Case Study

Gold Coast 2018 Commonwealth Games Corporation

Symantec Threat Monitoring and Intelligence Integrates with Multipartner IT and Cyber Security to Protect Major International Event

Challenge

- Integrate diverse security vendors and technologies
- Identify and mitigate cyber risks prior to Games
- Defend against cyber attacks during Games
- Collaborate with state and federal agencies

Solution

- Symantec Managed Security Services
- Symantec Incident Response
- Symantec Deepsight Intelligence including:
- Managed Adversary Threat Intelligence
- Direct Threat Research

Benefits

- Effortless creation of seamless security solution
- Reduced risk of becoming a cyber victim
- Actionable threat intelligence: prediction, detection, analysis
- Ability to stay ahead of threats
- Shared intelligence across stakeholders and systems

Client Profile

Site: gc2018.com
Industry: International multisport event
Headquarters: Gold Coast, Queensland, Australia
Employees: 1,600 plus 30,000 contractors

To help create a cyber defense for the 2018 Commonwealth Games, the Gold Coast 2018 Commonwealth Games Corporation (GOLDOC) selected Symantec Cyber Security Services—offering prediction, detection, analysis, and onsite response capabilities—as a key contributor to its multipartner IT and cyber security solution. GOLDOC chose Symantec for its broad threat monitoring and threat intelligence expertise as well as its proven ability to protect major events and work with other GOLDOC security vendors and partners including Australian state and federal agencies. With cyber attacks growing more frequent, intense, and sophisticated, and often driven by motives other than financial gain, the organization was especially alert to attackers bent on disrupting the Games. Such an event could cause financial and reputational damage, and compromise GOLDOC's ability to ensure spectators and athletes had the time of their lives.

A Long-Standing, World-Class, Multisport Athletic Event

The Commonwealth Games, an international multisport event involving athletes from the Commonwealth nations—mostly former territories of the British Empire—have been held every four years since 1930 (except 1942 and 1946). The Games include many Olympic sports plus some that are not commonly played outside the Commonwealth, such as lawn bowls and netball.

The Gold Coast 2018 XXI Commonwealth Games are the largest in history: More than 6,600 athletes and team officials competing in 18 sports and seven para-sports contested across more than 250 events. It is the largest sporting event staged in Australia this decade.

Challenges of Securing a High-Profile, Quadrennial Event

The Games, like virtually all high-profile events, attract cyber attackers for two primary reasons: They present both a tempting opportunity to steal money via fraud and a large stage on which to make a statement.

"Similar to the athletes who have been training and preparing for years to perform on the world stage, our technology security team has been striving to plan, deploy, and deliver a secure Commonwealth Games on the world stage, too."

– Mathew Peterson, Head of Technology, 2018 Commonwealth Games

The fraudsters are primarily interested in financial gain. The hacktivists, however, may simply want to gain notoriety, which means their attack methods are largely unpredictable. "As bad as fraud can be, the worst-case consequence for us would be disruption to the Games," says Leon Fouche, GOLDOC group manager for technology security.

Protecting 1.5 million spectators, 1,600 employees, 30,000 contractors, and thousands of athletes, officials, and members of the media is a huge security undertaking. The operation's scale becomes even more daunting with the need to safeguard more than 6,000 computers, 400 printers, 3,000 two-way radios, and internet services and WiFi across 30 games venues and more than 400 km of recently installed fiber optic cable.

"Similar to the athletes who have been training and preparing for years to perform on the world stage, our technology security team has been striving to plan, deploy, and deliver a secure Commonwealth Games on the world stage, too," says Mathew Peterson, Head of Technology, 2018 Commonwealth Games.

Finding the Right Cyber Security Partner

As GOLDOC began planning the 2018 Games, it faced two main cyber security challenges.

First: How to stay ahead of the rapidly changing threat landscape. For this, GOLDOC needed actionable threat intelligence and 24x7 monitoring. "The strategies and techniques used by our cyber adversaries have advanced unbelievably, even just since the Summer Olympic Games in Rio, two years ago," says Peterson. "It's as if cyber attack technology progresses in dog years, with seven years of advances every year."

Second: How to integrate a diverse set of IT and security vendors, each with its own unique requirements and cyber security posture, into a seamless team. "Symantec collaboration and integration across a diverse set of technology vendors was critical for us to deliver a reliable and seamless technology experience," says Peterson.

To create the right multivendor solution for the dynamic threat landscape, GOLDOC developed a list of key requirements for its security partner.

Actionable intelligence: The partner needed to provide actionable intelligence, as well as an expert team. "Symantec offered threat monitoring, threat intelligence, and incident response services, including threat hunting, plus a dedicated threat management team, all bundled into a single service offering," says Fouche. "That gave us the cyber resilience and early visibility into emerging threats we sought."

Threat sharing: The ability to seamlessly share threat information across all vendors and partners was another key requirement. Symantec had the ability to quickly share threat intelligence through its Managed Security Services (MSS) platform to GOLDOC and its games partners.

Multiproduct integration: Because the GOLDOC security solution collected and ingested logs from various technologies and endpoints, then provided the necessary alerts, its cyber security partner needed the proven ability to work with multiple security vendors and products. Symantec technology had been previously integrated effectively with numerous heterogeneous environments.

"It was extremely valuable having Symantec's holistic, forward-looking, and ongoing managed security services."

– Leon Fouche, GOLDOC Group Manager for Technology Security

Existing key relationships: GOLDOC security providers and partners had only a few weeks to gel as a team and put forth a singular cyber defense. Symantec quickly took advantage of its prior working relationships with the other security vendors and relevant state and federal agencies.

Major event experience: GOLDOC sought a partner with recent experience providing cyber security for a major event. Symantec had previously delivered similar services to multiple sporting events with a global audience.

Says Peterson, "Symantec's experience with major sporting events, relationships with our games partners and state and federal agencies, and deep expertise and capability with threat monitoring, intelligence, and sharing, as well as incident response and risk management, put it in a great position."

Symantec Impact: Integrating with GOLDOC Partners and Security Providers

Symantec's partner and vendor relationships was important to GOLDOC. For example, the company led discussions with government stakeholders and established a threat-sharing platform based on the Symantec MSS portal.

"Symantec took ownership and, with a 'can do' attitude, made that work, rather than leaving it to us to drive and implement," says Fouche. "Symantec quickly got on top of what needed to be done and integrated those threat-sharing platforms with federal and state government. The result was excellent collaboration and threat intelligence sharing between all the teams."

Symantec's relationships with other Games' security partners—garnered in the real world, including during major events— also proved quite valuable. "Here, too, Symantec demonstrated a 'can do' attitude, reaching out to vendors, some of whom could qualify as competitors, to make sure the Symantec environment integrated into their collective product set," says Fouche.

Symantec Impact: Pre-Emptive Threat Detection

In the weeks leading up to the Games, the GOLDOC team leaned on Symantec threat intelligence capabilities, and the MSS portal, to examine suspicious reconnaissance activity. Symantec's threat hunting identified potential cyber events, which the Symantec analyst team was able to track, investigate, and analyze.

"It was extremely valuable having Symantec's holistic, forward-looking, and ongoing managed security services," says Fouche.

Symantec Impact: Analysis and Remediation

Symantec helped detect and analyze cyber threats via the Symantec MSS portal, then strategized next steps with GOLDOC security. The team triangulated on threats based on related incidents, identified attackers, and determined how to best stop or defend against potential attacks. After post-event analysis, GOLDOC briefed its stakeholders on lessons learned.

"Reliable and secure IT systems were the backbone of hosting this momentous event."

– Leon Fouche, GOLDOC Group Manager for Technology Security

During the Games, the Symantec team generated a daily security report for the Games organizing committee. "Daily threat reports supported our strategy of early visibility into potential threats, rather than reactively responding to an incident," says Fouche. "The Symantec portal gave us the ability to collaborate with our government partners and other security providers, and those reports basically put everyone in the same room."

GOLDOC noted how threat actors have tried to disrupt other major sporting events, and in response staffed its technology operations center with key emergency response personnel, including Symantec analysts, during critical times. Those times included opening and closing ceremonies as well as some of the more popular and well-followed sporting events, such as the hundred-meter sprint.

The Symantec team for the Games included:

- Security analysts to investigate cyber incidents.
- Threat intelligence analysts to provide regular and actionable intelligence on emerging threats.
- Adversary threat intelligence analysts to create reports with a global view of emerging threats and the strategies behind them.
- A single-point-of-contact service delivery manager to assist with onboarding, and provide ongoing risk assessment, analysis, and more.
- Incident response specialists to investigate, contain, and remediate major incidents.

Making it a Memorable Event for All the Right Reasons

"We focused on providing the right security, in a way that didn't hinder our athletes, sponsors, spectators, and the media," says Fouche. "Reliable and secure IT systems were the backbone of hosting this momentous event."

Put another way: The Gold Coast 2018 Commonwealth Games wouldn't be remembered for the strength of its cyber defenses. With Symantec threat intelligence, the GOLDOC security team kept it eyes on the threat landscape and, by looking ahead, stopped and remediated threats before they became security incidents.

"Our Executive Committee was concerned with two forms of risk: reputational and operational," says Peterson. "Symantec helped us manage both and avoid any disruption at the Commonwealth Games. Success for us was delivering a reliable and seamless technology service to all of our clients."

Symantec™
A Division of Broadcom

For product information and a complete list of distributors, visit our website at: broadcom.com

SED-GOLDOC-CS100 June 3, 2020