

# L'événement mondial Expo 2020 Dubaï assure sa sécurité avec Splunk

## Défis clefs

Organiser un événement mondial nécessite une supervision de la sécurité exhaustive et flexible, et l'Expo 2020 Dubaï avait besoin d'une solution capable de répondre aux exigences dynamiques de son environnement hétérogène et de prévenir les potentielles menaces de cybersécurité.

## Résultats clefs

La plateforme Splunk a ingéré de multiples sources de données pour renforcer la cyber-résilience de l'Expo et permettre aux équipes de superviser attentivement un grand volume d'événements et de prendre rapidement des mesures préventives.

## Secteur :

Médias et divertissement

## Solutions/

Scénarios d'utilisation : opérations IT, cybersécurité, plateforme

## Sources de données :

serveurs web, système ERP, points d'accès au réseau

## Protéger un événement d'une telle envergure n'est pas une mince affaire.

C'est la raison pour laquelle la cybersécurité est une des priorités principales pour l'Expo 2020 Dubaï depuis sa création.

La protection d'un événement d'une ampleur et d'une durée inédites constitue le défi unique de l'Expo 2020 Dubaï. Premier événement de ce type dans la région, cette exposition universelle de six mois doit accueillir plus de 190 participants ainsi que leurs pavillons sur 4,38 kilomètres carrés, en plus des pavillons thématiques de l'Expo dédiés à la durabilité, à la mobilité et à l'opportunité. L'équipe de l'Expo est chargée de sécuriser l'écosystème technologique divers, évolutif et très dynamique qui va gérer des centaines de participants et des millions de visiteurs, parmi lesquels des VIP venus du monde entier.

Pour relever ces défis, l'Expo 2020 avait besoin d'une plateforme de sécurité capable d'évoluer rapidement, de gérer la sécurité opérationnelle de centaines de sources de données et de solutions technologiques différentes, et d'être suffisamment flexible pour s'adapter à l'évolution des besoins de cybersécurité de l'événement. La plateforme Splunk s'est avérée la meilleure pour satisfaire ces exigences.

## Flexibilité d'absorption des données et évolution rapide

Selon les estimations, l'Expo 2020 Dubaï va générer chaque jour environ un téraoctet de données réparties sur un vaste environnement comptant plus de 8 000 points d'accès, plus de 100 dispositifs de sécurité et plusieurs clouds.

Étant donné l'hétérogénéité de l'environnement et le volume considérable de données, l'Expo avait besoin d'une plateforme de données à la hauteur de la tâche. « Splunk offre une technologie SIEM suffisamment flexible, efficace et performante pour gérer les exigences changeantes de l'environnement de cybersécurité de l'Expo, » affirme Eman Al Awadhi, Vice-présidente de la cybersécurité et de la résilience de l'Expo.

## Résultats chiffrés

**Plus de 100**

dispositifs de sécurité et solutions technologiques sécurisés avec Splunk

**Un**

téraoctet de données ingéré chaque jour

**Plus de 8 000**

points d'accès et plus de 1 400 serveurs sécurisés avec Splunk

Comme Splunk incorpore de façon transparente les données d'un large éventail de sources, y compris de solutions technologiques spécialement conçues pour les opérations de l'Expo, la plateforme a démontré sa capacité à gérer à la fois un volume de données élevé et un environnement exigeant en évolution constante. De plus, Splunk a permis à l'équipe d'élargir rapidement la portée de la supervision dans un délai très court.

« Grâce à la flexibilité de Splunk, nous avons pu facilement élargir le déploiement pour répondre à l'évolution des besoins de l'Expo pendant la pandémie, et notamment au report d'un an de l'événement, » explique Mme Al Awadhi.

## Empêcher toute possibilité de menaces internes

Les événements et les organisations de grande envergure font régulièrement face à un grand nombre d'incidents de sécurité, et les menaces internes ont évolué pour devenir les risques les plus graves auxquels une entreprise est exposée.

Pour protéger ses écosystèmes technologiques des menaces internes, l'Expo s'appuie sur la supervision en temps réel pour identifier tous les comportements suspects. Parce qu'elle permet de signaler et de catégoriser toute activité inhabituelle, la plateforme Splunk permet à l'équipe de l'Expo de réagir immédiatement à toute menace potentielle et de prendre les mesures de correction qui s'imposent.



Grâce à la flexibilité de Splunk, nous avons pu facilement élargir le déploiement pour répondre à l'évolution des besoins de l'Expo pendant la pandémie, et notamment au report d'un an de l'événement. »

**Eman Al Awadhi**, Vice-présidente de la cybersécurité et de la résilience, Expo 2020 Dubaï



Splunk offre une technologie SIEM suffisamment flexible, efficace et performante pour gérer les exigences changeantes de l'environnement de cybersécurité de l'Expo. »

**Eman Al Awadhi**, Vice-présidente de la cybersécurité et de la résilience, Expo 2020 Dubaï

## Des données en temps réel pour une visibilité à 360°

La position de cybersécurité de l'Expo repose sur de nombreux facteurs, englobant aussi bien des initiatives stratégiques que des tableaux de bord Splunk qui agrègent et analysent les événements en temps réel.

Grâce à des informations rapides et exhaustives sur les événements de cybersécurité, l'équipe du CSOC identifie les perturbations potentielles et applique proactivement des contre-mesures si elle le peut. De plus, la capacité à trier et à catégoriser les données directement depuis la plateforme Splunk a permis à l'équipe des opérations de cybersécurité de prendre plus rapidement des décisions axées sur les données pour renforcer la cyber-résilience globale de l'Expo.

« Des rapports intelligents, une évolutivité flexible et une représentation complète des informations les plus importantes constituent des atouts stratégiques pour communiquer avec les différents décideurs, les équipes opérationnelles et, naturellement, la direction, » explique Mme Al Awadhi.

Téléchargez Splunk gratuitement ou commencez dès maintenant un [essai gratuit du cloud](#).

Environnement physique ou en cloud, petite équipe ou grand service, il existe un modèle de déploiement Splunk adapté à vos besoins.