Asian Games 2018: Cyber Security Lessons Learned

Andika Triwidada [ID-CERT]
Bisyron Wahyudi [ID-SIRTII]
Part #1 – Big Picture
National Cybersecurity Management Framework

Executive Coordinator Team

- Public Service & Utility: Protecting Cyberspace for Public Services & Utilities
- Defence: Protecting Military Cyberspace Environment
- Law Enforcement: Investigation & Prosecution of Cyber Crime
- Intelligence: Prevention and Capacity Building

Coordinator and consolidator of all relevant aspects as to cybersecurity

Relevant Elements and Units as to Cybersecurity

- NCSOC
- Sector-Specific CSIRT
- Cyber Defence
- Cyber Crime Units
- Community of Practice

Policy and Strategy Level
- Coordinating Ministry, Ministers

Tactical Level
- Cybersecurity Agency, Senior Officers, Senior Experts, Academicians

Operational Level
- Public Servants, Industry, Practitioners

1. Citizen and Children Protection
2. National Interests
3. Critical Information Infrastructures
Asian Games 2018

Turning physical event into the most connected game ever...
Equivalent to a company with 50,000 employees operating 24/7 serving millions of customers.

- The biggest multi-sport games after the Olympic Games
- The most prestigious event organized by the Olympic Council of Asia
- 40 sports
- 67 disciplines
- 462 events
Participants

The number of participants to be served by accreditation (each has different authority, access rights, facilities, etc.):

- 9,500 Athletes
- 5,500 Officials and Judge
- 2,500 VVIP and OCA
- 15,000 Volunteer
- 2,500 Journalist
Venue

All venues fully equipped with IT infrastructure

• 50 Competition Venues
• 130 Non Competition Venues:
  • Airports
  • Athlete villages and Hotels
  • Main Operation Center
  • IT Command Center
Our Program

Bringing together people, processes and technology for Cyber Security

Monitoring & Control
Network/Infrastructure Protection
Threat & Vulnerability Management
Cyber Security
Identification & Detection
Incident Management
Part #2 – Some Details
All Started in End of March, 2018

• New IT director & vice director
• No (new) budget (late for 2018)
• No project management
• No grand design & lack of documentation for existing infrastructure
• No (adequate) security
• Lack of staff
  • No network engineer; only from partners
  • No security engineer
  • No support staff
  • No help desk
Security in Place

• CDN
• DNS
• Load balancer
• WAF
• Pentest for certain service
Key Partners

• Timing & Scoring
• Application: Asian Games Information System
• Network Connectivity
• Venue Technology
• Cloud
• Endpoints & Peripherals
• (much later ...) Security
Complex System

- 40+ competition venues, 4 clusters spreads over 4 provinces
- 4000+ endpoints
- Internal backbone bandwidth potentially reach > 1 Gbps
- Closed network (initial requirement, but practically need to be exposed to Internet to serve some functions)
- First time deployment of Asian Games or similar big sporting event on cloud

- To support 45 countries, 465 events in 40 sports, 11k+ athletes, 3+ weeks, ...
  compared to 2016 Summer Olympics: 207 nations, 306 events in 28 sports, 11k+ athletes, 2+ weeks
AsianGames 2018 - Game Management System

Cloud Data Center Architecture
# Primary Data Center

<table>
<thead>
<tr>
<th>No.</th>
<th>System Name</th>
<th>Hostname</th>
<th>CPU (nCore)</th>
<th>Memory</th>
<th>Local Disk</th>
<th>SMB (CIFS, GB) / Mount Drive</th>
<th>Data Disk (for DBMS, GB) / Mount Drive</th>
<th>DBMS</th>
<th>Start of Operation</th>
<th>Finish of Operation</th>
<th>Duration (Days)</th>
<th>Expected usage per day (hour)</th>
</tr>
</thead>
<tbody>
<tr>
<td>1</td>
<td>GMS WEB Server</td>
<td>PDC-GMS-NV/NE/FW/V1</td>
<td>16</td>
<td>32GB</td>
<td>128GB</td>
<td>N/A</td>
<td>N/A</td>
<td>N/A</td>
<td>01/01/18</td>
<td>07/06/18</td>
<td>24</td>
<td>24</td>
</tr>
<tr>
<td>2</td>
<td>GMS WEB Server</td>
<td>PDC-GMS-NV/NE/FW/V2</td>
<td>16</td>
<td>32GB</td>
<td>128GB</td>
<td>N/A</td>
<td>N/A</td>
<td>N/A</td>
<td>01/01/18</td>
<td>07/06/18</td>
<td>24</td>
<td>24</td>
</tr>
<tr>
<td>3</td>
<td>GMS WAS Server</td>
<td>PDC-GMS-WA/WA-FW/V1</td>
<td>24</td>
<td>64GB</td>
<td>128GB</td>
<td>400 (N:1)</td>
<td>N/A</td>
<td>N/A</td>
<td>01/01/18</td>
<td>07/06/18</td>
<td>24</td>
<td>24</td>
</tr>
<tr>
<td>4</td>
<td>GMS WAS Server</td>
<td>PDC-GMS-WA/WA-FW/V2</td>
<td>24</td>
<td>64GB</td>
<td>128GB</td>
<td>N/A</td>
<td>N/A</td>
<td>N/A</td>
<td>01/01/18</td>
<td>07/06/18</td>
<td>24</td>
<td>24</td>
</tr>
<tr>
<td>5</td>
<td>GMS DB Server</td>
<td>PDC-GMS-FW/WV/01</td>
<td>32</td>
<td>128GB</td>
<td>128GB</td>
<td>N/A</td>
<td>600 / 8:1</td>
<td>MSSQL Primary</td>
<td>01/01/18</td>
<td>07/06/18</td>
<td>24</td>
<td>24</td>
</tr>
<tr>
<td>6</td>
<td>GMS DB Server</td>
<td>PDC-GMS-FW/WV/02</td>
<td>32</td>
<td>128GB</td>
<td>128GB</td>
<td>N/A</td>
<td>600 / 8:1</td>
<td>MSSQL Secondary</td>
<td>01/01/18</td>
<td>07/06/18</td>
<td>24</td>
<td>24</td>
</tr>
<tr>
<td>7</td>
<td>Online GMS WEB WAS Server</td>
<td>PDC-GWS-AP-WV/WV01</td>
<td>24</td>
<td>64GB</td>
<td>128GB</td>
<td>400 (N:1)</td>
<td>N/A</td>
<td>N/A</td>
<td>01/01/18</td>
<td>07/06/18</td>
<td>24</td>
<td>24</td>
</tr>
<tr>
<td>8</td>
<td>Online GMS WEB WAS Server</td>
<td>PDC-GWS-AP-WV/WV02</td>
<td>24</td>
<td>64GB</td>
<td>128GB</td>
<td>N/A</td>
<td>N/A</td>
<td>N/A</td>
<td>01/01/18</td>
<td>07/06/18</td>
<td>24</td>
<td>24</td>
</tr>
<tr>
<td>9</td>
<td>Online Volunteer Registration</td>
<td>PDC-GWS-AP-WV/WV03</td>
<td>24</td>
<td>64GB</td>
<td>128GB</td>
<td>400 (N:1)</td>
<td>N/A</td>
<td>N/A</td>
<td>01/01/18</td>
<td>07/06/18</td>
<td>24</td>
<td>24</td>
</tr>
<tr>
<td>10</td>
<td>WEB WAS Server</td>
<td>PDC-GWS-AP-WV/WV04</td>
<td>24</td>
<td>64GB</td>
<td>128GB</td>
<td>N/A</td>
<td>N/A</td>
<td>N/A</td>
<td>01/01/18</td>
<td>07/06/18</td>
<td>24</td>
<td>24</td>
</tr>
<tr>
<td>11</td>
<td>Online GMS DB Server</td>
<td>PDC-GWS-AP-WV/WV05</td>
<td>24</td>
<td>64GB</td>
<td>128GB</td>
<td>N/A</td>
<td>600 / 8:1</td>
<td>MSSQL Primary</td>
<td>01/01/18</td>
<td>07/06/18</td>
<td>24</td>
<td>24</td>
</tr>
<tr>
<td>12</td>
<td>Online GMS DB Server</td>
<td>PDC-GWS-AP-WV/WV06</td>
<td>24</td>
<td>64GB</td>
<td>128GB</td>
<td>N/A</td>
<td>600 / 8:1</td>
<td>MSSQL Secondary</td>
<td>01/01/18</td>
<td>07/06/18</td>
<td>24</td>
<td>24</td>
</tr>
<tr>
<td>13</td>
<td>IS WEB WAS Server</td>
<td>PDC-IS-AP-WV/WV01</td>
<td>24</td>
<td>64GB</td>
<td>128GB</td>
<td>N/A</td>
<td>1,000 (N:1)</td>
<td>N/A</td>
<td>01/01/18</td>
<td>07/06/18</td>
<td>24</td>
<td>24</td>
</tr>
<tr>
<td>14</td>
<td>IS WEB WAS Server</td>
<td>PDC-IS-AP-WV/WV02</td>
<td>24</td>
<td>64GB</td>
<td>128GB</td>
<td>N/A</td>
<td>N/A</td>
<td>N/A</td>
<td>01/01/18</td>
<td>07/06/18</td>
<td>24</td>
<td>24</td>
</tr>
<tr>
<td>15</td>
<td>IS WEB WAS Server</td>
<td>PDC-IS-AP-WV/WV03</td>
<td>24</td>
<td>64GB</td>
<td>128GB</td>
<td>N/A</td>
<td>N/A</td>
<td>N/A</td>
<td>01/01/18</td>
<td>07/06/18</td>
<td>24</td>
<td>24</td>
</tr>
<tr>
<td>16</td>
<td>IS WEB WAS Server</td>
<td>PDC-IS-AP-WV/WV04</td>
<td>24</td>
<td>64GB</td>
<td>128GB</td>
<td>N/A</td>
<td>N/A</td>
<td>N/A</td>
<td>01/01/18</td>
<td>07/06/18</td>
<td>24</td>
<td>24</td>
</tr>
<tr>
<td>17</td>
<td>IS WEB WAS Server</td>
<td>PDC-IS-AP-WV/WV05</td>
<td>24</td>
<td>64GB</td>
<td>128GB</td>
<td>N/A</td>
<td>N/A</td>
<td>N/A</td>
<td>01/01/18</td>
<td>07/06/18</td>
<td>24</td>
<td>24</td>
</tr>
<tr>
<td>18</td>
<td>IS WEB WAS Server</td>
<td>PDC-IS-AP-WV/WV06</td>
<td>24</td>
<td>64GB</td>
<td>128GB</td>
<td>N/A</td>
<td>N/A</td>
<td>N/A</td>
<td>01/01/18</td>
<td>07/06/18</td>
<td>24</td>
<td>24</td>
</tr>
<tr>
<td>19</td>
<td>IS WEB WAS Server</td>
<td>PDC-IS-AP-WV/WV07</td>
<td>24</td>
<td>64GB</td>
<td>128GB</td>
<td>N/A</td>
<td>N/A</td>
<td>N/A</td>
<td>01/01/18</td>
<td>07/06/18</td>
<td>24</td>
<td>24</td>
</tr>
<tr>
<td>20</td>
<td>IS WEB WAS Server</td>
<td>PDC-IS-AP-WV/WV08</td>
<td>24</td>
<td>64GB</td>
<td>128GB</td>
<td>N/A</td>
<td>N/A</td>
<td>N/A</td>
<td>01/01/18</td>
<td>07/06/18</td>
<td>24</td>
<td>24</td>
</tr>
<tr>
<td>21</td>
<td>IS WEB WAS Server</td>
<td>PDC-IS-AP-WV/WV09</td>
<td>24</td>
<td>64GB</td>
<td>128GB</td>
<td>N/A</td>
<td>N/A</td>
<td>N/A</td>
<td>01/01/18</td>
<td>07/06/18</td>
<td>24</td>
<td>24</td>
</tr>
<tr>
<td>22</td>
<td>IS WEB WAS Server</td>
<td>PDC-IS-AP-WV/WV10</td>
<td>24</td>
<td>64GB</td>
<td>128GB</td>
<td>N/A</td>
<td>N/A</td>
<td>N/A</td>
<td>01/01/18</td>
<td>07/06/18</td>
<td>24</td>
<td>24</td>
</tr>
<tr>
<td>23</td>
<td>IS WEB Server</td>
<td>PDC-IS-DB-WV/WV01</td>
<td>32</td>
<td>128GB</td>
<td>128GB</td>
<td>N/A</td>
<td>600 / 8:1</td>
<td>MSSQL Primary</td>
<td>01/01/18</td>
<td>07/06/18</td>
<td>24</td>
<td>24</td>
</tr>
<tr>
<td>24</td>
<td>IS WEB Server</td>
<td>PDC-IS-DB-WV/WV02</td>
<td>32</td>
<td>128GB</td>
<td>128GB</td>
<td>N/A</td>
<td>600 / 8:1</td>
<td>MSSQL Secondary</td>
<td>01/01/18</td>
<td>07/06/18</td>
<td>24</td>
<td>24</td>
</tr>
<tr>
<td>25</td>
<td>IS WEB Server</td>
<td>PDC-INF-AP-WV/WV01</td>
<td>24</td>
<td>64GB</td>
<td>128GB</td>
<td>N/A</td>
<td>N/A</td>
<td>N/A</td>
<td>01/01/18</td>
<td>07/06/18</td>
<td>24</td>
<td>24</td>
</tr>
<tr>
<td>26</td>
<td>IS WEB Server</td>
<td>PDC-INF-AP-WV/WV02</td>
<td>24</td>
<td>64GB</td>
<td>128GB</td>
<td>N/A</td>
<td>N/A</td>
<td>N/A</td>
<td>01/01/18</td>
<td>07/06/18</td>
<td>24</td>
<td>24</td>
</tr>
<tr>
<td>27</td>
<td>IS WEB Server</td>
<td>PDC-INF-AP-WV/WV03</td>
<td>24</td>
<td>64GB</td>
<td>128GB</td>
<td>N/A</td>
<td>N/A</td>
<td>N/A</td>
<td>01/01/18</td>
<td>07/06/18</td>
<td>24</td>
<td>24</td>
</tr>
<tr>
<td>28</td>
<td>IS WEB Server</td>
<td>PDC-INF-AP-WV/WV04</td>
<td>24</td>
<td>64GB</td>
<td>128GB</td>
<td>N/A</td>
<td>N/A</td>
<td>N/A</td>
<td>01/01/18</td>
<td>07/06/18</td>
<td>24</td>
<td>24</td>
</tr>
<tr>
<td>29</td>
<td>IS WEB Server</td>
<td>PDC-INF-AP-WV/WV05</td>
<td>24</td>
<td>64GB</td>
<td>128GB</td>
<td>N/A</td>
<td>N/A</td>
<td>N/A</td>
<td>01/01/18</td>
<td>07/06/18</td>
<td>24</td>
<td>24</td>
</tr>
<tr>
<td>30</td>
<td>IS WEB Server</td>
<td>PDC-INF-AP-WV/WV06</td>
<td>24</td>
<td>64GB</td>
<td>128GB</td>
<td>N/A</td>
<td>N/A</td>
<td>N/A</td>
<td>01/01/18</td>
<td>07/06/18</td>
<td>24</td>
<td>24</td>
</tr>
<tr>
<td>31</td>
<td>IS WEB Server</td>
<td>PDC-INF-AP-WV/WV07</td>
<td>24</td>
<td>64GB</td>
<td>128GB</td>
<td>N/A</td>
<td>400 (N:1)</td>
<td>N/A</td>
<td>01/01/18</td>
<td>07/06/18</td>
<td>24</td>
<td>24</td>
</tr>
</tbody>
</table>
18™ ASIAN GAMES
Jakarta Palembang 2018

- Accreditation Management
- Staff, Volunteer Management
- Transportation Management
- Medical Incident Tracking
- Arrival and Departure Management
- Protocol Management
- Athletes Service Management
- Security Tracking and Incident Management
- Uniform Management
- Space, Material & Logistic
- Help Desk
- Deployment Management
Impossible Requirement

• Zero downtime
• Fully redundant links
• Fully redundant servers
• Load balancing
• Checklist from IT Auditor: 30+ items
Unique Scope of Work

• Focus on AGIS
• Public web were only minimally handled by IT
  • Initially public web infrastructure were provided by IT
  • CMS were under other dept
  • Later, infrastructure were also provided by partner
  • IT only provide some realtime data to them
• Most infrastructure were not provided by IT
  • WiFi, internet, PCs
July – August 2018: Worrisome Situations

• Tight schedule
• Several important contracts were not signed yet
• Stories about Winter Games incident
  • all system down & wiped, 1 hour before opening ceremony
• Local politics
• 3 major availability losses
  • all due to accidents, not from external attacks
Start of Game, August 10\textsuperscript{th}, 2018

- Minimum new budget
- Minimum project management
- Minimum security
- Minimum staff (<20)
  - No network engineer
  - One security engineer
  - No support staff
  - Team of help desk
- IT Command Center: 60 seats, 40 large display, 24x7 operation
Tiny Core, Huge Overall Team

- ITTD Core less than 20
- Total personnel under ITTD reaches 5,000+
  - ~3,000 for network connectivity
  - ~900 for venue technology
  - ~600 IT Volunteers
  - ~300 T&S local Workforce, ~400 T&S expats
  - ~50 for cyber security
  - ~400 for endpoints & peripherals
  - ~20 for cloud
Some Security Measures were Ready

- Endpoints hardening done, but all 4000+ has same username & password 😞
- IDS in place, but only default rules
- 24x7 help desk & security monitoring team were ready
- Pentests done
- Stress test done
Some Security Measures were Ready (2)

• Link switch test done
• BCP, DRP, ERP were partially done
• Availability monitoring & alerting ready
• Venue-to-venue traffic blocked, except for several multiple-venue-sports
Initial Panic on Opening Ceremony Day

- 3 simultaneous alerts, significant volume
- Overnight learning
  - Tentative conclusions: all false alarm
Very Surprising Situation on Games Time

• Everything related to worked smoothly when needed!
Lies, Damned Lies, and Statistics :D

• Max 150k concurrent public web users
• 225+ M page views from public web
• 160+ M screen views from mobile app
• 40+ M events recorded by SIEM
• 1+ M messages processed by GMS; 8+ GB data
Anticlimatic End

• No apparent security breach
• No one interested in our system?
• or ... attacker already penetrated deep, undetected, but didn’t want to show his/her hand?
What Did We Do Correctly?

• Proper IP allocation plan
• Mapping IP range to venue
• Disseminate IP range vs venue info to availability monitoring/alerting and SIEM
• Realtime alert: network availability, service availability, performance threshold
What Did We Do Correctly? (2)

• Help desk prepared ever changing today’s focus at midnight
• Help desk proactively push vendors if any item on today’s focus was not green
• Low cost VPN appliance for quick deployment
• Good cooperation & communication
Lesson Learned

• Every vendors only concerns their own scope
  • We have to create end-to-end monitoring system
  • To quickly pinpoint which side has problem: Network or Application?

• No vendors understand the importance of performance baseline
  • We have to tell everyone, what kind of monitoring we need to see

• Veteran vendors didn’t care about security, because it has worked ok since long time ago ...
  • We have to reject insecure protocols and request them to use safer alternatives
Lesson Learned (2)

• Custom geolocation for public IPs & especially private IPs
  • Products/application with this feature will be very helpful

• Need to develop a mechanism to allow data sync but still limit trojan spread
  • For server to server and especially DC-DRC

• Use secure file sharing for dynamic data
  • IP alloc, TEAR, ...