splunk>

CASE STUDY

City of Gold Coast Gains Real-Time Visibility for the Commonwealth Games

CITY OF GOLD COAST

Executive summary

City of Gold Coast (CoGC) remains the second largest local government in Australia, based on the Gold Coast's resident population. With 3,900 staffers, CoGC provides a range of services, activities and facilities for residents and visitors including employment opportunities, events, libraries, city management, water and waste management and tourist information. After hosting the 2018 Commonwealth Games, CoGC needed to enhance its security operations and visibility across the organization. Since deploying Splunk Cloud and Splunk Enterprise Security (ES) as part of its security uplift, CoGC has seen value in the following areas:

- Real-time visibility into multiple environments
- Significant risk mitigation around a heightened threat environment through consolidated monitoring and investigation capabilities

Why Splunk

Previously, CoGC had multiple security systems running across different parts of the organization. "We lacked visibility across multiple environments, and we needed a solution that could consolidate and accommodate multiple environment types — from industrial control systems to traditional IT systems. It was important for us to be able to monitor different threat profiles and priorities across different environments on one holistic platform," says Matthew Walker, information technology security advisor, CoGC.

CoGC's deployment of Splunk Cloud and Splunk ES, part of the solution delivered by service provider Enosys, arrived on the back of a longer-term need to address cybersecurity for CoGC. The added impetus of the 2018 Commonwealth Games — an international multisport event involving athletes from the Commonwealth of Nations, an association of 71 members — and a heightened threat profile meant that there was some urgency in acquiring the capability to detect and respond to security threats.

Ensuring the safety of thousands of people is one of the key challenges faced by any host of a major sporting event, and CoGC needed to work with local, state, and federal partners to mitigate cyber risks and keep event attendees and the local community

Industry

- Public Sector

Splunk Use Cases

- Security

Challenges

- Greater visibility into security events across diverse and multiple technology environments
- Need to detect and respond to threats, particularly during the heightened threat profile during an international sporting event

Business Impact

- Achieved security outcome through efficient threat tracking and response, with no impact on operations
- Real-time visibility and actionable operational insights from multiple environments and systems, both within the organization and outside

Data Sources

- Application logs
- Key security and server infrastructure
- Operational technology and information technology network traffic
- External sources

Splunk Products

- Splunk Cloud
- Splunk Enterprise Security

safe. Major sporting events are a prime target for cybercrime due to worldwide attention and visibility, so it was vital to manage the risk of a cyberattack. Moreover, any disruption to critical infrastructure for the Games, such as power and water supply, would harm the success of the event and cause significant reputational damage to the organizers and CoGC.

In deploying Splunk solutions, CoGC established a core cybersecurity operations capability that would meet its current and future needs, beyond the Games.

Meeting Security Challenges

With its ecosystem of partners, CoGC successfully gained the optimal security outcome at the Games, without impact on operations. By navigating through multiple stakeholders, CoGC provided a complete platform that served four different environments, from the industrial systems of Gold Coast Water to traditional core IT systems.

CoGC worked closely with different asset owners and delivered a solution with Splunk that could address bespoke use cases for specific environments. The breadth of the solution capability meant that CoGC could effectively monitor different parts of the organizations with diverse needs. For example, in the industrial control systems environment, data availability and integrity would be a top priority while, in IT operations, data confidentiality would be a primary concern. The shift in priorities between the assets assisted in developing CoGC's Splunk use cases and in how it monitored the different environments.

During the Games, Splunk Cloud and ES flexibility enabled CoGC to deliver operational security visibility in real time enhancing the Gold Coast security team's contribution to joint threat intelligence with state agencies, sponsors and partners.

"Splunk allowed us to leapfrog our security service maturity. With the service now stabilized and operational cadence established, we are ready for new use cases and new data sources in other areas of the organization."

Matthew Walker, Information Technology Security Advisor
CoGC

Confidence in the future with Splunk

The success of the service, cemented by the ability offered by Splunk to monitor during the heightened threat period, has established confidence across the organization. Following the Games, the CoGC team fine-tuned and stabilized the service further. The CoGC's security committee is stronger than ever before and ready to harness the opportunities from the platform.

"Splunk allowed us to leapfrog our security service maturity. With the service now stabilized and operational cadence established, we are ready for new use cases and new data sources in other areas of the organization," says Walker.

Download Splunk for free or get started with the free cloud trial. Whether cloud, on-premises, or for large or small teams, Splunk has a deployment model that will fit your needs.

splunk> Learn more: www.splunk.com/asksales www.splunk.com

© 2018 Splunk Inc. All rights reserved. Splunk, Splunk>, Listen to Your Data, The Engine for Machine Data, Splunk Cloud, Splunk Light and SPL are trademarks and registered trademarks of Splunk Inc. in the United States and other countries. All other brand names, product names, or trademarks belong to their respective owners.