CASE STUDY: EXPO 2020 DUBAI

Background

One of the most anticipated World Expos of all time and the first ever to be hosted in the Middle East, Africa and South Asia (MEASA) region, Expo 2020 Dubai will host millions of visitors from across the world throughout its six-month run. With such a large number of visitors expected throughout the duration of Expo, as well as the fact that up to 130 buildings across the 4.38-square-kilometer site will be interconnected via Internet of Things (IoT), there is a cyber security risk to the event's infrastructure and operations. Therefore, all associated challenges relating to IoT security must be addressed. The digital infrastructure of Expo 2020 crosses several smart city domains and sub-domains, and a breach of IoT security and subsequent cyber-attack could pose a risk to the infrastructure and operational capacities of the event and ultimately damage its reputation.

The challenge

Expo 2020 will be one of the largest World Expos to date. More importantly, however, Expo 2020 Dubai is expected to be one of the most digitally advanced World Expos ever held[70] . IoT connectivity represents a critical component of the event's digital infrastructure, and the latest IoT technologies will be used across the entire IoT infrastructure and Expo 2020 site. Without appropriate cyber security protocols, IoT applications would be vulnerable to cyber attacks. The visibility of this physically connected infrastructure also poses a further risk given a breach could be observed by millions of visitors. A robust Security Operation Center (SOC) is critical to ensuring a seamless event and avoiding any incidents that may impact infrastructure and operations. The IoT ecosystem is particularly sensitive, emphasizing the need for enhanced data privacy and protection. The overarching goal is to safeguard the visitor experience and ensure the event serves as a proud legacy for Dubai and the UAE.

The more digitized an event becomes, the more vulnerable it is to security breaches, which presents a significant cyber security challenge. Because Expo 2020's digital agenda entails a unique and seamless digital user experience, cyber security is essential for the protection of data, instructure, and the network, as well as monitoring all operations.

The event's cyber security operations will revolve around the safety of all international participants and millions of visitors. A major threat is the risk of data leakage, which could have detrimental internal and external consequences. To counter this, Digital14 will create and maintain a solid foundation for a smart city environment and ensure a s smooth and secure digital experience. Any mega event requires cyber security of the highest possible standards due to its critical nature and the extensive cyber-attack surface presented by its digital footprint. To counter such risks, Expo 2020 requires innovative cyber security solutions, ground-breaking initiatives and ongoing services that secure new technologies and support cross-partner flexibility and functionality. On top of this, Expo 2020 aims to strike a balance between local and international best practice and regulations in data privacy and to comply with the General Data Protection Regulation (GDPR) – ensuring the safety and privacy of Expo visitors' data.

The solution

A homegrown UAE-based organization, Digital14 enjoys the reputation of a reliable and proven cyber security partner. Digital14 has a proven track record of working alongside many government entities and across critical infrastructures, delivering an integrated, holistic approach to cyber security while enabling enhanced visibility over all elements of a project.

In the context of a holistic cyber security framework, Digital14 will provide continuous application and infrastructure security monitoring, risk assessment, incident response, and digital forensics to ensure Expo 2020 will be one of the safest and most technologically secure World Expos ever held. At the core of its mandate as Expo 2020 Dubai's Official Cyber Security Provider, Digital14 will oversee the cyber security of the event's entire digital platform – as well as the applications and data it supports – to safeguard the digital experience of millions of visitors and more than 190 international participants.

Digital14 is responsible for delivering and managing a next generation Security Operations Center (SOC) for the duration of Expo 2020. This will provide increased visibility across critical areas in Information Technology, Operational Technology, and IoT. At the same time, it will support robust cyber security protocols and a resilient cyber security environment that delivers situational awareness, reduces risk and/or downtime, supports audit and compliance, prevents and controls threats, diminishes administrative overheads, and provides log forensics and reporting.

The team will detect, report, and respond to cyber security incidents throughout the organization to minimize disruption to Expo 2020. Incident priority will be determined according to the impact of the incident on Expo 2020's business and the urgency of the required response. In case of an incident, the primary concern is to restore services as quickly as possible and in compliance with service levels agreed with the business. In addition to technical considerations, the human factor is often the weakest link when it comes to cyber security. Irrespective of the technologies and controls in place, if an employee is not willing to take responsibility for cyber-secure practices, then this exposes the organization to even greater cyber security risk.

Expo 2020 selected the Cyber Smart programme from Digital14 with the aim of incorporating a thorough cyber security awareness program that will establish an intelligent, cyber-smart team capable of ensuring the data of all visitors and international participants is safe and secure. All employees and partners will undergo relevant training, which will in turn be invaluable with regard to maintaining safety and cyber security.

Expo 2020's cyber security team is organized to provide a comprehensive cyber security service covering infrastructure networks and application security, monitoring and operations, and compliance and governance. Alongside a specialized team of cyber security experts, all Expo employees will ensure operations related to the event are aligned with the highest standards of cyber security. To encourage this, Digital14 and Expo 2020 initiated an information security cyber awareness campaign 'Cy Safe'. The campaign targets different segments of Expo through a novel, interactive set of learning modules that can be easily shared with partners and staff.

Expected Outcomes

World Expos are widely regarded as catalysts of social and economic transformation that generate enduring impacts for host cities and nations. Promising to deliver a safe and secure digital experience like no other, Expo 2020 Dubai is set to create a lasting legacy for visitors, participants, and the UAE – underpinned by world-class cyber security innovations.

With the ever-growing adoption of connected devices globally, digital platforms will help shape each visitor's experience at Expo 2020 – making cyber security crucial to the success of the six-month event. Working hand-in-hand with Digital14, Expo 2020 Dubai is on track to deliver one of the most technologically secure World Expos in history.