenden AWS-Umgebung aufzubauen, einschließlich Infrastruktur, Services, Anwendungen, Microservices, Containern und AWS Lambda. Das Ergebnis waren unter anderem stark verkürzte Support-Zeiten, eine kürzere MTTR (Mean-Time-To-Resolution), weniger Unterbrechungen, glücklichere Kunden und eine geringere Arbeitslast für das technische Team von Acquia.



Komplexe Daten werden in Graphen und Diagrammen visuell aufbereitet, sodass die Benutzer sofort verstehen, worum es geht. Unser Team vertraut den Informationen, wir können uns bei unseren Gesprächen auf diese Daten beziehen und problemlos Screenshots mit Kunden austauschen, sodass alle denselben Informationsstand haben.“

— Aaron Pacheco, Product Manager, Product Delivery Infrastructure bei Acquia



Datengestützte Ergebnisse

26% geringerer
durchschnittlicher
Zeitaufwand pro Incident,
wodurch 140 Stunden pro
Monat eingespart werden

**Mehr als
600 Tsd. USD**
Einsparung an AWS-
Infrastrukturkosten
innerhalb weniger Wochen
nach der Bereitstellung

1 Mio. USD
jährlicher
Produktivitätszuwachs



Datengestützte Ergebnisse

Erhöhte Datentransparenz, verbesserte Zusammenarbeit und Prozessoptimierung für ein Team, das sich weltweit über drei Regionen verteilt

Reduzierung des Zeitaufwands für Fehleruntersuchungen **von Wochen auf Sekunden**, daher höhere Effizienz und Verfügbarkeit

Verwandlung von Daten in verlässliche Analysen durch **mehr Transparenz und bessere Vorhersagemechanismen**

Square Enix verkürzt Zeit für die Fehlerbehebung durch datengestützte Transparenz auf Sekunden

Zentrale Herausforderungen

Ohne eine datengestützte Analyseplattform ließ die operative Transparenz bei Square Enix zu wünschen übrig, was zeitintensive manuelle Prozessen nach sich zog.

Wichtige Ergebnisse

Seit Einführung der Splunk-Plattform hat Square Enix die Effizienz gesteigert und das Log-Management zentralisiert und konnte damit die Fehlerbehebungszeit von Wochen auf Sekunden reduzieren.

Im Online-Spielesektor ist es seit jeher nicht einfach, mit den steigenden Anforderungen der Benutzer Schritt zu halten. Bei Square Enix, Entwickler beliebter Kultspiele wie Final Fantasy, kam erschwerend hinzu, dass der Serverzustand manuell überwacht werden musste. Splunk spielte eine entscheidende Rolle bei Square Enix' Übergang von einer reaktiven Fehlerbehebung zum proaktiven Risikomanagement. Während zuvor nach plötzlich auftretenden Fehlern hastig Logs durchgegangen wurden, setzt das Team jetzt auf automatische Log-Analysen, um Anomalien zu entdecken, bevor sie sich zu Problemen entwickeln. Die schwerfällige manuelle Berichterstellung wurde durch einfache Dashboards und Visualisierungen ersetzt, durch die Daten für die Benutzer leichter zugänglich werden.



Splunk war entscheidend für die Optimierung unserer Geschäftsprozesse. Transparenzengpässe im Log-Management werden aufgelöst, sodass wir uns jetzt ein vollständiges Bild von unserem Technologie-Stack machen können und enorm von Echtzeitanalysen profitieren.“

— Junpei Kakefuda, Information System Department bei Square Enix

The background features a light blue topographic map with contour lines. Overlaid on the map are several decorative lines: a solid magenta line that starts from the bottom left and curves upwards; a dashed orange line that starts from the middle left and curves towards the right; and a dotted grey line that runs horizontally across the middle of the map.

Telekommunikations- und Versorgungs- unternehmen

TalkTalk nutzt Splunk zur frühen Problemerkennung und Verbesserung der Netzwerk-Performance

Zentrale Herausforderungen

Mit den bestehenden Systemen hatte TalkTalk Probleme, ausreichend Daten zu Netzwerk-Performance und Serviceausfällen zu erschließen. Dadurch waren auch die Möglichkeiten zur schnellen und effektiven Problemerkennung begrenzt.

Wichtige Ergebnisse

Dank eines vollständigeren Überblicks über Netzwerk- und Performance-Metriken konnte TalkTalk die Fälle von Minderleistung in mehr als 5.000 Vermittlungsstellen drastisch reduzieren und gleichzeitig den Markenruf stärken.

Als führender Anbieter von Festnetz-, Breitband-, TV- und Mobilfunkdiensten für Endkunden und Unternehmen in Großbritannien entschied sich TalkTalk ursprünglich für Splunk, um Daten als Grundlage für Fragen zu seinem bestehenden System zu nutzen, nachdem der Verdacht einer Minderleistung des DNS (Domain Name System) aufgekommen war. Da das Team keinen zeitnahen Zugang zu relevanten Informationen hatte, kam es bei TalkTalk früher zu kosten- und zeitintensiven Service-Ausfällen. Dank der Splunk-Plattform ist das Unternehmen nun in der Lage, einen Ausfall innerhalb von Sekunden oder gar Millisekunden anstelle von Minuten zu entdecken. TalkTalk kann jetzt genau erkennen, welche Kunden betroffen sind und profitiert von einer schnelleren Problemlösung, höherer Verfügbarkeit und zufriedeneren Kunden.

[Video ansehen](#)

INHALT



Es geht darum, fehlerhafte Prozesse zu erkennen und die Splunk-Plattform zu nutzen, um eine Liste betroffener Kunden auszugeben, damit wir die Probleme mit robotergestützter Prozessautomatisierung (RPA) beheben können. Splunk verschafft uns Zugang zu den Daten und hilft uns daher bei der taktischen Optimierung von Prozessen.“

— Paul Emmett, Head of Network Operations bei TalkTalk



Datengestützte Ergebnisse

Reduzierung der wöchentlichen Anzahl kritischer „Red Exchange“-Incidents von mehreren Tausend auf höchstens 10

Bessere Netzwerk-Performance, Zuverlässigkeit und Verfügbarkeit

Höhere Kundenzufriedenheit durch die Fähigkeit, Netzwerkausfälle nahezu unverzüglich zu erkennen und genau zu bestimmen, welche Kunden betroffen sind

Belong treibt die Digitalisierung voran

Zentrale Herausforderungen

Bei Belong liegt der Fokus auf einer nahtlosen Kundenerfahrung und das Unternehmen suchte nach einer Möglichkeit, die Kundenbindung zu stärken, Echtzeitdaten zu interpretieren und einen robusteren, proaktiveren Sicherheitsansatz zu finden.

Wichtige Ergebnisse

Belong konnte die Problembehebungszeit um die Hälfte verkürzen und damit Zeit und Geld sparen, gleichzeitig die Kundenerfahrung verbessern und einen proaktiven Ansatz für die Lösung von geschäftlichen Problemen umsetzen.

Das Unternehmen bietet für Millionen von Menschen in Australien Bereitband- und Mobilfunkdienste an und ist für eine gute Kundenbindung und Umsatzoptimierung auf eine nahtlose Kundenerfahrung angewiesen. Mit der Splunk-Plattform hat Belong die Produktentwicklung beschleunigt und vereinfacht und seine Mitarbeiter in die Lage versetzt, Probleme wesentlich rascher zu erkennen, zu überwachen und zu lösen. Dank der Dashboards und Datenvisualisierungen von Splunk kann das Team komplexe Log-Daten als Handlungsgrundlage nutzen und hat ein Performance-Analyse-Tool mit Ampelsystem entwickelt, um Kundeninteraktionen zu optimieren und die Erfahrung von Kunden und Mitarbeitern zu verbessern.



Splunk war und ist eine Triebfeder unserer Digitalisierungsinitiative. Wir konnten unseren Produktentwicklungsteams über Echtzeit-visualisierungen Zugriff auf die Daten unseres Unternehmens verschaffen. Letztendlich trägt dies zu einer kundenorientierten, experimentellen Unternehmenskultur bei, die ein integraler Stützpfeiler einer nachhaltigen Digitalisierung und Business Performance ist.“

— Natalie Field, Chief Digital Officer bei Belong

Datengestützte Ergebnisse

75 % weniger Fehler beim Kunden

Halbierung des Zeitaufwands für das Ermitteln und Beheben von Problemen

Millionen von Echtzeit-Datenpunkten in Splunk zur proaktiven Lösung von IT-, Business- und Sicherheitsproblemen im gesamten Unternehmen



Branche
Energie- und
Versorgungs-
unternehmen

Lösungen
IoT und Industrie 4.0
IT Operations

Puget Sound Energy

verbessert die Reaktionszeit
mit Echtzeitdaten und profitiert
von Einsparungen durch
Anlagenintelligenz

Zentrale Herausforderungen

Bei Puget Sound Energy (PSE) sorgten veraltete Software und ein Mangel an Echtzeitdaten für lange Reaktionszeiten bei Stromausfällen, von denen Kunden betroffen waren.

Wichtige Ergebnisse

Dank umsetzbarer Erkenntnisse von Splunk kann PSE jetzt besser priorisieren und bei Stromausfällen schneller reagieren. Mit den Erkenntnissen aus den Anlagen hat PSE darüber hinaus die Zusammenarbeit optimiert und die Wartungskosten gesenkt.

Wenn es zu Stromausfällen kommt, muss PSE sich schnell einen Überblick über die betroffenen Bereiche und Kunden verschaffen. Mit Splunk kann das Team proaktiv reagieren und über die Wiederherstellung der Stromversorgung auf dem Laufenden bleiben, was mit einer Reduzierung des Callcenter-Volumens und einer höheren Kundenzufriedenheit einhergeht. Splunk-Dashboards und Splunk Augmented Reality (AR) bieten nun konsistente Einblicke in zahlreiche Datenquellen. Dadurch ist das Team nun eher in der Lage, Probleme zu beheben und bei der Entsendung von Einsatzteams Prioritäten zu setzen.

Das Team musste außerdem sicherstellen, dass Mitarbeiter standortunabhängig zusammenarbeiten können. Mit Splunk kann das Team nun in Echtzeit auf die Daten der Einsatzzentrale zugreifen (einschließlich der 60 Ausrüstungsgegenstände im Raum), Probleme schneller beheben und die Wartungskosten gering halten.

[Video ansehen](#)

INHALT



Splunk for Industrial IoT ist wichtig für uns, da dieses Tool alle Details über unsere Anlage sehr schnell bereitstellt und wir diese Daten als Grundlage für unsere Entscheidungen nutzen können. Wir müssen wissen, wie viele Kunden von Stromausfällen betroffen sind.“

— Chris Perez, Enterprise Technology Solutions Advisor bei Puget Sound Energy



Datengestützte Ergebnisse

500 Tsd. USD erwartete
Einsparung durch Konsolidierung von
Analyselösungen

135 Tsd. USD jährlicher ROI durch
die Abschaffung veralteter Tools

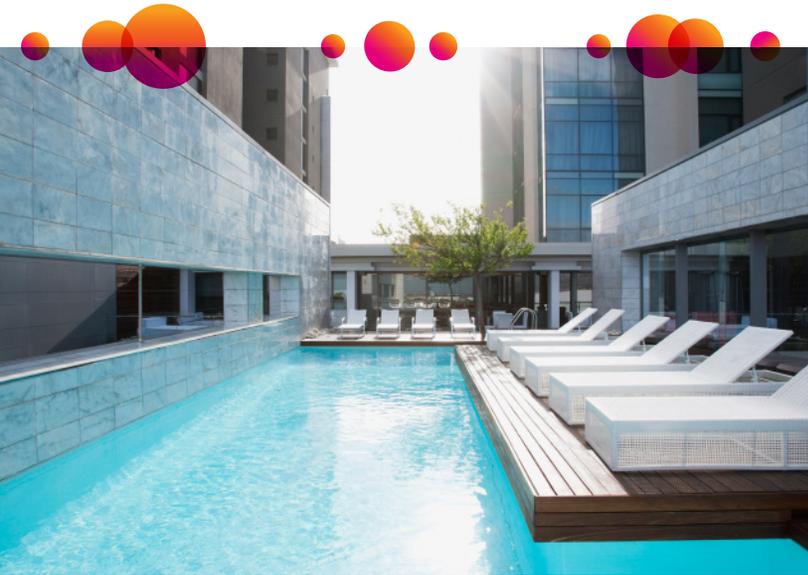
150 Kommunikationsstandorte und
70 Bürostandorte arbeiten jetzt effizienter

A topographic map with light blue contour lines is the background. Overlaid on the map are several lines representing travel routes: a solid magenta line that starts from the left and curves upwards; a solid orange line that continues from the magenta line and curves to the right; and a dashed orange line that branches off from the solid orange line and curves further to the right. A faint dotted grey line also follows a path across the map.

Reise und Verkehr

Branche
Reise und Verkehr

Lösungen
IT Operations
Security
Unternehmerische Erkenntnisse



Datengestützte Ergebnisse

Erweiterter Zugriff auf die Splunk-Plattform von
12 Personen auf mehr als 100 Benutzer täglich

Verkürzung der MTTR von Stunden auf Echtzeit

Höhere Kundenzufriedenheit durch proaktives
Monitoring

HYATT senkt die MTTR und gibt Entwicklern mehr Zeit für innovative Lösungen

Zentrale Herausforderungen

Um seinen Gästen in 700 Hotels und auf ebenso vielen Servern eine nahtlose Erfahrung bieten zu können, benötigte Hyatt zuverlässige IT-Prozesse, eine ständige Verfügbarkeit ohne Ausfälle und eine einzige Plattform, um Daten überwachen und als Handlungsgrundlage heranziehen zu können.

Wichtige Ergebnisse

Von Reservierungen bis zum Einchecken gewinnt Hyatt nun unternehmensweit Erkenntnisse, die ein schnelles Erkennen und Lösen von Problemen sowie eine bessere Gasterfahrung ermöglichen.

Hyatt wollte seinen Gästen eine durchgehend angenehme Erfahrung bieten und suchte zu diesem Zweck eine zentralisierte Lösung zur Verbesserung der Anwendungsbereitstellung und Problembeseitigung auf seinen 700 Servern. Vor der Nutzung der Splunk-Plattform war der Online-Check-In nicht wirklich zuverlässig und die Entwickler mussten sich bei einem einzelnen Server anmelden und ein Suchwerkzeug ausführen, um herauszufinden, was passiert war. Das konnte Stunden dauern. Außerdem hatte das Team keine Möglichkeit, festzustellen, ob ein Problem lokal auf einem Server oder auf mehreren Servern auftrat. Mit der Technologie von Splunk beheben die Mitarbeiter von Hyatt Serverprobleme nun umgehend und die schnellere Problemlösung sorgt für zufriedeneren Gäste.



Splunk ist das Fenster, durch das wir den Zustand unserer Anwendungen sehen können.“

— Cesar Mendoza, Application Development Manager, Strategic Systems and Innovation

Splunk macht operative Erkenntnisse „ready for take off“ bei **Gatwick Airport**

Zentrale Herausforderungen

Gatwick Airport musste riesige Mengen unzusammenhängender Daten aus unterschiedlichen Quellen auswerten. Dazu war eine vollständige Live-Übersicht über die Flughafenabläufe erforderlich.

Wichtige Ergebnisse

Durch Splunk haben mehr Teams in Gatwick Zugang zu den Daten erhalten. Dadurch wurde die Effizienz verbessert, Kosten gesenkt und das Team erhielt Unterstützung durch den Rund-um-die-Uhr-Support von Splunk Cloud und ein SLA, das 100 % Verfügbarkeit verspricht.

Im Gatwick Airport werden jährlich 46 Millionen Passagiere abgefertigt und er ist damit weltweit der effizienteste Flughafen mit nur einer aktiven Start- und Landebahn. Gatwick konkurriert in und um London mit einer Reihe weiterer Flughäfen, ist jedoch aufgrund dieser einen Start- und Landebahn, auf der stündlich bis zu 55 Flugbewegungen stattfinden, im Nachteil. Folglich ist das Wachstum stark davon abhängig, dass es gelingt, die Effizienz für diese eine Start- und Landebahn zu steigern. Durch Splunk haben mehr Teams Zugang zu Live-Informationen erhalten. Mithilfe der Software konnte die Ointime-Leistung verbessert und die Effizienz gesteigert werden. So ist Gatwick über sich hinausgewachsen und hat seine Ziele erreicht.

[Video ansehen](#)

INHALT



Wir haben jetzt eine Granularitätsstufe erreicht, bei der wir uns zu jeder beliebigen Position der Sicherheitskontrollen ein umfassendes Bild der Performance machen können. Unsere Daten liefern Antworten auf Fragen wie etwa: ‚Wie können wir die gestrige Ointime-Leistung verbessern?‘ oder ‚Was verursachte die Verschlechterung?‘“

— Alex Webber und Paul Bannister, IT Development Specialists



Datengestützte Ergebnisse

Nr. 1 – der weltweit effizienteste Flughafen mit nur einer Start- und Landebahn

95 % der Passiere passieren die Sicherheitskontrollen in weniger als fünf Minuten

945 Flugbewegungen täglich, jährliches Passagieraufkommen von 46 Millionen

Branche
Reise und Verkehr

Lösungen
IT Operations
Security
IoT und Industrie 4.0



Datengestützte Ergebnisse

95 % der Passiere passieren die Sicherheitskontrollen in maximal fünf Minuten

Nr. 1 – schnellstes Flughafen-WLAN der Welt, komplett ohne Funklöcher

150 Mio. Gepäckstücke erreichen jährlich durch Monitoring von 200 Datenpunkten ihr Ziel

Dubai Airports fliegt mit Splunk in die Zukunft

Zentrale Herausforderungen

Dubai Airports ist der verkehrsreichste Flughafen der Welt. Da eine physische Ausdehnung aus Platzmangel nicht möglich ist, musste die Flughafenkapazität erhöht werden, ohne die Terminals, die Infrastruktur oder die Anzahl der Start- und Landebahnen zu erweitern.

Wichtige Ergebnisse

Mithilfe von Sensordaten konnte der Flughafen seine Kapazität erweitern und gleichzeitig das Erlebnis der Reisenden verbessern. Dabei wurde unter anderem die Wartezeit für die Sicherheitskontrolle auf unter fünf Minuten verkürzt und das Gepäckaufkommen zwecks Effizienzsteigerung vorhergesagt.

Dubai Airports ist mit einem erwarteten Fluggastaufkommen von 100 Millionen Reisenden pro Jahr der weltweit verkehrsreichste Flughafen für internationale Reisen. Mit Splunk erreicht der Flughafen sein Ziel, die Sicherheitsabfertigung von 95 % der Passagiere in maximal fünf Minuten durchzuführen, und zwar durch Monitoring der Metalldetektoren, damit Entwicklungen erkannt und die Wartenden optimal verteilt werden können. Das IT-Team setzt Echtzeit-Monitoring für sämtliche WLAN-Zugriffspunkte des Flughafens ein, um Engpässe und fehlerhafte Hotspots sofort erkennen und beheben zu können.

Jedes Gepäckstück im Gepäcksystem von Dubai Airports erzeugt mehr als 200 Datenpunkte, die alle in Splunk überwacht werden, um sicherzustellen, dass das Gepäck das gewünschte Ziel erreicht. Eine weitere Effizienzsteigerung erreicht der Flughafen durch die Kombination von Gepäckdaten und Ablaufdaten. So kann das Gepäckaufkommen prognostiziert und Ressourcen können entsprechend zugewiesen werden.

[Video ansehen](#)



Wir setzen Splunk ein, um das Reiseerlebnis von Millionen von Menschen deutlich zu verbessern.“

— Michael Ibbitson, Executive Vice President, Technology & Infrastructure bei Dubai Airports

Branche
Reise und Verkehr

Lösungen
IT Operations
IoT und Industrie 4.0

Sapura nutzt Splunk für die IoT-Vernetzung an Bord, an Land und unter Wasser

Zentrale Herausforderungen

Sapura benötigte Echtzeittransparenz für das Monitoring komplexer Systeme und vernetzter Schiffe, um Sicherheitsstandards einzuhalten und Umweltkatastrophen zu verhindern.

Wichtige Ergebnisse

Sapura nutzt die Splunk-Plattform zur Anwendung eines datengestützten Ansatzes für seine Unterseekonstruktion und steigert damit seine operative Effizienz bei gleichzeitiger Stärkung der Sicherheitsstandards.

An Bord der Schiffe führt ein Team von Sapura-Crewmitgliedern gemeinsam mit Technikern, Ingenieuren, Mechanikern und Kapitänen von Kunden und Drittanbietern komplexe Abläufe durch, um die Rohrverlegung 3.000 Meter unter dem Meeresspiegel durchzuführen. Sapura benötigte Lösungen für das Echtzeit-Monitoring und -Troubleshooting auf diesen Schiffen, bei denen es sich im Wesentlichen um schwimmende Rechenzentren handelt. Noch bis vor Kurzem wurden die einzelnen Datenströme in separaten Silos erfasst. Auf den Schiffen tätige Crews setzten Splunk-Dashboards ein, um kritische Situationen zu überwachen und erhielten Einblick in Sapuras zentrales Rohrverlegesystem.



Splunk for Industrial IoT ist eine leistungsstarke Lösung zur Verbesserung unserer Möglichkeiten, Daten in unserem gesamten Unternehmen zu nutzen, um unsere Sicherheitsstandards zu stärken, die operative Performance zu steigern und unseren Kunden bessere Lösungen zu liefern.“

— André Merlino, CEO von Sapura Brazil



Datengestützte Ergebnisse

Schneller Return-on-Investment

Verbesserung der **Sicherheit und Produktivität im Betrieb**

Echtzeiteinblicke **in komplexe Industriesysteme** und Reduzierung der Anlagenausfälle

Mehr Erfahrungsberichte von Unternehmen,
die das volle Potenzial ihrer Daten nutzen,
finden Sie unter splunk.com/data-pioneers.