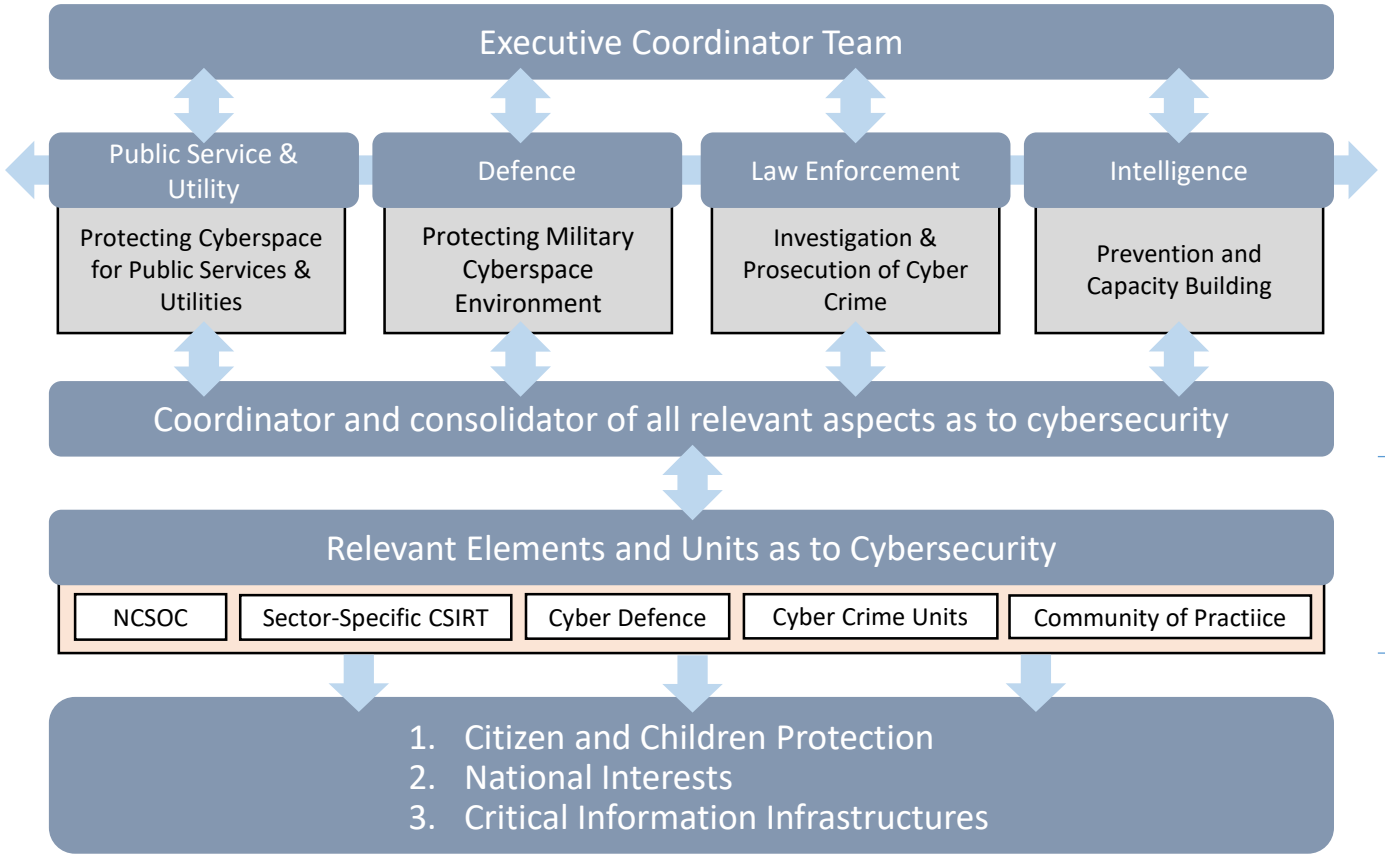
Asian Games 2018: Cyber Security Lessons Learned

Andika Triwidada [ID-CERT]
Bisyron Wahyudi [ID-SIRTII]

Part #1 – Big Picture

National Cybersecurity Management Framework

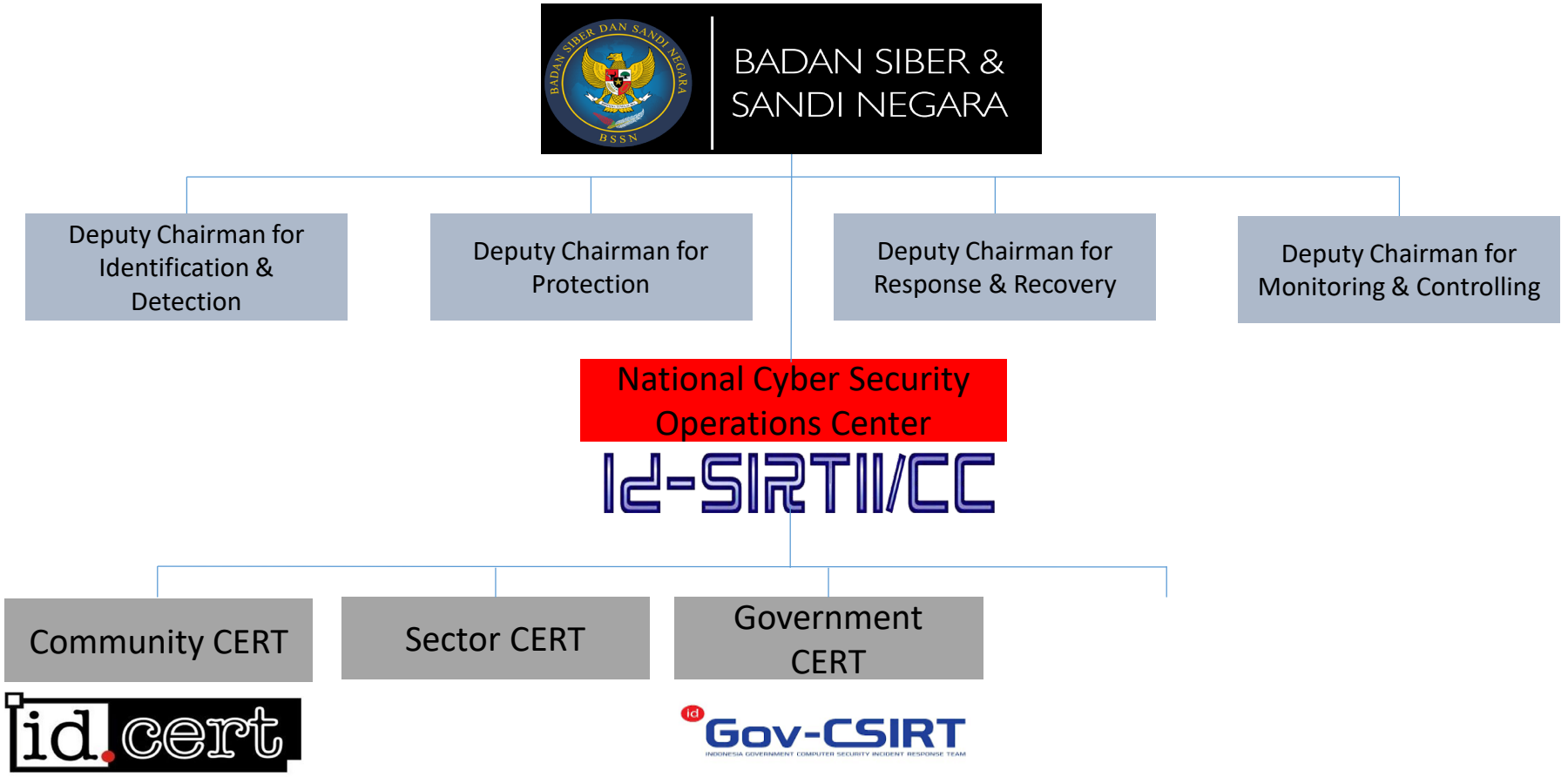


Policy and Strategy Level
Coordinating Ministry, Ministers

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

Operational Level
Public Servants, Industry, Practitioners

National Cyber Security Structure



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.):

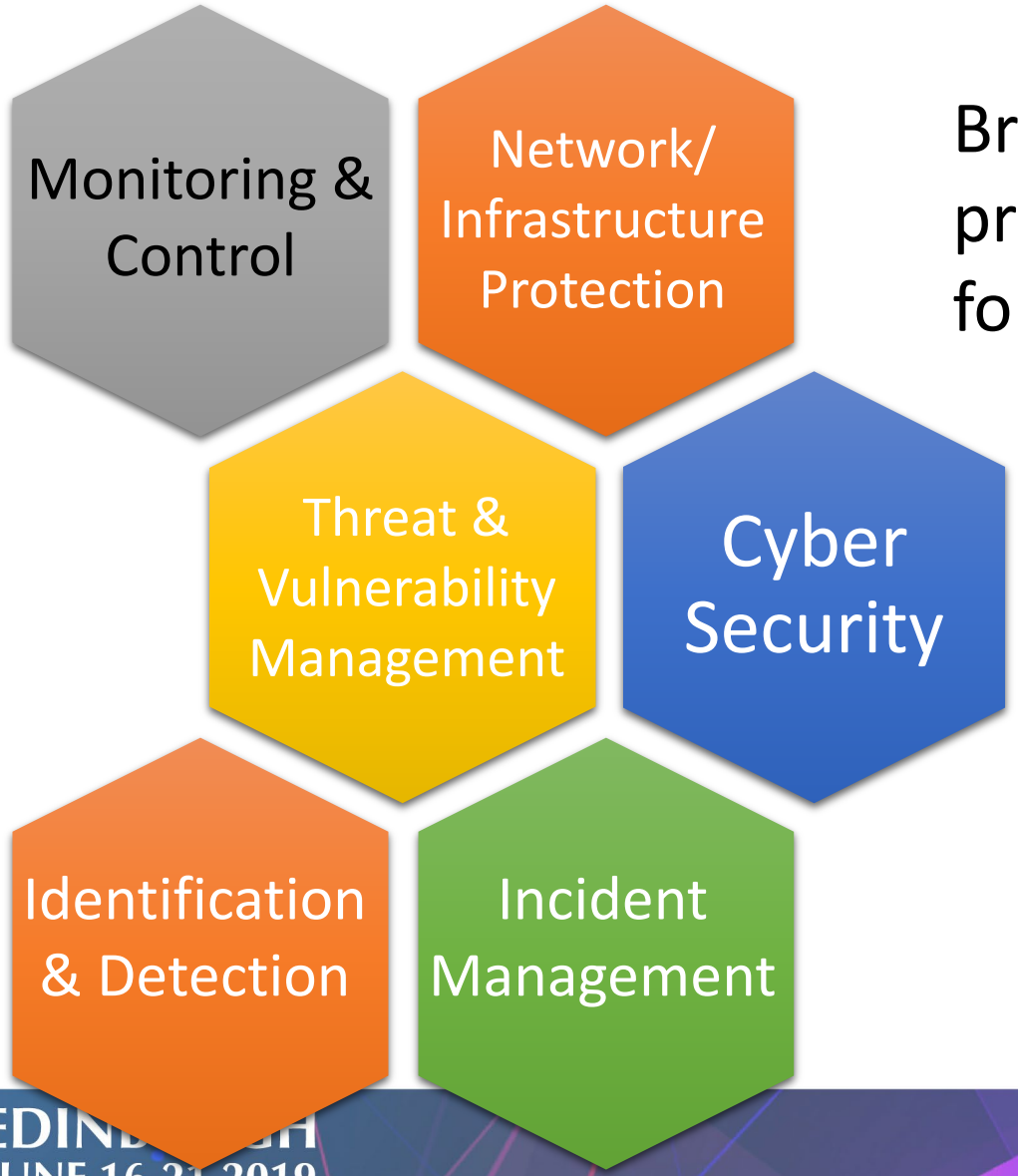
- 9.500 Athletes
- 5.500 Officials and Judge
- 2.500 VVIP and OCA
- 15.000 Volunteer
- 2.500 Journalist

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

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

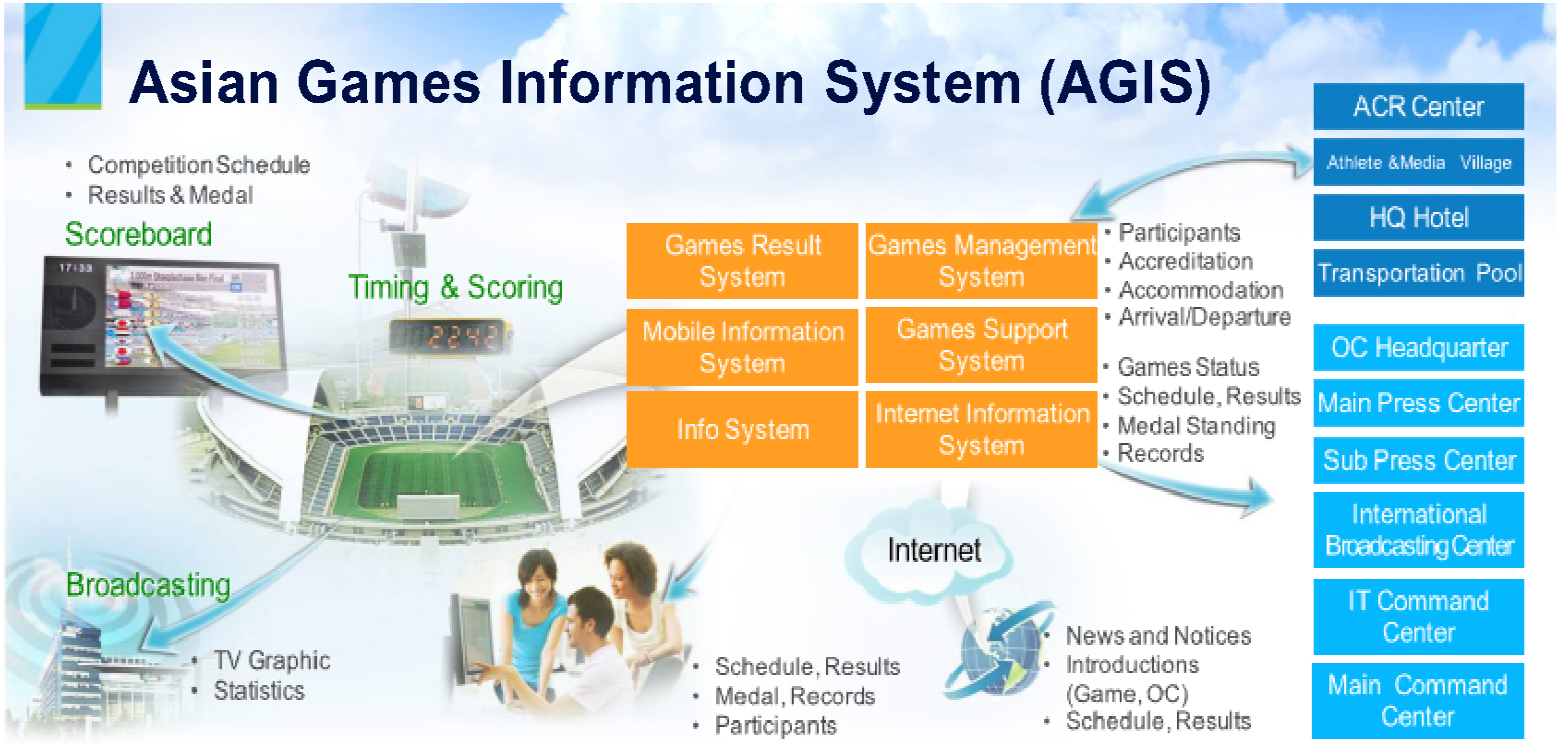
Security in Place

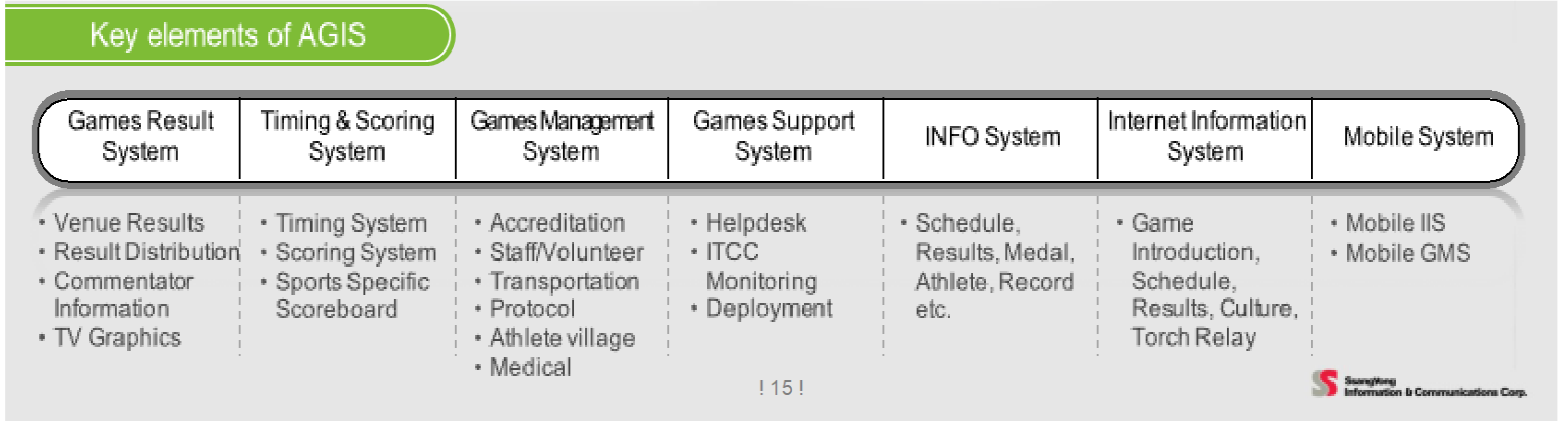
- CDN
- DNS
- Load balancer
- WAF
- Pentest for certain service

Key Partners

- Timing & Scoring
- Application: Asian Games Information System
- Network Connectivity
- Venue Technology
- Cloud
- Endpoints & Peripherals

- (much later …) Security



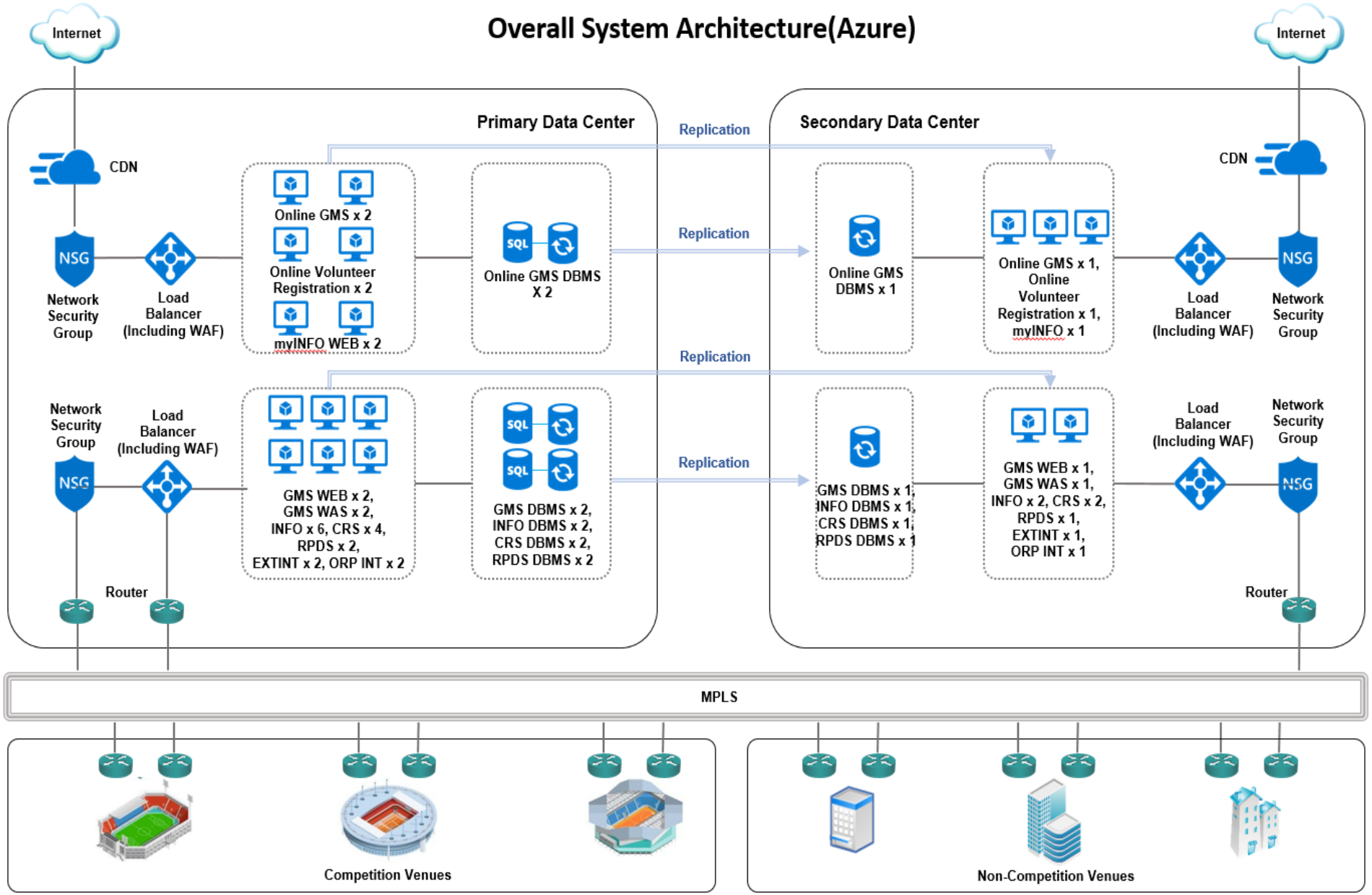


Complex System

- 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

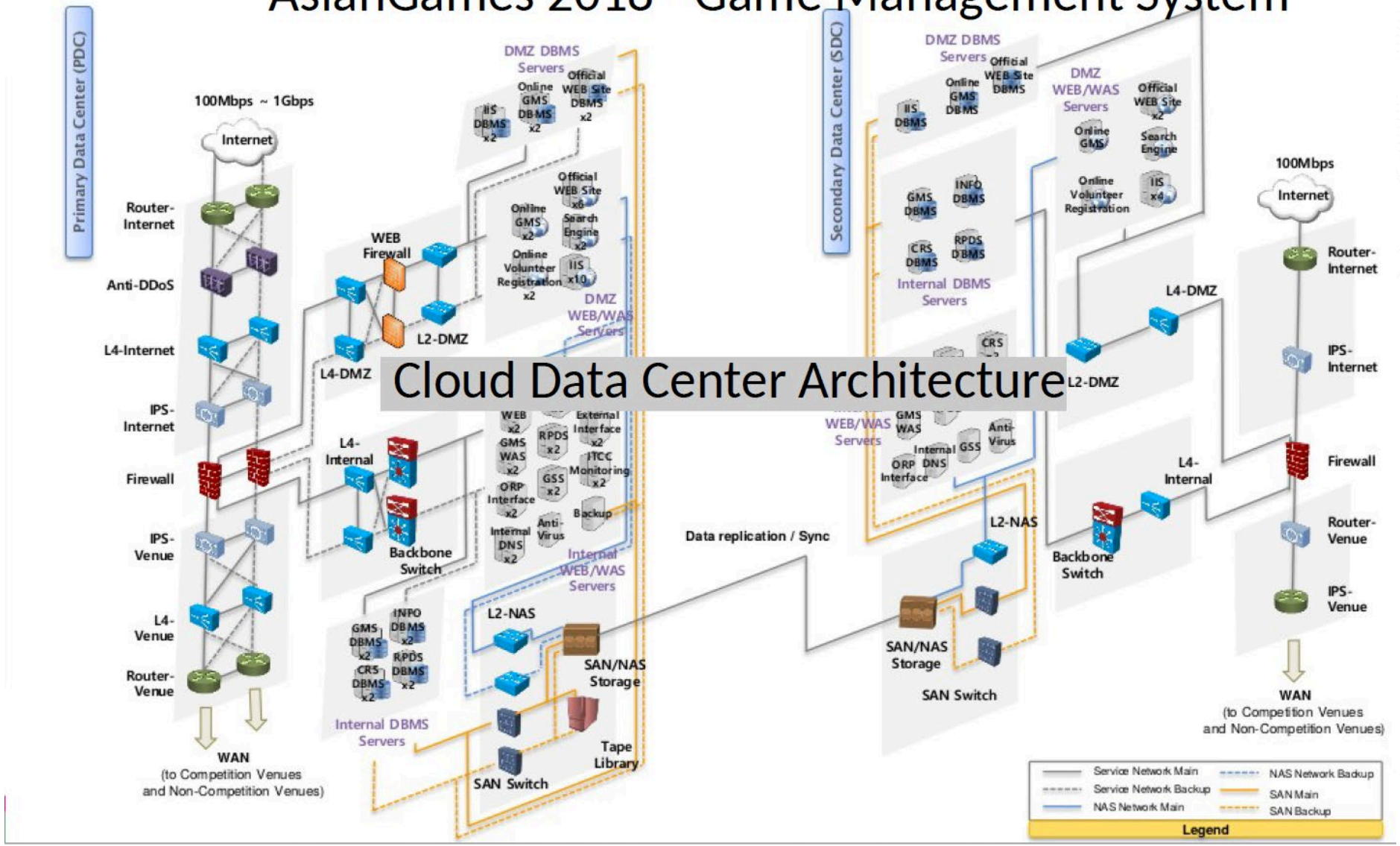
- To support 45 countries, 465 events in 40 sports, 11k+ athletes, 3+ weeks, …
  compared to 2016 Summer Olympics: 207 nations, 306 events in 28 sports, 11k+ athletes, 2+ weeks

Overall System Architecture(Azure)



AsianGames 2018 - Game Management System

Cloud Data Center Architecture



4. Production Environment - Game Time

Primary Data Center

No	System Name	Hostname	CPU (vCore)	Memory	Local Disk	SMB(CIFS, GB) / Mount Drive)	Data Disk (for DBMS, GB) / Mount Drive	DBMS	Start of Operation	Finish of Operation	Duration (Days)	Expected usage per day (hour)
1	GMS WEB Server	PDC-GMS-WE-WV01	16	32GB	128GB	N/A	N/A		01/01/18	07/09/18	249	24
2		PDC-GMS-WE-WV02	16	32GB	128GB	N/A	N/A		01/01/18	07/09/18	249	24
3	GMS WAS Server	PDC-GMS-WA-WV01	24	64GB	128GB	400 / N:\	N/A		01/01/18	07/09/18	249	24
4		PDC-GMS-WA-WV02		64GB	128GB		N/A		01/01/18	07/09/18	249	24
5	GMS DB Server	PDC-GMS-DB-WV01	32	128GB	128GB	N/A	500 / S:\	MSSQL Primary	01/01/18	07/09/18	249	24
6		PDC-GMS-DB-WV02	32	128GB	128GB	N/A	500 / S:\	MSSQL Secondary	01/01/18	07/09/18	249	24
7	Online GMS WEB/WAS Server	PDC-OGS-AP-WV01	24	64GB	128GB	400 / N:\	N/A		01/10/17	07/09/18	341	24
8		PDC-OGS-AP-WV02	24	64GB	128GB		N/A		01/10/17	07/09/18	341	24
9	Online Volunteer Registration WEB/WAS Server	PDC-EVR-AP-WV01	24	64GB	128GB	400 / N:\	N/A		01/12/17	07/09/18	280	24
10		PDC-EVR-AP-WV01	24	64GB	128GB		N/A		01/12/17	07/09/18	280	24
11	Online GMS DB Server	PDC-OGS-DB-WV01	24	64GB	128GB	N/A	500 / S:\	MSSQL Primary	01/10/17	07/09/18	341	24
12		PDC-OGS-DB-WV02	24	64GB	128GB	N/A	500 / S:\	MSSQL Secondary	01/10/17	07/09/18	341	24
13	IIS WEB/WAS Server	PDC-IIS-AP-WV01	24	64GB	128GB	1,000 / N:\	N/A		01/07/18	07/09/18	68	24
14		PDC-IIS-AP-WV02	24	64GB	128GB		N/A		01/07/18	07/09/18	68	24
15		PDC-IIS-AP-WV03	24	64GB	128GB		N/A		01/07/18	07/09/18	68	24
16		PDC-IIS-AP-WV04	24	64GB	128GB		N/A		01/07/18	07/09/18	68	24
17		PDC-IIS-AP-WV05	24	64GB	128GB		N/A		01/07/18	07/09/18	68	24
18		PDC-IIS-AP-WV06	24	64GB	128GB		N/A		01/07/18	07/09/18	68	24
19		PDC-IIS-AP-WV07	24	64GB	128GB		N/A		01/07/18	07/09/18	68	24
20		PDC-IIS-AP-WV08	24	64GB	128GB		N/A		01/07/18	07/09/18	68	24
21		PDC-IIS-AP-WV09	24	64GB	128GB		N/A		01/07/18	07/09/18	68	24
22		PDC-IIS-AP-WV10	24	64GB	128GB		N/A		01/07/18	07/09/18	68	24
23	IIS DB Server	PDC-IIS-DB-WV01	32	128GB	128GB	N/A	600 / S:\	MSSQL Primary	01/07/18	07/09/18	68	24
24		PDC-IIS-DB-WV02	32	128GB	128GB	N/A	600 / S:\	MSSQL Secondary	01/07/18	07/09/18	68	24
25	INFO WEB/WAS Server	PDC-INF-AP-WV01	24	64GB	128GB	400 / N:\	N/A		01/07/18	07/09/18	68	24
26		PDC-INF-AP-WV02	24	64GB	128GB		N/A		01/07/18	07/09/18	68	24
27		PDC-INF-AP-WV03	24	64GB	128GB		N/A		01/07/18	07/09/18	68	24
28		PDC-INF-AP-WV04	24	64GB	128GB		N/A		01/07/18	07/09/18	68	24
29		PDC-INF-AP-WV05	24	64GB	128GB		N/A		01/07/18	07/09/18	68	24
30		PDC-INF-AP-WV06	24	64GB	128GB		N/A		01/07/18	07/09/18	68	24
31	INFO DB Server	PDC-INF-DB-WV01	32	128GB	128GB	N/A	600 / S:\	MSSQL Primary	01/07/18	07/09/18	68	24


18TH ASIAN GAMES
Jakarta Palembang 2018
Accreditation Management
Staff, Volunteer Management
Transportation Management
Medical Incident Tracking
Arrival and Departure Management
VIP
Protocol Management
Athletes Service Management
Security Tracking and Incident Management
Uniform Management
24
Space, Material & Logistic
Help Desk
Deployment Management

Medal Standings

					Total
1	JPN	11	9	11	31
2	KOR	10	11	6	27
3	KAZ	8	4	9	21
4	NEP	8	4	6	18
5	THA	7	6	6	19

Latest Medallists

VANZANDT Lakesha	OMA
HAZARIKA Ela	MYA
WALMAN Tianna	MAC
Hong Kong, China	HKG
Palestine	PLE

MEDAL

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 10th, 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


Cubicle3


ENERGY OF ASIA
18th ASIAN GAMES
Jakarta
Palembang
2018
TISSOT
Grab

Tiny Core, Huge Overall Team

- ITTD Core less than 20
- Total personnels 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 treshold

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, …