Expo 2020 Dubai – Sicheres Mega-Event dank Splunk

Zentrale Herausforderungen

Der Aufbau eines Mega-Events erfordert umfassendes und flexibles Monitoring. Die Expo 2020 benötigte eine Lösung, die den dynamischen Anforderungen ihrer vielfältigen Umgebung gerecht wird und die potentielle Cyber-Bedrohungen bewältigen kann.

Wichtige Ergebnisse

Die Splunk-Plattform erfasste mehrere Datenquellen und stattete die Expo mit belastbaren Cyber-Sicherheitsfunktion aus, welche die Möglichkeit boten, eine große Anzahl an Netzwerkereignissen genau zu überwachen, um so bei Bedarf schnell präventive Maßnahmen zu ergreifen.

Branche: Medien und Unterhaltung

Lösungen: IT Operations, Cyber-Security, Plattform

Datenquellen: Web Server, ERP-Systeme, Network Access Points

Der Schutz eines einzigartigen Mega-Events ist kein leichtes Unterfangen.

Und genau deshalb hatte die Cybersicherheit von Anfang an höchste Priorität für die Expo 2020 Dubai.

Der Schutz eines Events dieser Größenordnung und Dauer ist eine enorme Herausforderung. Die sechsmonatige Veranstaltung war die erste ihrer Art in der Region. Sie umfasste mehr als 190 Teilnehmer mit ihren entsprechenden Pavillons auf einer Fläche von 4,38 Quadratkilometern. Hinzu kamen die Themenpavillons, die sich mit Nachhaltigkeit, Mobilität und Zukunftschancen beschäftigten. Das Expo-Team ist für den Schutz des vielfältigen, dynamischen und progressiven Technologie-Ökosystems verantwortlich, das auf Hunderte von Teilnehmern sowie Millionen von Besuchern, einschließlich VIPs aus aller Welt, ausgelegt ist.

Um diese Herausforderungen zu bewältigen, brauchte die Expo 2020 eine Sicherheitsplattform, die schnell skalierbar ist, die operative Sicherheit Hunderter unterschiedlicher Datenquellen und Technologielösungen verwalten und flexibel an die wechselnden Cybersicherheitsanforderungen der Veranstaltung angepasst werden konnte. Die Splunk-Plattform erwies sich mit Blick auf diese Anforderungen als die beste Alternative.

Flexible Datenerfassung. Schnelle Skalierung.

Die Expo 2020 Dubai generiert erwartungsgemäß täglich etwa einen Terabyte an Daten, verteilt über eine riesige Umgebung, die mehr als 8.000 Zugriffspunkte, über 100 Sicherheitsgeräte und mehrere Clouds umfasst.

Angesichts einer so vielfältigen Umgebung und eines so hohen Datenvolumens brauchte die Expo eine Datenplattform, die dieser Aufgabe gewachsen war. „Splunk kristallisierte sich als eine SIEM-Technologie heraus, die flexibel,

Datengestützte Ergebnisse

Über 100
Sicherheitsgeräte und Technologielösungen werden mit Splunk geschützt

Ein
Terabyte an Daten werden pro Tag erfasst

Über 8.000
Zugriffspunkte und über 1.400 Server werden mit Splunk geschützt

effizient und effektiv genug ist, um die dynamischen Anforderungen der Cybersicherheitsumgebung der Expo zu bewältigen“, erklärt Eman Al Awadhi, Vice President Cybersecurity and Resilience bei der Expo.

Splunk ermöglichte die nahtlose Einspeisung von Daten aus einer Vielzahl von Quellen, einschließlich maßgeschneiderter Technologielösungen für den Expo-Betrieb. Es stellte sich heraus, dass die Plattform sowohl große Datenmengen als auch die anspruchsvolle, progressive Umgebung bewältigen kann. Darüber hinaus hat Splunk das Team in die Lage versetzt, das Monitoring innerhalb eines engen Zeitrahmens zusätzlich auszuweiten.

„Mit der Flexibilität von Splunk konnten wir die Bereitstellung problemlos an den veränderten Bedarf der Expo während der Pandemie anpassen, insbesondere mit Blick auf die Verschiebung des Events um ein Jahr.“, so Al Awadhi.

> Splunk kristallisierte sich als eine SIEM-Technologie heraus, die flexibel, effizient und effektiv genug ist, um die dynamischen Anforderungen der Cybersicherheitsumgebung der Expo zu bewältigen.“
>
> — **Eman Al Awadhi,** Vice President of Cybersecurity and Resilience, Expo 2020 Dubai

Mögliche Insider-Bedrohungen abwenden

Mega-Events und Großunternehmen werden regelmäßig mit einer Vielzahl von Sicherheitsvorfällen konfrontiert. Zudem haben sich Insider-Bedrohungen zu einem der größten Risiken für diese Organisationen entwickelt.

Um ihre Technologie-Ökosysteme vor Insider-Bedrohungen zu schützen, setzen die Verantwortlichen der Expo auf Echtzeitmonitoring zur Identifizierung von verdächtigem Verhalten. Die Splunk-Plattform bietet die Möglichkeit, ungewöhnliche Aktivitäten zu kennzeichnen und zu klassifizieren und ermöglicht es dem Expo-Team, unverzüglich auf potenzielle Bedrohungen zu reagieren und Abhilfemaßnahmen zu ergreifen.

> Mit der Flexibilität von Splunk konnten wir die Bereitstellung problemlos an den veränderten Bedarf der Expo während der Pandemie anpassen, insbesondere mit Blick auf die Verschiebung des Events um ein Jahr.“
>
> — **Eman Al Awadhi,** Vice President of Cybersecurity and Resilience, Expo 2020 Dubai

Echtzeitdaten für 360°-Transparenz

Die Cybersicherheitslage der Expo hängt von vielen unterschiedlichen Faktoren ab – von strategischen Initiativen bis hin zu angepassten Splunk-Dashboards, die Events in Echtzeit aggregieren und analysieren.

Dank schneller, umfassender Erkenntnisse zu Cybersicherheits-Events kann das CSOC-Team potenzielle Störungen erkennen und wenn möglich proaktiv Gegenmaßnahmen ergreifen. Außerdem lassen sich Daten direkt innerhalb der Splunk-Plattform mit dem Slice-und-Dice-Verfahren aufbereiten, sodass das Team schnellere, datengestützte Entscheidungen treffen und die Cyber-Resilienz der Expo gegen Angriffe insgesamt stärken kann.

„Intelligentes reporting, flexible Skalierbarkeit und eine umfassende Darstellung der wichtigsten Informationen, das alles sind sind entscheidende Aspekte für die Kommunikation mit unterschiedlichen Führungskräften, Operations-Teams und natürlich der Unternehmensleitung“, so Al Awadhi.

21-17410-SPLK-Expo2020DubaiMega-EventEnsuresSecurityWithSplunk-A4-102-CSTier2_DE