What does it take to deliver the most technologically advanced Games ever?

Enzo Sacco, Quang Tu

October 20, 2015
To share our experiences and lessons learned in securing the most technologically advanced Games ever
Quick facts: largest multi-sporting event in Canada

- 7600 Athletes
- 64 Sporting events
- 33 Venues
- 16 Municipalities
- 41 Delegations
- 23,000+ Volunteers
- 1200+ Employees
- 9 Partners
- 30 Official suppliers
- 2015 Pan Am/Parapan Am
By the numbers

- 350 million website hits / 5000 help desk tickets
- 100,000 meters of cable / 10,000 meters of new dark fiber
- 6525 radios / 3000 cell phones / 3200 email accounts
- 18000 network ports / 2500 laptops / 1571 VoIP phones
- 760 printers / 4000 reams of paper
- 575 televisions / 2000+ wifi access points
- 2 data centers / 1 Technology Operations Center
Security technologies deployed

- Firewall
- Web content filtering
- Email security
- Intrusion detection & prevention
- Identity management
- Two factor authentication
- SIEM
- Threat intelligence
- Vulnerability management
- DoS / DDoS protection
- VPN
- Endpoint protection
What are we aiming for?

Athletes competing without worry

Spectators able to enjoy the games
How is this accomplished?

Results services

Venue technology

Telecoms

Business applications

Internet technology
Challenges with achieving key technology deliverables

- Everything is temporary and will be dismantled post-competition
- Budget constraints
- Compressed timelines
- Games must start on time
Start early, design effectively

- Security design requirements
- Tactical strategies
  - Incident response and escalation
  - Vulnerability management
  - Staffing requirements
  - Contingency plans
- Continually review and assess
18 months

- Continual vulnerability management
- Continually review contingency plans
- Continual review of technologies, processes and procedures
  - Assess effectiveness & relevancy
  - Changes in environment
  - Unforeseen gaps
Expect the unexpected

- 2014 – “the year the internet fell apart”
- Everything changed overnight
- Re-prioritization
  - Patching became higher priority with management

“Here is the plan, please don’t confuse it with what is going to happen”
Be prepared

- Table top exercise
  - First time all teams came together
  - Familiarity with chain of command for games time
  - Play out case scenarios to review and assess escalation processes and procedures
Sharing threat intelligence

- Establish cyber security threat intelligence committee
  - Identify security participants
  - Establish meeting schedule
Organization official declares “Games time”

- TOC & MOC goes live
  - Technology Operation Centre
  - Management Operation Centre
Threat landscape

- High alert on any potential rumblings
  - Scan social media / news feeds
  - Protests, general dissent negativity, threats
Games are a go!
I bet you are wondering what happened...
Focus on what matters

- Data traffic volume spikes over 9000%
  - 13 GB / day to 1200 GB / day
- Pre-games: ~25 alerts / day
- Pan Am Games: ~750 alerts / day
- Parapan Am Games ~250 alerts / day
- 88 security incidents (228 total)
  - Malicious Code Attack 71%
  - Unauthorized Access / Theft 18%
  - Network Reconnaissance Probe 7%
  - Acceptable Use Policy Violation 4%
- 3 instances of Zeus activity
- 2 instances of ransomware
- 3 instances of laptops missing
- 1 instance of reported stolen identity
Closing time
Taking it forward

- Be prepared
- Executive support
- Effective execution
  - Process maturity
  - Security intelligence sharing
  - Expert staff
- Continuous validation
Parting thoughts
Thank you!

Questions?