INVICTUS GAMES SYDNEY 2018

CLIENT CASE STUDY

INVICTUS GAMES SYDNEY 2018

UNISYS | Securing Your Tomorrow®

UNISYS DELIVERS AS THE OFFICIAL TECHNOLOGY AND CYBERSECURITY SUPPORTER

The Invictus Games is a global sporting competition that sees wounded, injured or ill veterans and serving personnel compete in adaptive sports including wheelchair basketball, sitting volleyball, cycling and indoor rowing.

On 20 October 2018 the Invictus Games descended upon Sydney, Australia for eight days of intense competition with almost 500 competitors representing 18 countries.

However preparation for the Games was well underway before the competitors arrived. With an immovable deadline, Unisys, as the Official Information Technology and Cybersecurity Partner of the Invictus Games Sydney 2018, had to scale quickly.

The Games presented Unisys with a unique opportunity to further its commitment to the defence community, an industry Unisys is focused on supporting the technology infrastructure of defence services around the globe as well as the employment opportunities of ex-military personnel.

The Brief

When Unisys partnered with the Invictus Games Sydney 2018, there were just seven short weeks until the Games went live.

The brief was simple but critical – secure the Games technology infrastructure, data (including highly classified data), cloud based applications and end user devices whilst providing, implementing and supporting the Games workspace and end users. A project that required specialist expertise and experience with a can do, agile mindset.

Unisys had to consider:

1. **The scope:** What had to be identified, assessed and physically set-up within the timeframe spanning cybersecurity, data security, infrastructure, end user, service desk, hardware and field support.
2. **The people:** Who was going to use the technology, and their vast range of understanding of how to use it effectively and securely.
3. **The event:** How to successfully assess, design, implement, educate, manage and monitor cybersecurity throughout the Games.

This large and high-profile global event, watched throughout the world, presented an exciting and exhilarating challenge because the majority of work was focused on forward planning and effective preparation. By the time the Invictus Games took place, the Unisys team had prepared all of the technical requirements from end user device set-up to a full IT enterprise, all of which was enveloped with a security centric program and policy for 248 Invictus Games HQ employees, 1,000 volunteers and Games officials.

The Scope: Creating a Blueprint for Success

Unisys took a people-focused approach to the project. The primary goal was to ensure the right people were part of the project. Each core area of delivery had a senior specialist to oversee the implementation. Everyone who worked on the project was an expert in their field.

To achieve this, support was drawn from Unisys teams around the world. From the UK, US to India and New Zealand, teams worked together to craft a practical and realistic plan of what was required.

For the next seven weeks a dedicated team of 60 Unisys staff members from across the globe, worked around the clock to test, trial, tweak, review, update and reengineer policies, procedures, applications, tools, software and hardware to ensure they worked within the environment of the Invictus Games.

"We effectively designed a roadmap and solution for the digital workplace of the future: users are fully mobile, accessing cloud-based applications and workspace productivity tools securely, across the open internet, using a range of devices including BYOD. In all reality we developed a template to address the challenges businesses face as the traditional secure network boundaries are pushed beyond the corporate network and out to the end user devices."

- Anthony Wilson, Invictus Games Sydney 2018
Program Director, Unisys Asia Pacific

Security: Unisys takes a 'Zero Trust' approach to security. Data security was ensured via security assessments, policy development, user awareness training, cloud access and user application security testing, end user device hardening (including device management, email and internet monitoring for malicious attacks), plus infrastructure and network security using Unisys Stealth®. With cloud-based Games applications and collaboration tools, end users were connected via an open public Wifi network at Sydney Olympic Park without the traditional network or firewall protection. Unisys Stealth software suite of identity driven microsegmentation was used to control and harden the devices making them invisible. A private network hidden within a public network.

The Unisys Zero Trust approach clearly defined and articulated the risk profile to the Games executives and from that, agreed and targeted actions executed, tracked and reported, reducing the cybersecurity risk for the Games. Unisys also worked with the Australian Cyber Security Centre (ACSC) to help monitor, investigate and report any other cyber threats. A "command centre" was formed at the Games Operations Centre. This was the single point of management escalation for all cybersecurity, SOC, third parties, applications and technology escalations, and any possible major outages.

Service Desk and Field Service Support: Availability of technology is critical leading up to and including the Games, with no time to wait. The Unisys Service Desk, located at the Games Operations Centre at Sydney Olympic Park, was the single point of contact for all end user technology requirements. Calls were immediately dispatched to Unisys field technicians located at each venue, or to third parties who were providing supporting technology and applications.

Unlike many corporate environments, where end users use technology every day, not all Games officials or volunteers would be familiar with the technology applications, tools and software needed to do their job.

End User Devices: A range of laptops, phones, monitors and printers were to be used at the Invictus Games to support operations and keep events and activities on schedule — all of which needed to be secure.

In the few weeks leading into the Opening Ceremony, Unisys was on-boarding 25 Invictus Games staff a week utilising cloud based security systems and tools to support the IT operations of the Games.

The Unisys team headed into these Games with an 'expect a little chaos' attitude and an adaptive mindset that allowed for fast, and decisive, resolutions to technical challenges as they arose.

User Education and Service Support

Unisys knew this highly mobile user behaviour had the potential to be one of the biggest security risks to operational success.

Prior to the Games, Unisys supported all types of users (such as Games management, scoring, marketing, finance, medical teams and a large pool of volunteers) via cybersecurity awareness training. This addressed areas such as phishing and password security to ensure that everyone had a base level of IT security understanding.

The Unisys team provided service desk and onsite support to address rapid onboarding issues, created new user logins, and ensured all systems were operational at all times to keep up with the volume of events with response times during the Games of five minutes or less.

By the Numbers

The Team

16	25	6	13
Core onsite team members	Service desk agents	Global teams supporting Unisys solution implementation	Unisys venue support

The Devices

195	200	81
117 Unisys-supplied Dell laptops, 64 Invictus Games-owned Lenovo laptops, 14 BYO laptops	Mobile phones (BYO), IG2018 ZTE & Motorola handsets	40 LED monitors, 41 Fuji Xerox printers

The Technology

Stealth™ software, Office 365 with Intune, anti-virus and email filtering software	Proxy servers, Azure Public Cloud, IT Service Management (ITSM)

Securing the Invictus Games

Unisys Stealth, zero trust security software built on identity-based, encrypted microsegmentation was used to divide Invictus Games' IT equipment into their own security zones, allowing Unisys to implement the required security policies to keep the equipment secure on public wireless networks.

"Data security was critical. The Invictus Games held highly sensitive data on competitors, including medical details on active and former Defence personnel from 18 countries. We were also required to comply with the new European General Data Protection Regulation (GDPR) as many nations involved in the Games hail from countries where the GDPR is applicable. This also extended to local regulations such as the Australian Data Privacy Laws as well as applicable regulations of the athletes' respective countries."

- Ashwin Pal, Director Cybersecurity, Unisys Asia Pacific

A Truly Agile Approach

Planning, preparing for and delivering the Invictus Games scope of works on an immovable deadline was time intensive, challenging and at times, emotional for the team as they came face-to-face with the spirit of the Games.

The Unisys Invictus Games Sydney 2018 project team came together to collaborate, educate, and create a comprehensive suite of IT support quickly and securely in an environment that was set up and shut down within 15 weeks.

The key to an adaptive approach at an event such as the Invictus Games, stems from the whole team understanding the broader objectives of the event. Each Unisys employee understood the primary goals, expectations for success and how their contribution would impact the outcomes of the project.

In the end, more than 248 Invictus Games employees, 1,000 Invictus Games volunteers and almost 500 competitors were supported by Unisys during the Games.

Unisys can see the difference that the Invictus Games have on rehabilitation and is proud to have been a part of an initiative that continues to heal, support, inspire and encourage wounded, injured and ill military personnel.

"Unisys came on board as our technology partner. It was extraordinary the difference they made, so very quickly. They gave us a massive acceleration to really put in place the right strategies, bring on board the right equipment, and then bring together an incredible team of people who effectively ensured that we delivered the Games in the way we did – with confidence and with the right information being moved at the right time."

- Patrick Kidd, CEO, Invictus Games Sydney 2018

Watch Unisys Invictus Games Sydney 2018 client testimonial: www.unisys.com/IG2018

For more information visit www.unisys.com