WHITEPAPER

Splunk-Lösungen für die Reaktion auf COVID-19

Unterstützung des öffentlichen Sektors in Zeiten der Coronavirus-Pandemie

splunk> turn data into doing™

Inhalt

Einleitung

Die COVID-19-Pandemie stellt im Hinblick auf die öffentliche Gesundheit Einzelpersonen und eine breite Palette von Organisationen – von Schulen und Krankenhäusern bis hin zu Kommunen und Zentralregierungen – vor beispiellose Herausforderungen. In einer Zeit, in der schnelles Handeln entscheidend ist, steht Splunk an der Seite seiner Kunden. Das gilt insbesondere für diejenigen, die unmittelbar im Rahmen der Versorgung und Krisenbewältigung tätig sind. Diese Personen mit Tools und Lösungen zur effektiven Nutzung ihrer Daten zu unterstützen, damit sie mit der Geschwindigkeit, die diese Krise erfordert, fundierte Entscheidungen treffen und entschlossen handeln können, ist eine unserer vordringlichsten Aufgaben.

Weltweit wird darauf hingearbeitet, die Ausbreitung des Virus zu stoppen, Test- und Behandlungsergebnisse zu verbessern und die am stärksten gefährdeten Bevölkerungsgruppen zu schützen. Hierbei sind Daten eine wertvolle Ressource. Sie helfen bei der Umsetzung von Maßnahmen zur Verlangsamung der Virusausbreitung sowie bei der Aufrechterhaltung und Bereitstellung wichtiger Infrastrukturen und Services und helfen uns gleichzeitig, nicht in Panik und Angst zu verfallen. Daher unterstützt Splunk Organisationen dabei, ihre Daten während dieser Krise bestmöglich zu nutzen, um so angemessen reagieren und die negativen Auswirkungen der Pandemie abwenden zu können. Bereits in der Vergangenheit hat Splunk im Rahmen der Katastrophenhilfe mit unterschiedlichen Partnern zusammengearbeitet. Unsere Reaktion auf COVID-19 baut auf diesem Fundament auf.

Um Organisationen zu helfen, sich in der aktuellen Situation besser zurechtzufinden und krisenbedingte neue Betriebsmodelle einfacher umzusetzen, hat Splunk für seine Kunden Informationen, praktische Tipps und eine Liste mit **eigens konzipierten Lösungen** zusammengestellt. Die entsprechenden Informationen finden Sie auf unserer **Website zur Reaktion auf COVID-19**. Einige dieser Lösungen können kostenlos auf einer bestehenden Splunk-Plattform eingesetzt werden. Bei anderen handelt es sich um kommerzielle Angebote.

Auf den kommenden Seiten dieses Whitepapers legen wir dar, wie Splunk Sie bei der Bewältigung von etwaigen Herausforderungen in den folgenden Bereichen unterstützen kann:

- Besseres Situationsbewusstsein
- Remote-Arbeit
- Eindämmung von Cyberbedrohungen
- Skalierbarkeit und Flexibilität

Technologie spielt besonders in der aktuellen Lage eine wichtige Rolle, um wesentliche Services am Laufen zu halten und Unterstützung zu bieten, wo und wann immer es erforderlich ist und Splunk ist entschlossen hierbei seinen Beitrag zu leisten. Wir haben einige kurzfristige Lösungen erarbeitet, um Organisationen bei der Bewältigung aktueller Herausforderungen zu unterstützen. Selbstverständlich bieten wir nach wie vor unser traditionelles Lösungspaket an, mit dem Sie sich auch langfristig strategische Vorteile sichern können.

Die Lockdown-Maßnahmen werden in ganz Europa nach und nach aufgehoben, aber für viele Menschen, auch in öffentlichen Verwaltungen, bleibt Remote-Arbeit an der Tagesordnung. Jetzt, bevor ein Impfstoff zur Verfügung steht, muss die Welt lernen, wie man mit dem Virus leben kann. Wir bei Splunk sind davon überzeugt, dass Daten beim globalen Neustart eine wichtige Rolle spielen müssen. Dank Datenanalysen können Unternehmen und Organisationen des öffentlichen Sektors wieder sicher an die Arbeit gehen. Ein umfangreiches Verständnis der am Arbeitsplatz generierten Daten – z. B. Ausweisaktivität, Sensoren in der Fabrikhalle, Muster zur Aufzugsnutzung usw. – ist der Schlüssel zur Entwicklung einer auf die jeweiligen Organisationen zugeschnittenen Strategie zur Rückkehr an den Arbeitsplatz. Durch die Kombination einer solchen Analyse mit öffentlich verfügbaren Daten über lokale Gesundheitssysteme, öffentliche Verkehrsmittel oder Wettervorhersagen, können Organisationen datengestützte Entscheidungen treffen, die einen großen Anteil an der Sicherheit von Mitarbeitern am Arbeitsplatz haben.

Erfahren Sie mehr darüber, in unserem Global Restart Programm.

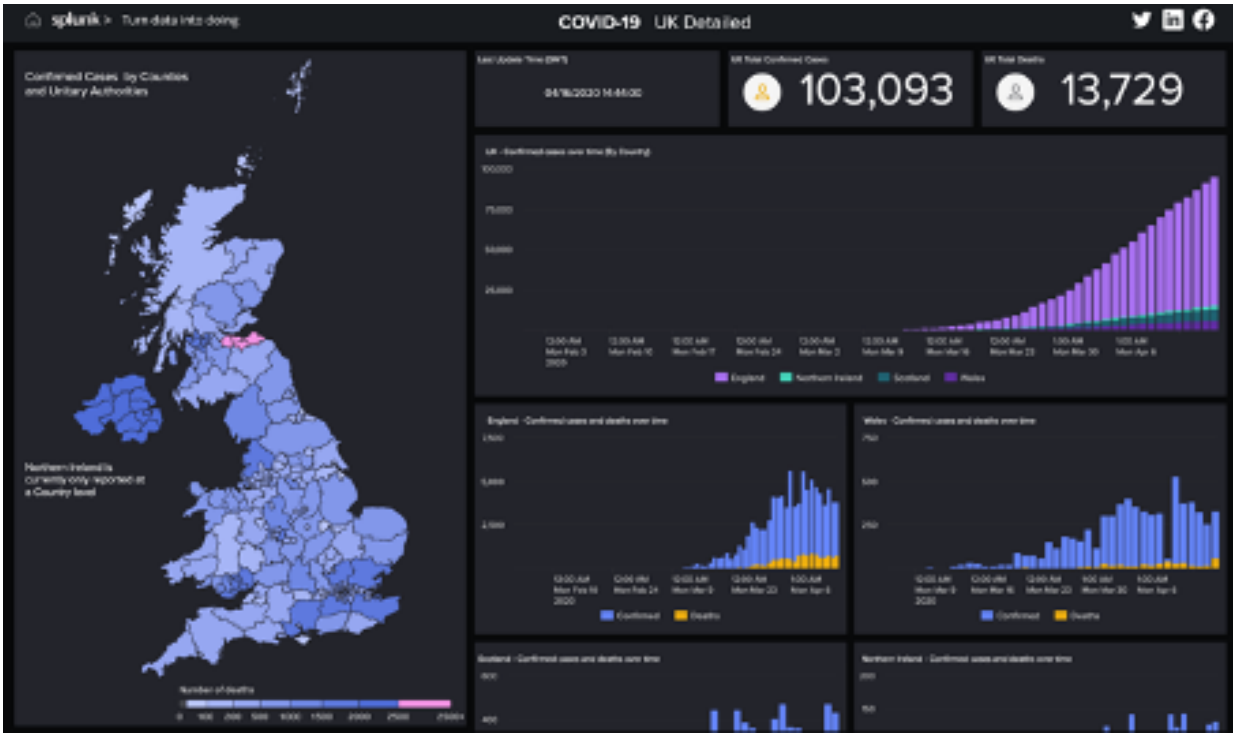
Besseres Situationsbewusstsein

Es ist wichtig, dass Regierungsorganisationen Entwicklungen rund um COVID-19 zuvorkommen und die globale und lokale Lage bestmöglich monitoren. Regierungsstellen müssen wichtige Informationen an ihre Bürger und Partner weitergeben und darüber hinaus die interne Service-Bereitstellung auf effiziente Weise überwachen.

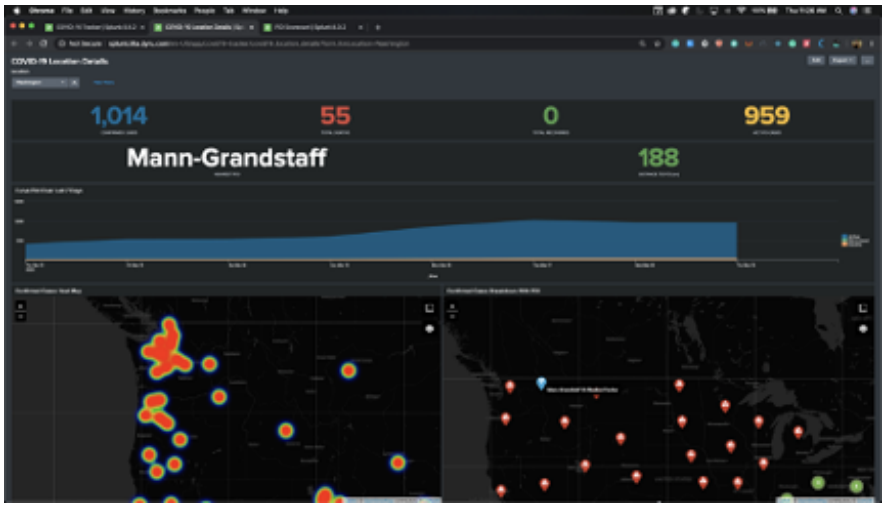
Splunk COVID-19-Dashboard

Im März hat Splunk ein **neues Dashboard** bereitgestellt, das öffentlich zugängliche Daten verwendet, um die globale Ausbreitung von COVID-19 zu verfolgen. Parallel dazu haben wir **eine Anwendung** veröffentlicht, die von unserer Kunden- und User-Community mit eigenen Daten gefüllt und dazu verwendet werden kann, die Datenlage rund um die Pandemie besser zu verstehen. Es mangelt nicht unbedingt an stimmigen und belastbaren Daten, allerdings kann es schwer sein, diese zu identifizieren und auszuwerten. Dank unserer jahrzehntelangen Erfahrung in der Bereitstellung datengestützter Lösungen für Kunden auf der ganzen Welt können wir beim schnellen Identifizieren, Erfassen und Korrelieren relevanter Daten helfen und über anpassbare Dashboards ansprechende, leicht verständliche Visualisierungen bieten.

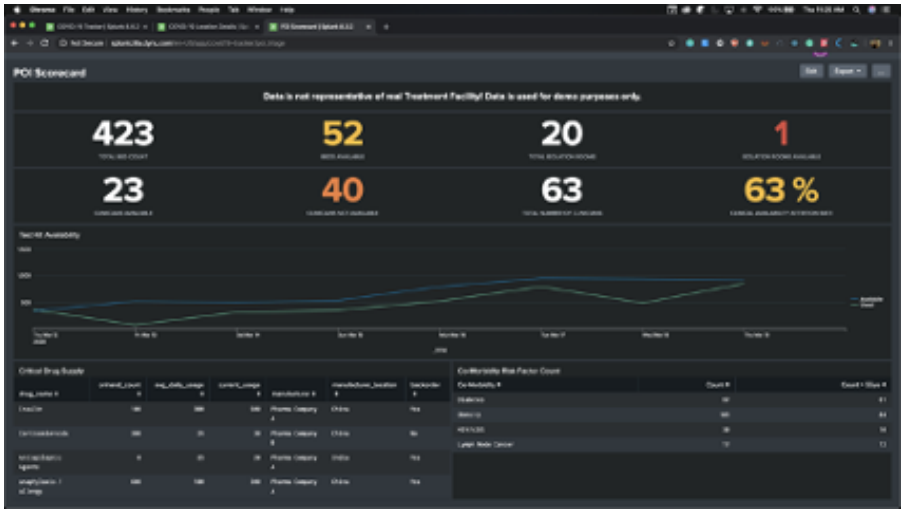
Nachfolgend finden Sie einige Dashboards, die von uns selbst sowie dem Team bei Leidos Healthcare mit der Hilfe von Splunk entwickelt wurden. Diese Dashboards wurden mit Daten der Johns Hopkins University bzw. der britischen Regierung erstellt. Alle Dashboards bieten ansprechende, leicht verständliche Visualisierungen und können angepasst werden oder bestimmte weitere Datenquellen erfassen und die relevanten Daten rasch korrelieren.



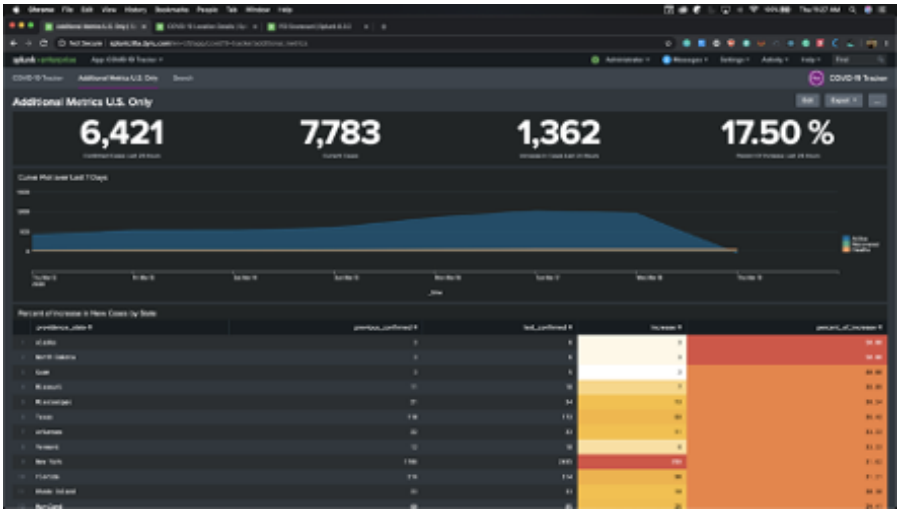
COVID-19: Großbritannien – detaillierte Metriken mit Karte



COVID-19: Standortspezifische Metriken mit nächstgelegenem Point-of-Interest, einschließlich Heatmap und Standortkarten mit Ausbruchsclustern.



COVID-19: Pandemiebezogene Informationen wie Versorgung mit wichtigen Medikamenten, Verfügbarkeit von Testkits, Anzahl risikofördernder Zusatzerkrankungen, Ausfallquote bei Ärzten, verfügbaren Betten



COVID-19: Klinisches Ressourcenmanagement mit prozentualem Anstieg neuer Fälle nach Bundesstaat und VISN

VPN-Dashboard

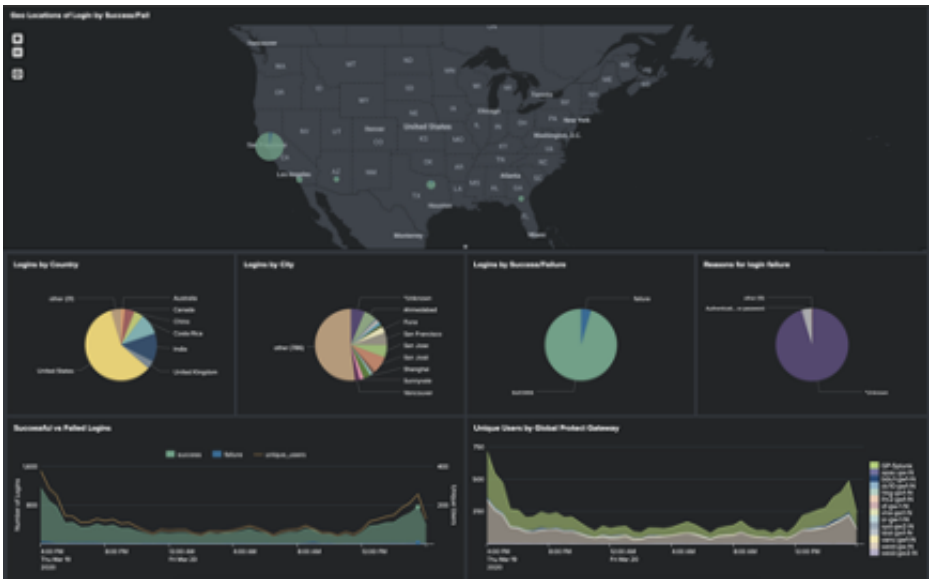
Das Konzept der Telearbeit ist zwar nicht neu, doch aufgrund der sich ausbreitenden Pandemie ist der Bedarf an Remote-Arbeitsplätzen enorm angestiegen.

In den meisten Staaten Europas wurden mittlerweile auf allen Ebenen – von den Kommunalverwaltungen und Landesregierungen bis hin zur Zentralregierung – Möglichkeiten zu Remote-Arbeit eingerichtet. In den EU-Institutionen kommen überall Technologien für Remote-Zusammenarbeit zum Einsatz. Andere politische Institutionen wie etwa die Houses of Parliament in London nutzen Telefonkonferenzeinrichtungen für die Anhörungen der Ausschüsse.

Da Organisationen zunehmend auf Remote-Arbeit umsteigen und ihre Kapazitäten in diesem Bereich ausbauen, ist beim Einsatz von Netzwerk-, Remote-Zugriffs- und Kollaborationssoftware ein rapider Anstieg zu verzeichnen. Angesichts der steigenden Anzahl von Endpunkten, die von entfernten Standorten auf Ihr Netzwerk zugreifen, sollten Sie mit einer raschen Zunahme der VPN-Verbindungen und -Nutzung rechnen. Darüber hinaus können Social-Media-Streaming und andere außerfachliche Aktivitäten Ihr Netzwerk verstopfen und Reaktionen verlangsamen.

Da VPNs häufig für Remote-Arbeitszwecke eingesetzt werden, ist Splunk Partnerschaften mit Anbietern branchenführender VPN-Technologien (**Cisco, Palo Alto, Fortinet und andere**) eingegangen, um umfassende Endpunkttransparenz und das Monitoring des VPN-Betriebs zu ermöglichen. Die meisten Organisationen möchten ihren Mitarbeitern ein effektives Arbeiten aus der Ferne ermöglichen und sie mit den Tools ausstatten, die sie zum bestmöglichen Erfüllen ihrer Aufgaben benötigen. Die strategischen Partner von Splunk haben Tools entwickelt, mit denen Endpunktdaten analysiert und über eine angepasste Monitoring- und Warnkonsole dargestellt werden können. So können Kunden die User Experience und das Endpunktverhalten schnell analysieren und kritische Sicherheits- und Betriebsfragen unter Verwendung von Infrastruktur- und Endpunktdaten beantworten, die sich innerhalb oder außerhalb des eigenen Netzwerks befinden.

Im nachfolgend als Beispiel angeführten VPN-Dashboard werden der geografische Standort von vernetzten Geräten sowie erfolgreiche und fehlgeschlagene Anmeldungen dargestellt und die Zahl der User aufgezeigt, die das VPN im zeitlichen Verlauf nutzen.



Mit Splunk erfasste und analysierte Server- und Endpunktdaten werden beispielsweise für folgende VPN-Anwendungsfälle verwendet:

Status und Statistiken von Client Sessions

- Wie viele Clients sind verbunden und sind deren Sitzungen effizient?
- Optimieren der MTTR (Mean Time to Resolution) bei VPN-Serviceproblemen

Monitoring der VPN-Infrastruktur

- Ressourcen-Monitoring zur Analyse und Überwachung der Auslastung der VPN-Infrastruktur
- Monitoring des Netzwerkverkehrs, um Erkenntnisse über Auswirkungen auf das Netzwerk zu gewinnen

Feststellen von Datenverlust

- Datenhortung – Download- und Upload-Verhalten
- Exfiltration – Upload auf externe Domänen und Netzwerkfreigaben

Zero-Day-Malware und Bedrohungssuche

- Ungewöhnliches Verhalten von Apps/Prozessen – ausgeführt auf Root-Ebene oder Nichtstandard-Ports
- Erkennung von Command & Control-Servern – sprunghafter Anstieg von Verbindungen zu neuen, ungewöhnlichen oder ungültigen Domänen
- Bedrohungserkennung – Korrelation zwischen Anwendungsprozess und Hostdomäne

Zero-Trust-Monitoring

- Monitoring von Geräten außerhalb des eigenen Netzwerks – Benutzer-, Geräte-, Datenverkehr-, App- und Datenverhalten
- SaaS-Nutzungsverhalten – verfolgen, welche SaaS-Services genutzt werden
- Nicht vertrauenswürdige Verbindungen – verfolgen, wenn eine Verbindung zu nicht vertrauenswürdigen Netzwerken herstellt wird

Sichtbarkeit von nicht genehmigten Anwendungen und SaaS

- SaaS-Domänen mit Zugriffen – Verbindungen und SaaS-Nutzungsverhalten
- Sichtbarkeit von Anwendungen und Prozessen – Apps und Prozesse finden, die auf Geräten ausgeführt werden

Umgehung von Sicherheitsmaßnahmen und Benutzerzuordnung

- Sicherheitsanwendungen für Endpunkte – erkennen, ob deaktiviert oder nicht installiert
- CESA – erkennen, ob deaktiviert oder nicht installiert
- Zuordnen von Benutzern zu Netzwerkzugriff – Benutzeraktivität bis hinunter zum Netzwerkschnittstellen-Controller

Bestandsaufnahme

- Bestandsaufnahme von Gerätetypen und Betriebssystemen – identifizieren und Bericht nach Typ erstellen
- Einhaltung von Datenschutzrichtlinien – bestätigen des Entfernens personenbezogener Daten von Geräten

Remote-Arbeit

Dadurch das Einzelpersonen und Organisationen immer mehr auf Remote-Arbeit umsteigen, werden Netzwerke zunehmend belastet und sogar überlastet. Wenn Beschäftigte des öffentlichen Diensts auf Telearbeit umsteigen, ist der Zugang zu sicheren Kollaborationstools entscheidend, damit öffentliche Einrichtungen ihre Bürgerservices aufrechterhalten können.

Remote Work Insights (RWI)

Für Organisationen, die unmittelbare Unterstützung benötigen, hat Splunk eine angepasste Version seines Cloud-Autobahn-Programms (**Remote Work Insights (RWI) Autobahn**), eingeführt. Es soll Behörden dabei unterstützen, eine Reihe wichtiger Datenquellen in **Splunk Cloud** zu integrieren und rasch umsetzbare Erkenntnisse zu gewinnen. Dieses kostenlose Programm zum Nutzennachweis (Proof-of-Value) bietet berechtigten Kunden einen präskriptiven Ansatz für proaktive Sichtbarkeit und zur Verkürzung der Problemlösungszeit in ihrer Organisation. Mit den Remote-Monitoring-Funktionen von Splunk lassen sich wichtige KPIs überwachen, auftretende Probleme erkennen und umfangreiche Kernursachenanalysen durchführen – alles auf einer Plattform. Weitere Informationen zu den Ressourcen, die über Remote Work Insights bereitstehen, darunter Apps und Add-ons für lokale Splunk-Installationen und Anleitungen für den Einstieg, sind auf unserer **Website zur Reaktion auf COVID-19** verfügbar.

ITSI

IT Service Intelligence (ITSI) von Splunk kann als zusätzliche Ebene über den Solution Stack gelegt werden, um von Monitoring-, Analyse- und KI-Funktionen zu profitieren, die Erkenntnisse aus der gesamten Infrastruktur, Business Services und Anwendungen liefern. Durch das Korrelieren von Protokollen, Metriken und Änderungs-Management-Daten aus mehreren Silos können Behörden komplexe Abhängigkeiten nachvollziehen und nahezu in Echtzeit den Status erfolgskritischer Lösungen (beispielsweise den VPN-Zugriff für Mitarbeiter im Home-Office) anzeigen lassen. Mithilfe den integrierten Machine Learning-Funktionen von ITSI können Administratoren Anomalien erkennen, Ausfälle vor deren Eintreten prognostizieren und bereits zur Kernursachenanalyse übergehen, bevor die Systemverfügbarkeit von einem Ausfall beeinträchtigt wurde.

VictorOps

Des Weiteren stellt sich die wichtige Frage, was öffentliche Einrichtungen tun können, damit ihre Mitarbeiter in einer Remote-Umgebung optimal arbeiten können. Kollaborationstools sind grundsätzlich entscheidend für erfolgreiches Arbeiten und zwar nicht nur für Knowledge Worker oder Fallmanager, sondern auch für die Mitarbeiter im Helpdesk- und Support-Bereich. Wenn die gesamte Infrastruktur auf die Bereitstellung erfolgskritischer Services ausgerichtet ist, müssen Systeme im Falle von Ausfällen, Unterbrechungen oder gar einem Cyberangriff schnell wiederherstellbar sein. Während Monitoring-Tools eingesetzt werden, um Mitarbeiter zu benachrichtigen, kann eine effektive Zusammenarbeit entschlossenes Handeln beschleunigen.

Splunk kann Ihre Teams beim Ausbau der Systeme für die Remote-Arbeit unterstützen. Unsere Kollaborationslösung, **VictorOps**, lässt sich zur Automatisierung des Incident-Managements nahtlos in Splunk Enterprise oder Splunk Cloud integrieren und sorgt für eine Reduzierung von Over-Alerting und eine Erhöhung der Uptime. Die Lösung gibt Warnmeldungen direkt an die richtigen Mitarbeiter weiter und versetzt Teams damit in die Lage, Probleme gemeinsam schneller zu lösen. Durch das Optimieren von Bereitschaftsplänen und Eskalationsrichtlinien sorgt VictorOps für Effektivität bei Routing und Problembehandlung. Und durch die Bereitstellung von sowohl Warnmeldungen samt Kontextdaten als auch von Machine Learning getriebenen Lösungsvorschlägen wird die Zusammenarbeit gefördert und eine schnelle und effiziente Problemlösung erreicht. Gleichzeitig werden wichtige Daten zur Problembehebung erfasst. Über native iOS- und Android-Apps kann der zuständige Mitarbeiter auf jedem Gerät mit Metadaten angereicherte Benachrichtigungen empfangen.

Eindämmung von Cyberbedrohungen

Die Bedrohung

Regierungsorganisationen und kritische Infrastrukturen geraten zunehmend ins Visier von Angreifern, die unsichere Zustände skrupellos ausnutzen. Seit dem Ausbruch der Krise sind sogar Gesundheitsorganisationen zur Zielscheibe von Cyberangriffen geworden – beispielsweise Krankenhäuser in Paris oder das Nationale Institut für öffentliche Gesundheit in den Niederlanden. Durch die Zunahme der Remote-Arbeitsmöglichkeiten bietet sich eine noch größere Angriffsfläche. Endpunkt-Monitoring ist daher wichtiger denn je.

Das Nationale Zentrum für Cybersicherheit (NCSC) in Großbritannien hat für Organisationen Empfehlungen zur Senkung des Risikos von Cyberangriffen auf eingesetzten Geräten wie Laptops, Mobiltelefonen und Tablets sowie Tipps für Mitarbeiter zum Erkennen der typischen Anzeichen von Phishing-Angriffen veröffentlicht. Das NCSC gibt darin einen Überblick über empfehlenswerte Schritte für Organisationen zur Vorbereitung auf Telearbeit, Einrichtung neuer Konten und Zugriffsdaten, Steuerung des Zugriffs auf Unternehmenssysteme, Unterstützung der Mitarbeiter beim Schutz ihrer Geräte sowie zur Senkung des Risikos von Wechselmedien. Die Agentur der Europäischen Union für Cybersicherheit (ENISA) hat ähnliche Empfehlungen für Unternehmen veröffentlicht, die auf Remote-Arbeit umsteigen. In Deutschland hat das Bundesamt für Sicherheit in der Informationstechnik (BSI) ebenfalls Richtlinien für die Senkung von Cyberrisiken in Zeiten des Coronavirus erstellt.

Für alle öffentlichen Einrichtungen in Großbritannien, die jetzt schnell sichere Remote-Arbeit ermöglichen müssen, hat das NCSC einen **COVID-19-Warnhinweis** herausgegeben. Splunk kann Sie bei der raschen Optimierung des Sicherheitsniveaus Ihrer Organisation unterstützen, Risiken mindern und versteckte Lücken in Sicherheits- und Betriebsprozessen aufdecken, die Systeme anfällig für Datenschutzverletzungen und die Nichteinhaltung von Vorschriften machen. Mithilfe von Machine Learning automatisiert Splunk Security Monitoring sowie Bedrohungs- und Anomalie-Erkennung, damit Ihre begrenzten Sicherheitsressourcen mehr Zeit für die Analyse von zuverlässigeren, verhaltensbasierten Warnmeldungen aufwenden und rascher Lösungen finden können.

Splunk Security Essentials (SSE)

Insbesondere Konto-Kompromittierungen spielen eine immer größere Rolle, da die Endpunkte Ihrer Mitarbeiter aufgrund von Faktoren, die sich Ihrer Kontrolle entziehen, einem höheren Risiko ausgesetzt sind. Beispielsweise werden Benutzer anfälliger für Angriffe, wenn auf ihren privaten Routern keine Sicherheitsmechanismen eingerichtet sind. **Splunk Security Essentials (SSE)** ist eine kostenlose Anwendung, die Security-Abläufe vereinfacht und Ihnen die Möglichkeit gibt, Datenquellen und Funktionen zu überprüfen sowie Erkennungsfunktionen zu testen und zu implementieren, die Cybersicherheits-Frameworks wie **MITRE ATT&CK** und anderen zugeordnet sind.

Splunk ermöglicht **ausgereiftere Sicherheitsabläufe** über den gesamten Event-Lebenszyklus hinweg und kann Unternehmen bei der Verbesserung ihrer Richtlinien für Cybersicherheit unterstützen. Über das **Adaptive Operations Framework** steht ein robustes Partnernetzwerk mit führenden Akteuren der Cybersicherheitsbranche bereit, sodass unsere Kunden von leistungsfähigen Instrumenten zur Erkennung und Eindämmung von Bedrohungen profitieren. Die Best Practices, die Sie heute anwenden, können Ihr Sicherheitsniveau in Zukunft beträchtlich erhöhen.

Phantom

Mit Splunk **Phantom**, der Plattform für Orchestrierung und Automatisierung von Splunk, wird Automatisierung einfach, intuitiv und effektiv. Monotone Routinearbeiten werden übernommen, sodass Ihre knappen Personalressourcen für wichtigere Aufgaben eingesetzt werden können.

Phantom wird in der Regel in Sicherheits- oder Netzwerkbetriebszentren eingesetzt, um Herausforderungen bei Volumen, Reaktionszeit, Wiederholbarkeit und Know-how zu bewältigen. Eine wichtige Herausforderung im Zusammenhang mit COVID-19 ist ein reduzierter Personalbestand, da Mitarbeiter möglicherweise nicht vom Büro aus arbeiten können, weil sie verstärkt in die Kinderbetreuung eingebunden sind, oder schlimmstenfalls gar nicht in der Lage sind zu arbeiten. Wenn die Anzahl der Warnmeldungen steigt und die Personaldecke dünner wird, sind SOCs und NOCs mit sowohl volumenbezogenen Herausforderungen als auch mit fehlendem Know-how konfrontiert, weil wichtige Mitarbeiter nicht mehr an ihrem Arbeitsplatz sein können. Automatisierung bietet Technologieteams die Möglichkeit, den erheblichen Rückstau beim Workload aufzulösen, mehr zu schaffen und sich auf die Aufgaben zu konzentrieren, die wirklich personelle Aufmerksamkeit erfordern.

Mit automatisierten Reaktionen – in Phantom „Playbooks“ genannt – lassen sich Prozesse so einrichten, dass auch unerfahrene Benutzer sie genau so ausführen können, wie Experten es tun würden. Das ist ein entscheidender Vorteil. Dadurch kann das tatsächliche Qualifikationsniveau eines Teams beträchtlich erhöht und Druck von den Schultern der überlasteten Führungskräfte genommen werden. Die Folge sind frei werdende Kapazitäten, eine drastisch gesenkte Reaktionszeit, eine verbesserte Konsistenz sowie Reaktionsfähigkeit rund um die Uhr. Wo es zulässig ist, ermöglicht Phantom den Teams auch eine Reaktion über Mobilgeräte.

Skalierbarkeit und Flexibilität

Der öffentliche Sektor stellt wichtige Services für Bürger in ganz Europa bereit. In diesen schwierigen Zeiten geschieht dies in der Regel mit reduzierten Ressourcen und enormen Anforderungen an die IT-Infrastruktur.

Splunk Cloud

Da die meisten Behörden noch immer auf ältere, lokale Anwendungen angewiesen sind, die nicht auf Remote-Zugriffe ausgelegt sind, können die Beschäftigten nur von ihren Workstations aus darauf zugreifen. Für Remote-Arbeit bieten VPN-Technologien sicheren Zugriff auf Anwendungen, was unter normalen Bedingungen auch gut funktioniert. Angesichts des Umfangs virtueller Arbeitsplätze in der aktuellen Situation, in der fast alle Mitarbeiter auf Remote-Zugriff angewiesen sind, kann der Zugriff über VPN jedoch einen Engpass verursachen. Cloud-Lösungen bieten gegenüber einer herkömmlichen lokalen Architektur den entscheidenden Vorteil, dass sie Skalierbarkeit „on demand“ ermöglichen und speziell auf Flexibilität und sicheren Zugriff ausgelegt sind.

Bei der Migration von Behörden in die Cloud ist die operative End-to-End-Transparenz vor, während und nach der Umstellung unerlässlich, um Einblick in die Performance zu erhalten und Bedenken hinsichtlich der Infrastruktur- und Anwendungstransparenz auszuräumen. Außerdem lassen sich damit eventuelle Schuldzuweisungen vermeiden, falls wichtige SLAs nicht eingehalten werden und der Ruf des IT-Teams auf dem Spiel steht.

Wie bedeutet also operative Transparenz in einer Cloud-/Hybrid-Umgebung? Es handelt sich um eine umfassende Sicht auf die Infrastruktur- und Anwendungs-Performance über Workloads und Microservices hinweg, wobei deren Standort keine Rolle spielt. Diese Sicht liefert die Informationen, die für das Monitoring und Bewerten von KPIs erforderlich sind, um eine überzeugende User-/Bürgererfahrung zu gewährleisten, wenn die Infrastruktur öffentliche und private Domänen (Cloud und lokal) umfasst.

Wenn die Nutzung der unterschiedlichen Komponenten überwacht wird, aus denen sich Anwendungen oder Systeme zusammensetzen, hat das IT-Team darüber hinaus eine fundierte Basis für die Rationalisierung von Anwendungen. So können nur wirklich erforderliche Komponenten migriert, irrelevante eliminiert und Kosten gesenkt werden.

Splunk kann öffentlichen Einrichtungen zu objektiven, datengestützten Erkenntnissen verhelfen und beispielsweise den Ablauf von Initiativen modellieren und prognostizieren, um die gewünschten Ergebnisse zu erzielen. Das detaillierte Echtzeit-Monitoring hilft nicht nur beim Überwachen aller Migrationsphasen und erhöht so die Erfolgswahrscheinlichkeit, sondern kann auch einen Beitrag dazu leisten, Budgetüberschreitungen zu vermeiden, die durch übermäßigen Ressourcenverbrauch, unerwartete Ausgaben und fehlerhafte Abrechnungen verursacht werden. Dank datengestützter Erkenntnisse werden Behörden in die Lage versetzt, rasch fundierte Entscheidungen zu treffen und Maßnahmen einzuleiten. Egal ob für cloudbasierte oder lokale Umgebungen, große oder kleine Teams – Splunk hat in jedem Fall ein passendes Verteilungsmodell für Sie parat.

Fazit

Während COVID-19 weltweit weiterhin zu massiven Einschränkungen führt, konzentrieren wir uns bei Splunk darauf, unsere Stakeholder und unser gesamtes Umfeld in dieser Zeit anhaltender Unsicherheit zu unterstützen. Wir haben Schritte unternommen, um sicherzustellen, dass sich unsere Kunden auf der ganzen Welt weiterhin auf die Produkte und Services von Splunk verlassen können, um ihre Daten in konkrete Ergebnisse zu verwandeln. Wir wissen, wie wichtig unsere Plattform für die reibungslosen Abläufe unserer Kunden ist und arbeiten mit aller Kraft daran sicherzustellen, dass Sie Ihre angestrebten Ziele erreichen können.

Wenn Sie sich über den Inhalt dieses Whitepapers austauschen möchten, wenden Sie sich bitte an folgenden Kontakt:
Telefon: **+44 020 3204 4300** E-Mail: **Kontaktieren Sie unser Vertriebsteam für EMEA**

2020-pubsec-Splunk Solutions for COVID-19 Response-A4-107-WP