29th ANNUAL FIRST CONFERENCE

SAN JUAN
PUERTO RICO
JUNE 11-16, 2017

FIGHTING PIRATES AND PRIVATEERS

WWW.FIRST.ORG

Rio 2016 CSIRT

Creation, operations and lessons learned – Rômulo Rocha

29th ANNUAL FIRST CONFERENCE
SAN JUAN PUERTO RICO

Bio

- Rômulo Rocha
- From Rio de Janeiro , Brazil
- @romrocha
- Love topics related to hunting and incident response
- Security Consultant at Tempest Security Intelligence

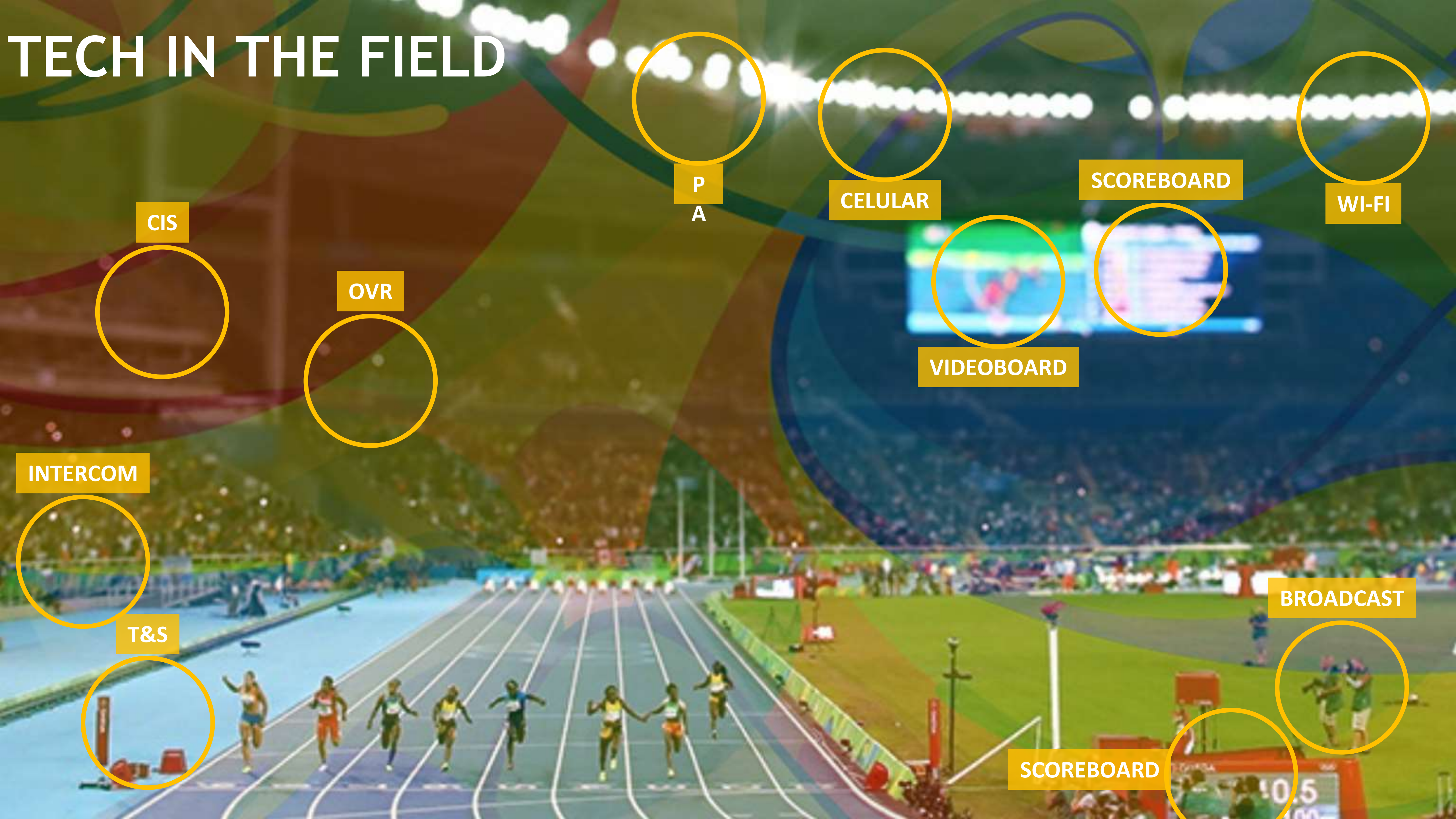
Agenda

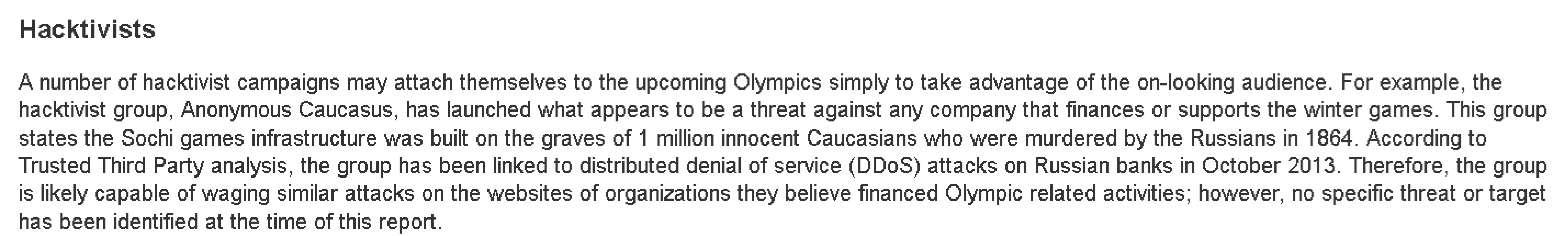
- Olympics briefing
- CSIRT (strategy, timeline, operations, channels,etc)
- Wargames
- Games Time! (*focus only on Olympic games)
- Lessons Learned

Olympics briefing

Two Events in the same city

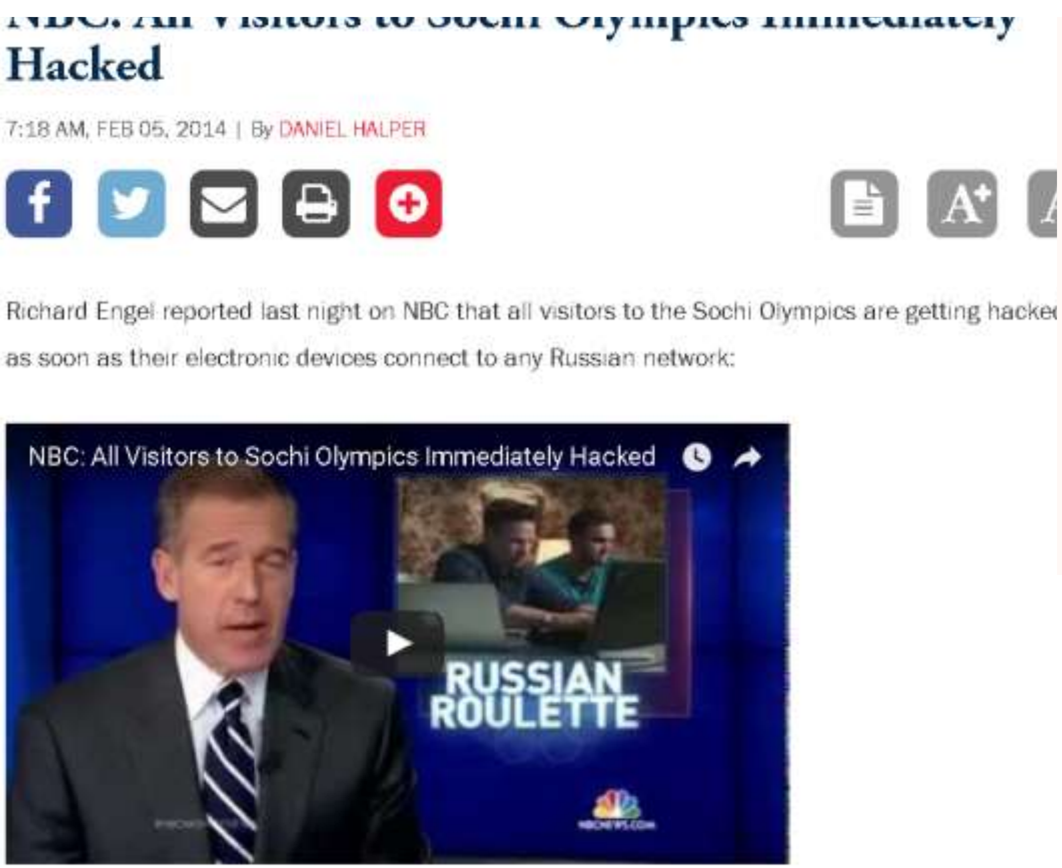
TECH IN THE FIELD





Hacktivists

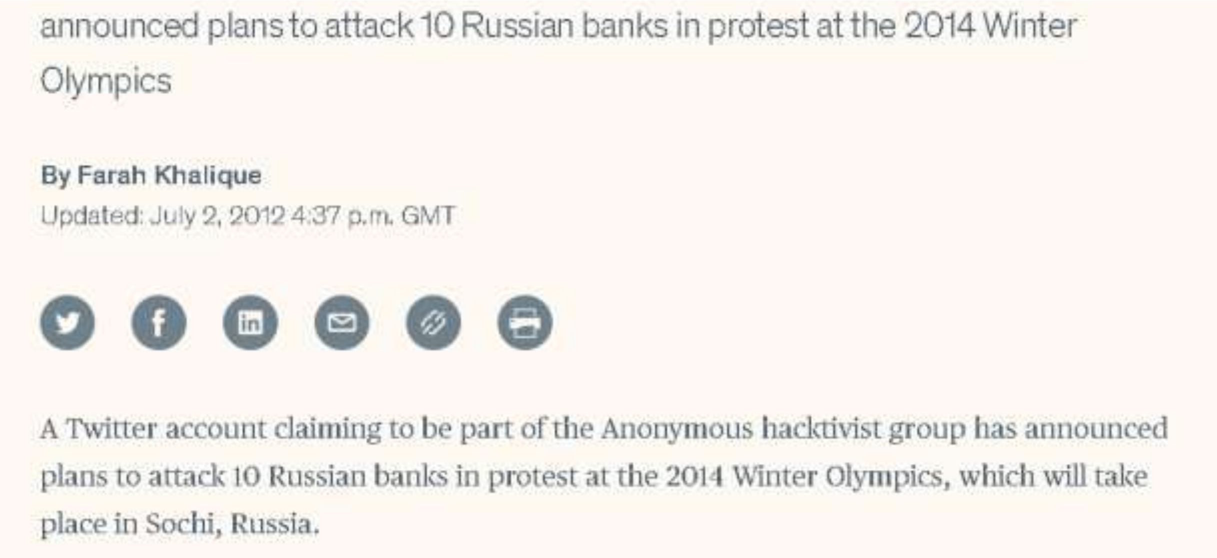
A number of hacktivist campaigns may attach themselves to the upcoming Olympics simply to take advantage of the on-looking audience. For example, the hacktivist group, Anonymous Caucasus, has launched what appears to be a threat against any company that finances or supports the winter games. This group states the Sochi games infrastructure was built on the graves of 1 million innocent Caucasians who were murdered by the Russians in 1864. According to Trusted Third Party analysis, the group has been linked to distributed denial of service (DDoS) attacks on Russian banks in October 2013. Therefore, the group is likely capable of waging similar attacks on the websites of organizations they believe financed Olympic related activities; however, no specific threat or target has been identified at the time of this report.



NBC: All Visitors to Sochi Olympics Immediately Hacked

7:18 AM, FEB 05, 2014 | By DANIEL HALPER

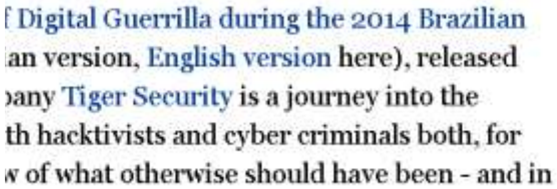
Richard Engel reported last night on NBC that all visitors to the Sochi Olympics are getting hacke as soon as their electronic devices connect to any Russian network:



announced plans to attack 10 Russian banks in protest at the 2014 Winter Olympics

By Farah Khalique
Updated: July 2, 2012 4:37 p.m. GMT

A Twitter account claiming to be part of the Anonymous hacktivist group has announced plans to attack 10 Russian banks in protest at the 2014 Winter Olympics, which will take place in Sochi, Russia.



f Digital Guerrilla during the 2014 Brazilian
an version, English version here), released
pany Tiger Security is a journey into the
th hacktivists and cyber criminals both, for
v of what otherwise should have been - and in

etc

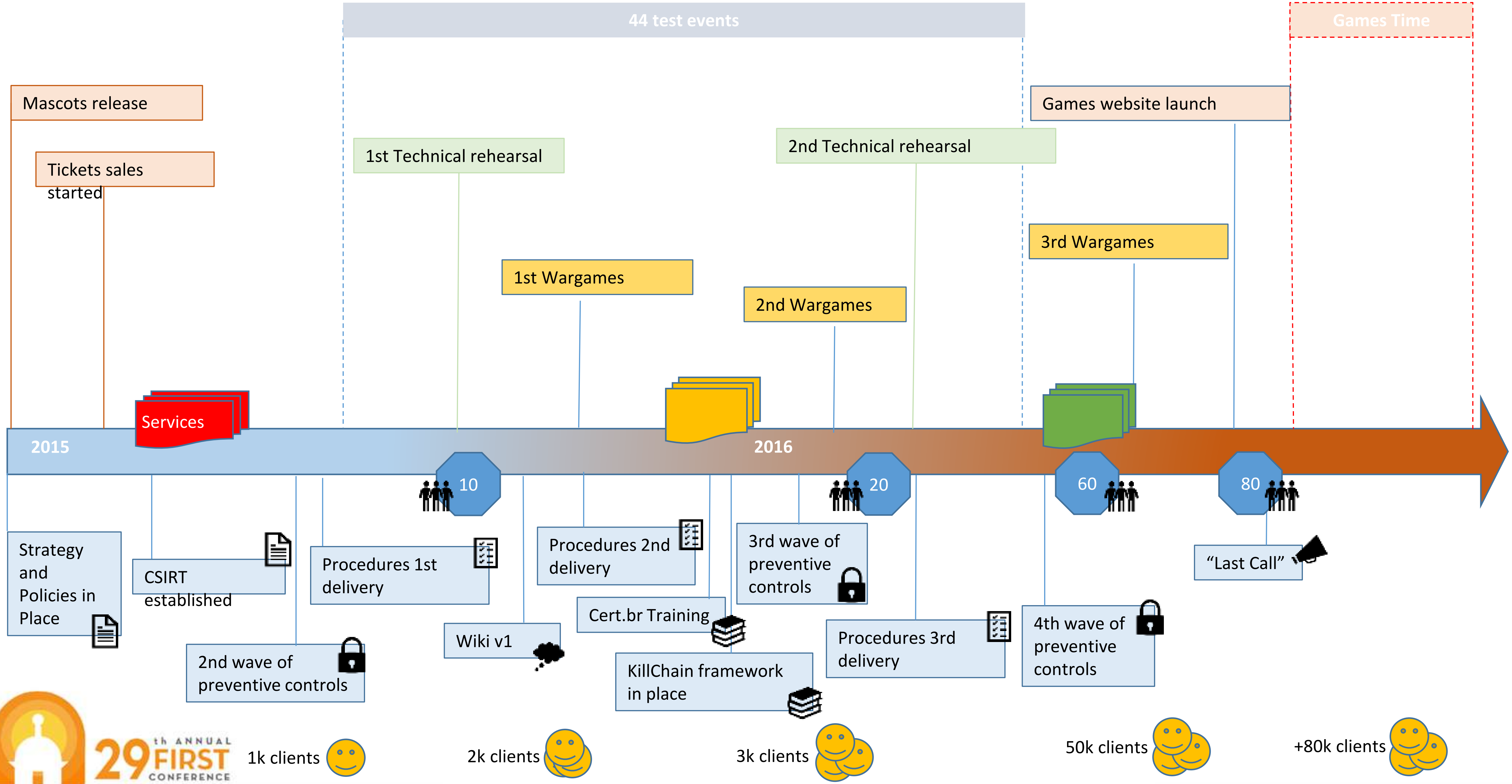
ite)

g

CSIRT

Strategy

- Necessity of a CSIRT were clear for Rio 2016 employees and C level, some threat actors were active by end of World Cup 2014 and politic clashes were erupting all around
- Defined a strategy at beginning and followed until the end, simple is better
- Well defined rules and responsibilities
- Training of employees and trust of CSIRT inside company.
- Communication is key, be announced globally and have clear/strong communication channels with local ISP, content providers, Cert.br , CDCiber (army), government agencies, sponsors and local security community.
- Trying not recreate the wheel, use what you have already.



44 test events

Games Time

Mascots release

Tickets sales started

1st Technical rehearsal

2nd Technical rehearsal

Games website launch

1st Wargames

2nd Wargames

3rd Wargames

Services

2015

2016

10

20

60

80

Strategy and Policies in Place

CSIRT established

2nd wave of preventive controls

Procedures 1st delivery

Wiki v1

Procedures 2nd delivery

Cert.br Training

KillChain framework in place

3rd wave of preventive controls

Procedures 3rd delivery

4th wave of preventive controls

“Last Call”

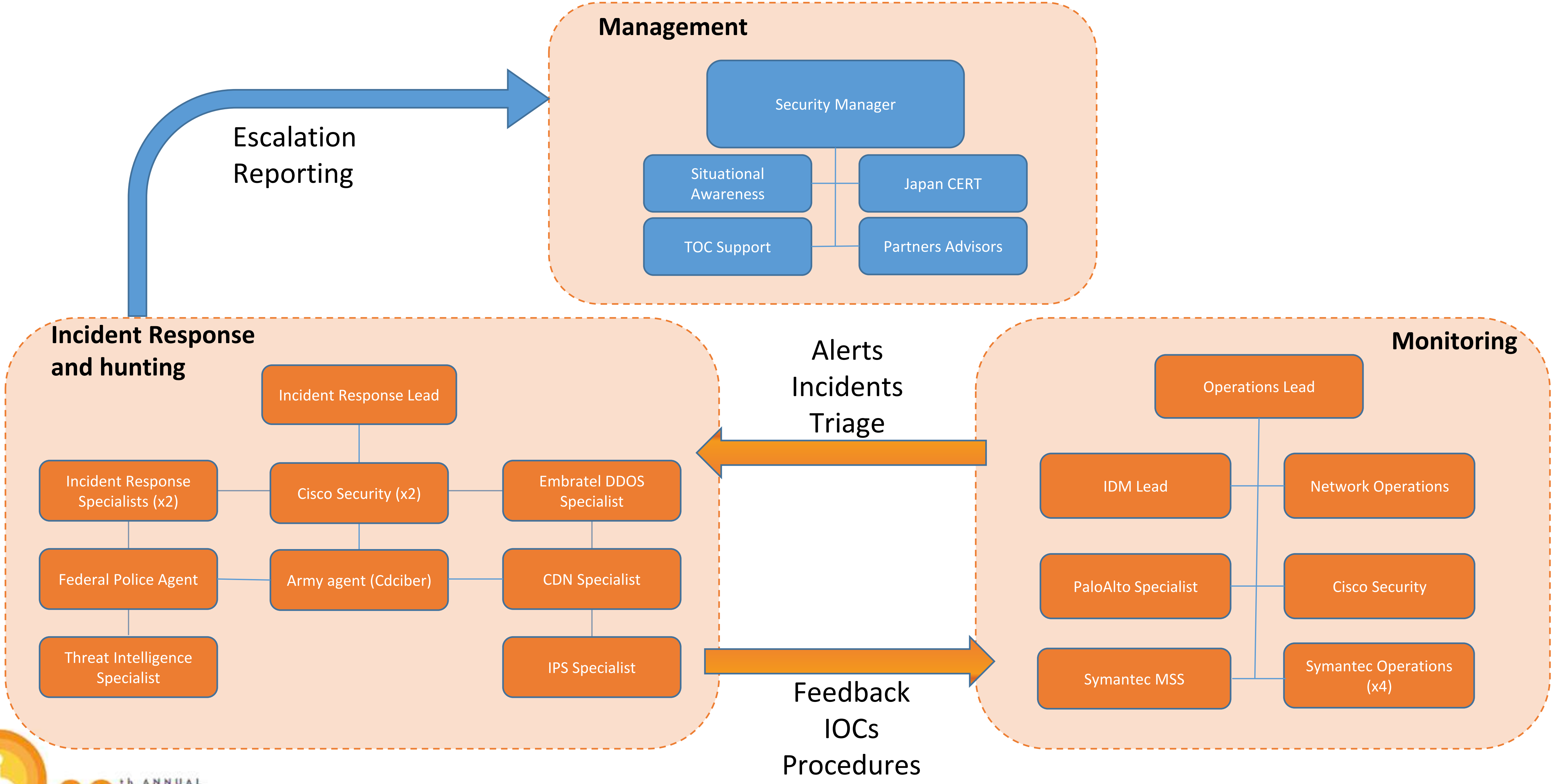
1k clients

2k clients

3k clients

50k clients

+80k clients



Escalation
Reporting

Management

Security Manager

Situational Awareness

Japan CERT

TOC Support

Partners Advisors

Incident Response and hunting

Incident Response Lead

Incident Response Specialists (x2)

Cisco Security (x2)

Embratel DDOS Specialist

Federal Police Agent

Army agent (Cdciber)

CDN Specialist

Threat Intelligence Specialist

IPS Specialist

Alerts
Incidents
Triage

Feedback
IOCs
Procedures

Monitoring

Operations Lead

IDM Lead

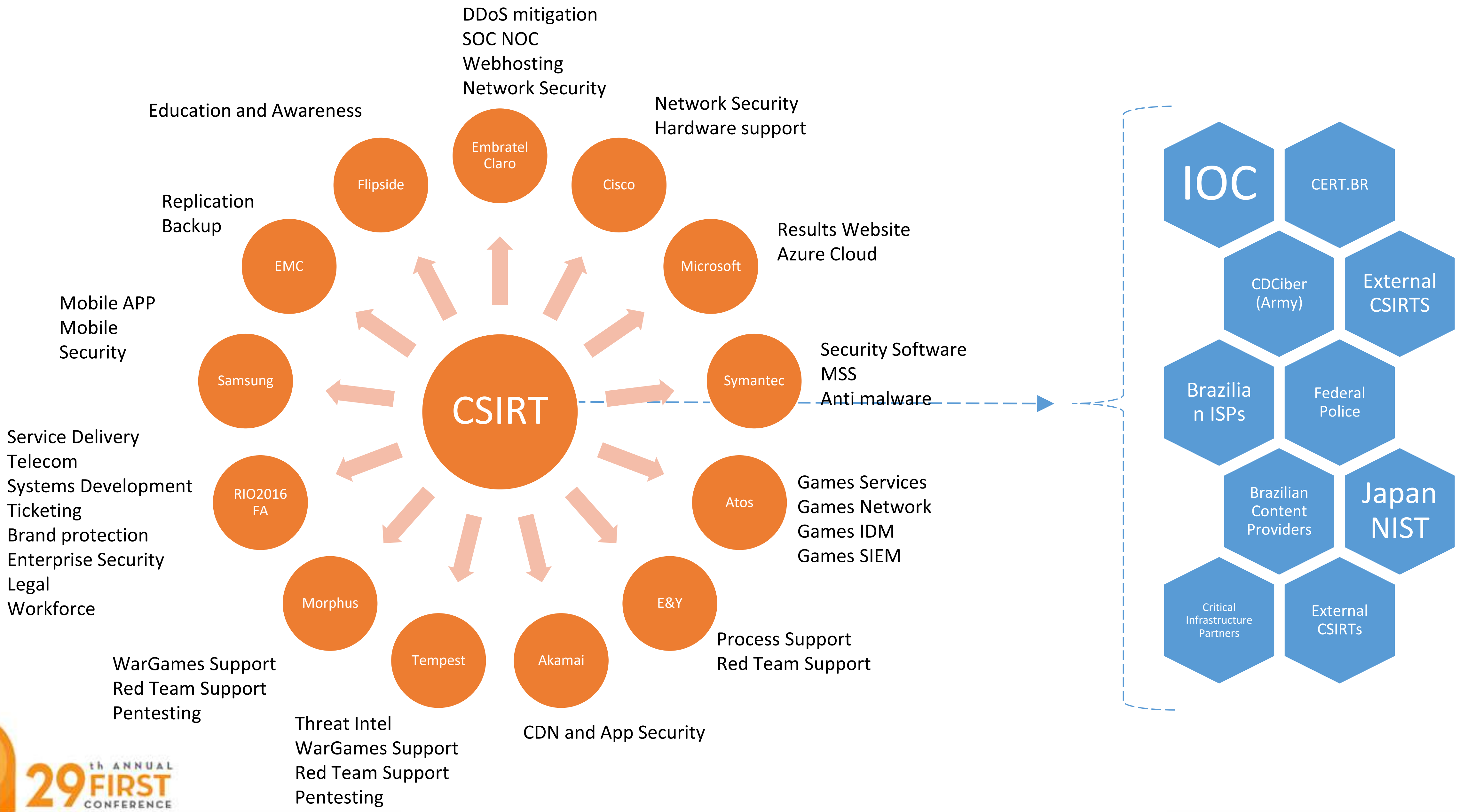
Network Operations

PaloAlto Specialist

Cisco Security

Symantec MSS

Symantec Operations (x4)



DDoS mitigation
SOC NOC
Webhosting
Network Security

Network Security
Hardware support

Results Website
Azure Cloud

Security Software
MSS
Anti malware

Games Services
Games Network
Games IDM
Games SIEM

Process Support
Red Team Support

CDN and App Security

Threat Intel
WarGames Support
Red Team Support
Pentesting

WarGames Support
Red Team Support
Pentesting

Service Delivery
Telecom
Systems Development
Ticketing
Brand protection
Enterprise Security
Legal
Workforce

Mobile APP
Mobile
Security

Replication
Backup

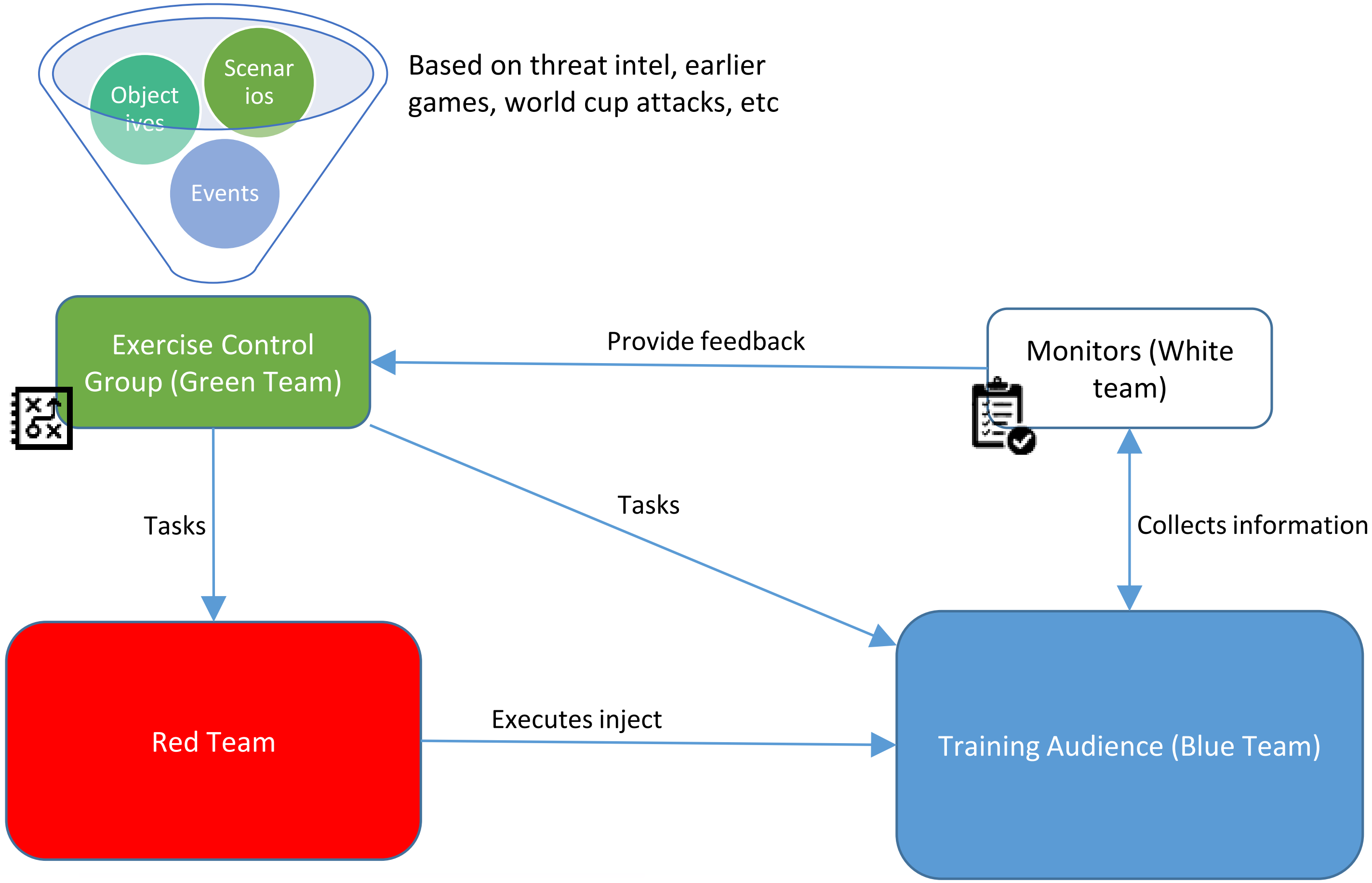
Education and Awareness

Wargames

How it worked?

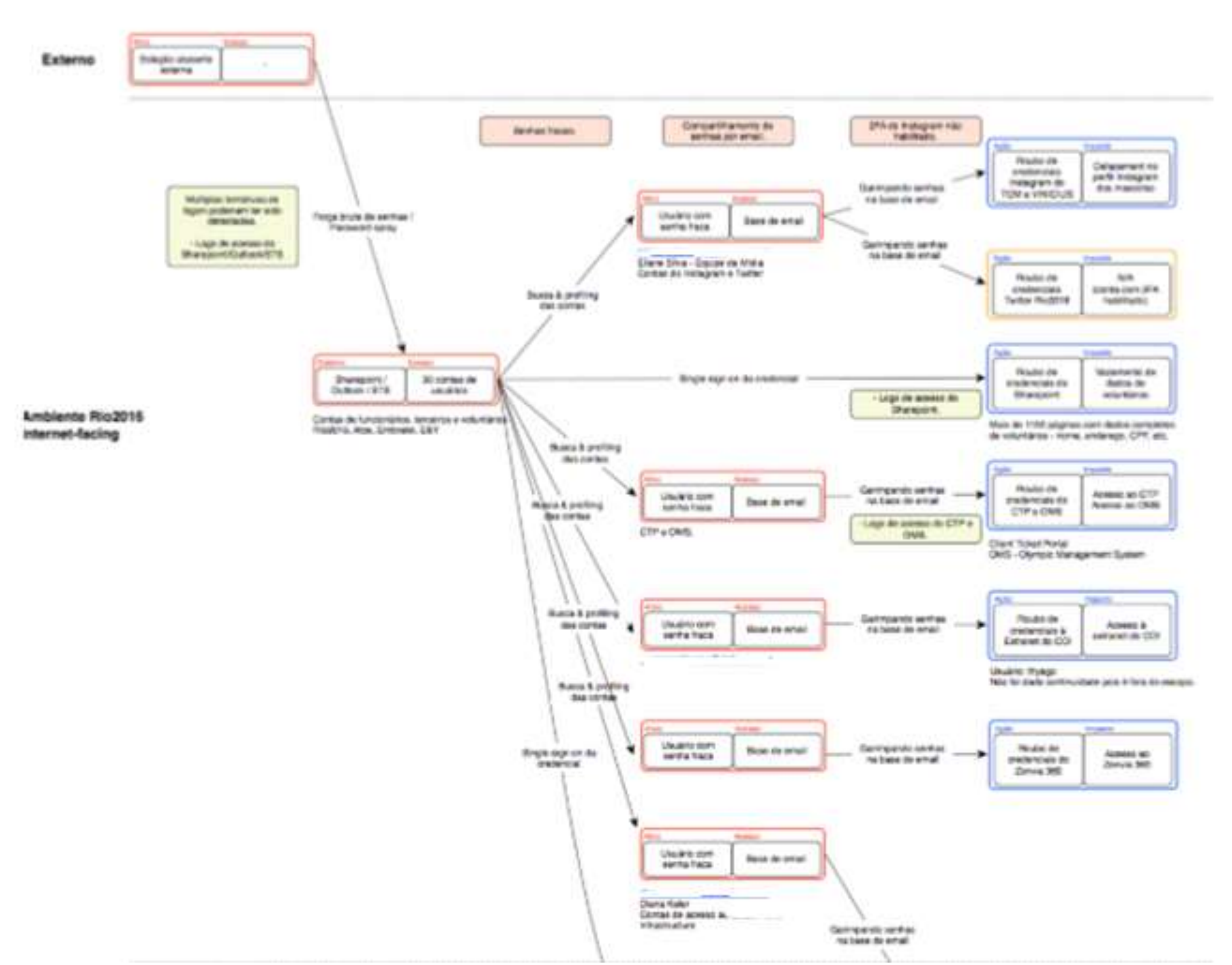
Objectives:

- Stimulates communication
- Team readiness and rehearsal
- Test effectiveness of incident response processes and procedures
- Evaluate alert triggering on tools (bonus)
- Assess exposure of the corporate network to attack vectors (bonus)
- Based on common practices (Mitre, Nato, Enisa, Poland Cyber, etc)


Objectives
Scenarios
Events
Based on threat intel, earlier games, world cup attacks, etc
Exercise Control Group (Green Team)
Provide feedback
Monitors (White team)
Tasks
Tasks
Collects information
Red Team
Executes inject
Training Audience (Blue Team)

Our W

- Three ti
- Full live
- To achie d no contact and wor
- None of
- Scenaric cted previous
- Number
- After ea improve our capabili


Externo
Senhas fracas
Compartilhamento de senhas por email
2FA do Instagram não habilitado
Força bruta de senhas / Password spray
Busca & profiling das contas
Usuário com senha fraca
Base de email
Garimpando senhas na base de email
Ambiente Rio2016 internet-facing
Sharepoint / Outlook / ETS
30 contas de usuários
Single sign on de credencial
Logs de acesso do Sharepoint
CTP e OMS

WG1 briefing

- 28th Sep – 2nd Oct , 2015
- Scope: Corporate Network (some interfaces with Games Network as well)
- Over 20 people
- 16 Scenarios

Red team briefing	
Intentions:	Abuse the brand and public image of games to spread politically motivated message.
Capabilities:	Not cutting-edge attacks, 0days , attacks like SQLi, XSS, Spear Phishing, Password attacks, Wifi, Common-grade malwares, Windows Attacks (passhash, lateral movement, AD compromise,etc)
Goals:	• Compromise and alter Rio 2016 websites • Compromise Rio 2016 social media presence • Access and leak confidential documents • Access and leak volunteers information • Access and leak financial information

WG1 in a nutshell

Red Team	Blue Team
Used a lot smoke screen attacks to distract Blue Team	Detected and blocked all smoke screen attacks
Send spear phishing attacks to important accounts based on social media gatherings	Detected and contained a spear phishing attack but did not investigated source of attack
Got administrative control over domain	Triage was not effective
Got administrative control over switches and Wifi	Tools getting alarms, but lacking correlation and automatization
Lateral movement and persistence on network	Lack of procedures
Completed all scenarios, including taking accounts of mascots in twitter	Preventive controls and fine adjustment on tools still needed
Unleashed #op_olympic_chaos in the last day	

WG2 briefing

- Feb 22 Nd – Feb 26th – 2016
- Repeated the first, to validate improvements
- CSIRT more structured and with processes
- Over 40 people
- 16 Scenarios

Red team briefing	
Intentions:	Abuse the brand and public image of games to spread politically motivated message.
Capabilities:	Not cutting-edge attacks, 0days , attacks like SQLi, XSS, Spear Phishing, Password attacks, Wifi, Common-grade malwares, Windows Attacks (passhash, lateral movement, AD compromise,etc)
Goals:	• Compromise and alter Rio 2016 websites • Compromise Rio 2016 social media presence • Access and leak confidential documents • Access and leak volunteers information • Access and leak financial information

WG2 in a nutshell

Red Team	Blue Team
Used a lot smoke screen attacks to distract Blue Team in critical moments	Majority of smoke screen attacks didn't take time to contain, but drained team resources
Send spear phishing attacks to important accounts	Successfully detected and contained the majority of the high-impact attacks performed by the red team
Got credentials to CSIRT back office system using spear phishing against one team member	Communication was way better but still lacking procedures and investigations in depth, should take more intel from attacks
Got credentials mining emails	Tools getting alarms and some automatization
Got Rio 2016 Facebook credentials	Triage was better
Created a spear phishing hosted in one of our websites	More preventive tools in place (endpoint hardening, network monitoring,etc)
In the end, received gold ticket to create a hard scenario for blue team	Better SIEM adjustments and triggering, correlation stills weak

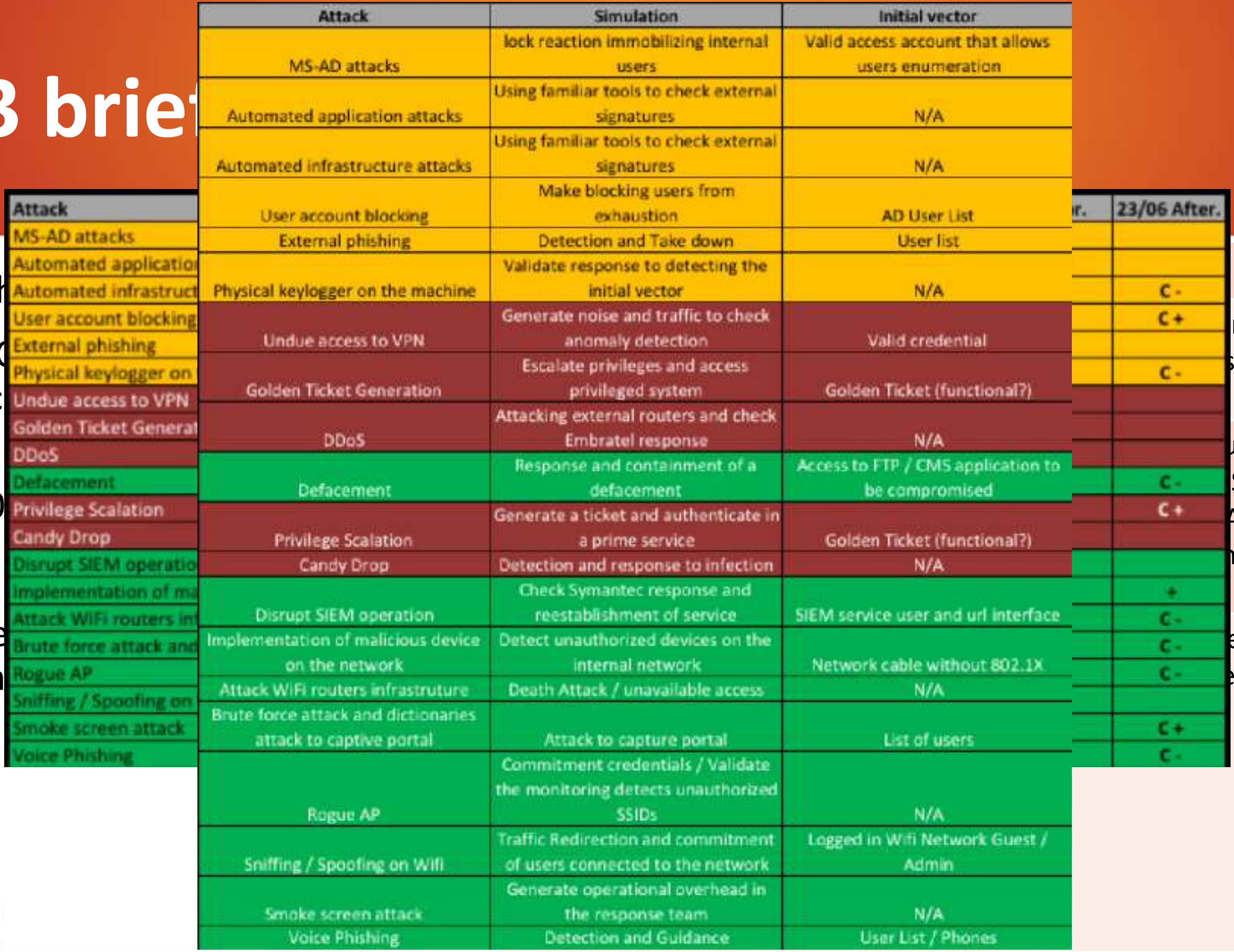
WG3 brie

- Jun 20th
- Scope: (
  interfac
  well)
- Over 70
- 3 Shifts
- Same te
  includin
- 34 Scen

niques as attackers, which
, fraudsters and bankers.

uteForce, Evil Twind,
S, Spear Phishing, Social
Attacks, Windows
nformation Leakage, etc

eam response to some
enarios. (table below)



Attack	Simulation	Initial vector
MS-AD attacks	lock reaction immobilizing internal users	Valid access account that allows users enumeration
Automated application attacks	Using familiar tools to check external signatures	N/A
Automated infrastructure attacks	Using familiar tools to check external signatures	N/A
User account blocking	Make blocking users from exhaustion	AD User List
External phishing	Detection and Take down	User list
Physical keylogger on the machine	Validate response to detecting the initial vector	N/A
Undue access to VPN	Generate noise and traffic to check anomaly detection	Valid credential
Golden Ticket Generation	Escalate privileges and access privileged system	Golden Ticket (functional?)
DDoS	Attacking external routers and check Embratel response	N/A
Defacement	Response and containment of a defacement	Access to FTP / CMS application to be compromised
Privilege Scalation	Generate a ticket and authenticate in a prime service	Golden Ticket (functional?)
Candy Drop	Detection and response to infection	N/A
Disrupt SIEM operation	Check Symantec response and reestablishment of service	SIEM service user and url interface
Implementation of malicious device on the network	Detect unauthorized devices on the internal network	Network cable without 802.1X
Attack WiFi routers infrastruture	Death Attack / unavailable access	N/A
Brute force attack and dictionaries attack to captive portal	Attack to capture portal	List of users
Rogue AP	Commitment credentials / Validate the monitoring detects unauthorized SSIDs	N/A
Sniffing / Spoofing on Wifi	Traffic Redirection and commitment of users connected to the network	Logged in Wifi Network Guest / Admin
Smoke screen attack	Generate operational overhead in the response team	N/A
Voice Phishing	Detection and Guidance	User List / Phones

Attack	r.	23/06 After.
MS-AD attacks		
Automated applicatio		
Automated infrastruct		C -
User account blocking		C +
External phishing		
Physical keylogger on		C -
Undue access to VPN		
Golden Ticket Generat		
DDoS		
Defacement		C -
Privilege Scalation		C +
Candy Drop		
Disrupt SIEM operatio		
Implementation of ma		+
Attack WiFi routers inf		C -
Brute force attack and		C -
Rogue AP		C -
Sniffing / Spoofing on		
Smoke screen attack		C +
Voice Phishing		C -

WG3 in a nutshell

Red Team	Blue Team
Used a lot smoke screen attacks to distract Blue Team	Still needs automatization for some types of attacks
Still getting network credentials in ticket systems	Ticket system was too slow for incident response
Spear phishing specially crafted to administrators in third party companies	Contained majority of attacks
Disruption of SIEM tool	Triage working better
Bypassed 802.1x auth and implanted Rogue AP in new networks	Still lacking some procedures for incident response

Marks between Wargames

CWG1

Sep 28th – Oct 2nd 2015

+20 people

- Rules and responsibilities diffused, team without instructions
- Lot of failures in tools configurations and infrastructure not mature.
- Privileged local accounts on border
- Domain admins without necessity
- Critical accounts without proper security (2fa)
- Lateral movement easily
- Network segmentation immature
- Triage inefficient, low severity incidents consuming analysts time
- Lack of integration with important areas like communication and social media

CWG2

Feb 22nd – 26th 2016

+40 people

- Better infrastructure and monitoring
- Critical accounts monitored
- Triage and incident classification
- Cyber Kill Chain and TTP idea adopted by the team
- Improvement on documentation and processes
- Better network segmentation
- Endpoint hardening improvements
- Better CSIRT notifications (templates and automatization)
- Post-Mortem still bad
- IOCs monitoring and sharing being used, but in not all cases
- Better integration with service desk and field services

CWG3

Jun 20th – 24th 2016

+70 people

- Rules and responsibilities well defined and understood by team
- Incident response process documented
- 802.1x auth in the network
- Better network segmentation (avoiding network lateral movement)
- Endpoint hardened
- Better intel extraction after incidents
- Utilization of IOCs
- Windows accounts sanitization and control in place

Lessons learned from Wargames

- Training your team under high pressure is essential, you will be surprised
- Rules and responsibilities must be aligned and understood by everyone
- Communication between teams and shifts are key, incident analysis should flow no matter who is in the charge
- Yes, still have to tune that tool =D
- Briefing before critical moments is valuable
- Your backoffice tool, should be more secure than anything. (and have backup)
- Use a back office tools, that gives speed, security and an excellent flow for incident and investigation procedures
- The importance to understand TTPs of adversaries is key for training and proper incident response methods, intel have to been extracted from attacks
- People still sharing passwords through email, 2fa is a must
- When triage does not work well, nothing works well
- Review every admin account that used in our domain, specially if they are running as a service, avoid that with your heart (MS LAPS can help too)
- User education is a relief during a scenario of attacks, they helped a lot in spear phishing attacks detection

Photos

Games time!

(*focus only on Olympic games)

OLIMPIC GAMES

11.303 athletes

207 delegations

205 Countries
+Team of Refugees
+Independent athletes

974 Medals

Tickets

+6.1 millions tickets
(London 2012: 8.8 millions)

701 sport sessions

GAMES VISIBILITY

+4,5 BI SPECTATORS

+350,000
HOURS OF TRANSMISSIONS
(London 2012: 200,000)

+500 CHANNELS

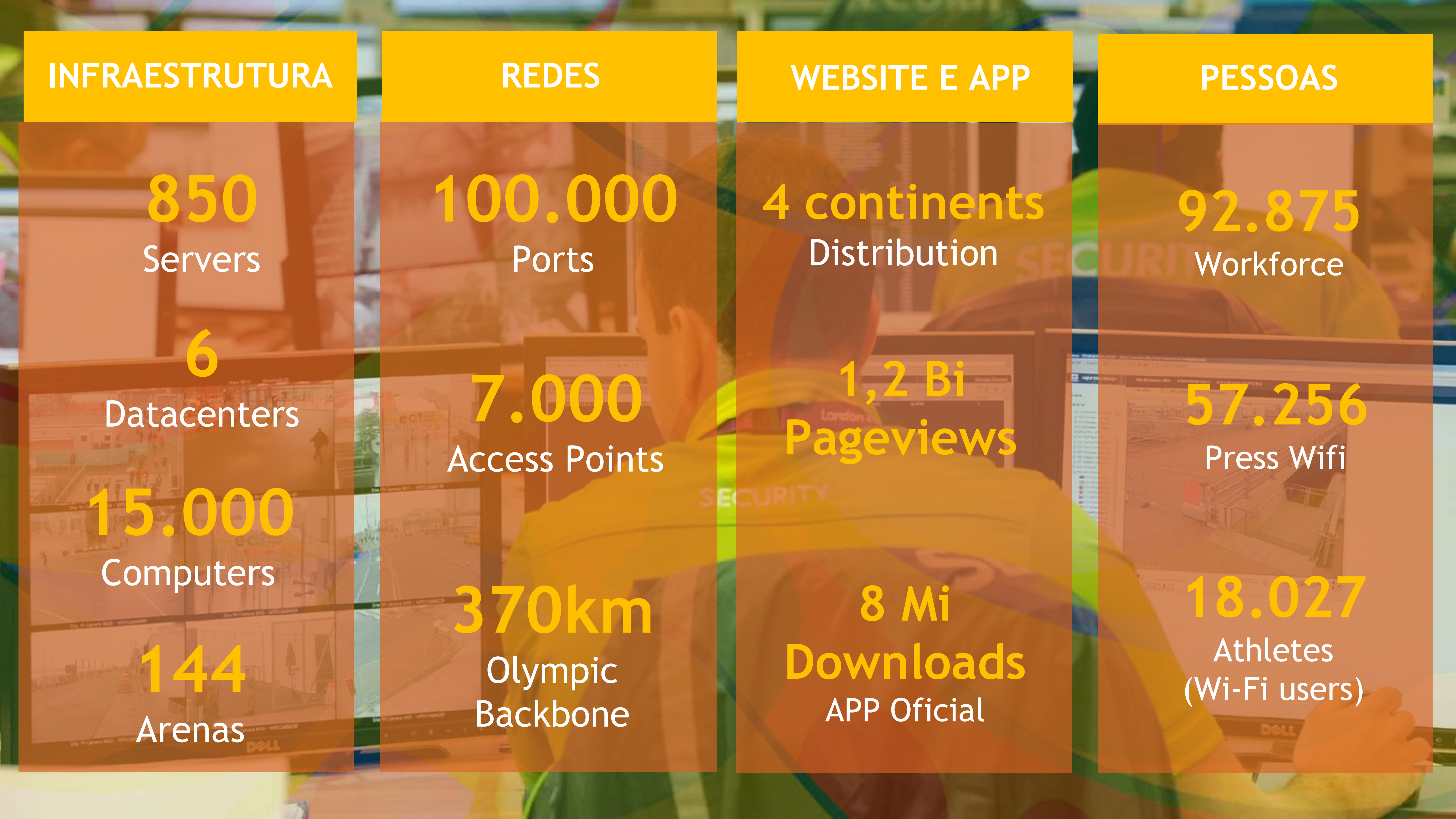
+250 DIGITAL PLATFORMS

PEOPLE

7,262
IT & TELECOM professionals

5,509
Partners and contractors

1,341
Volunteers



INFRAESTRUTURA

850
Servers

6
Datacenters

15.000
Computers

144
Arenas

REDES

100.000
Ports

7.000
Access Points

370km
Olympic
Backbone

WEBSITE E APP

4 continents
Distribution

1,2 Bi
Pageviews

8 Mi
Downloads
APP Oficial

PESSOAS

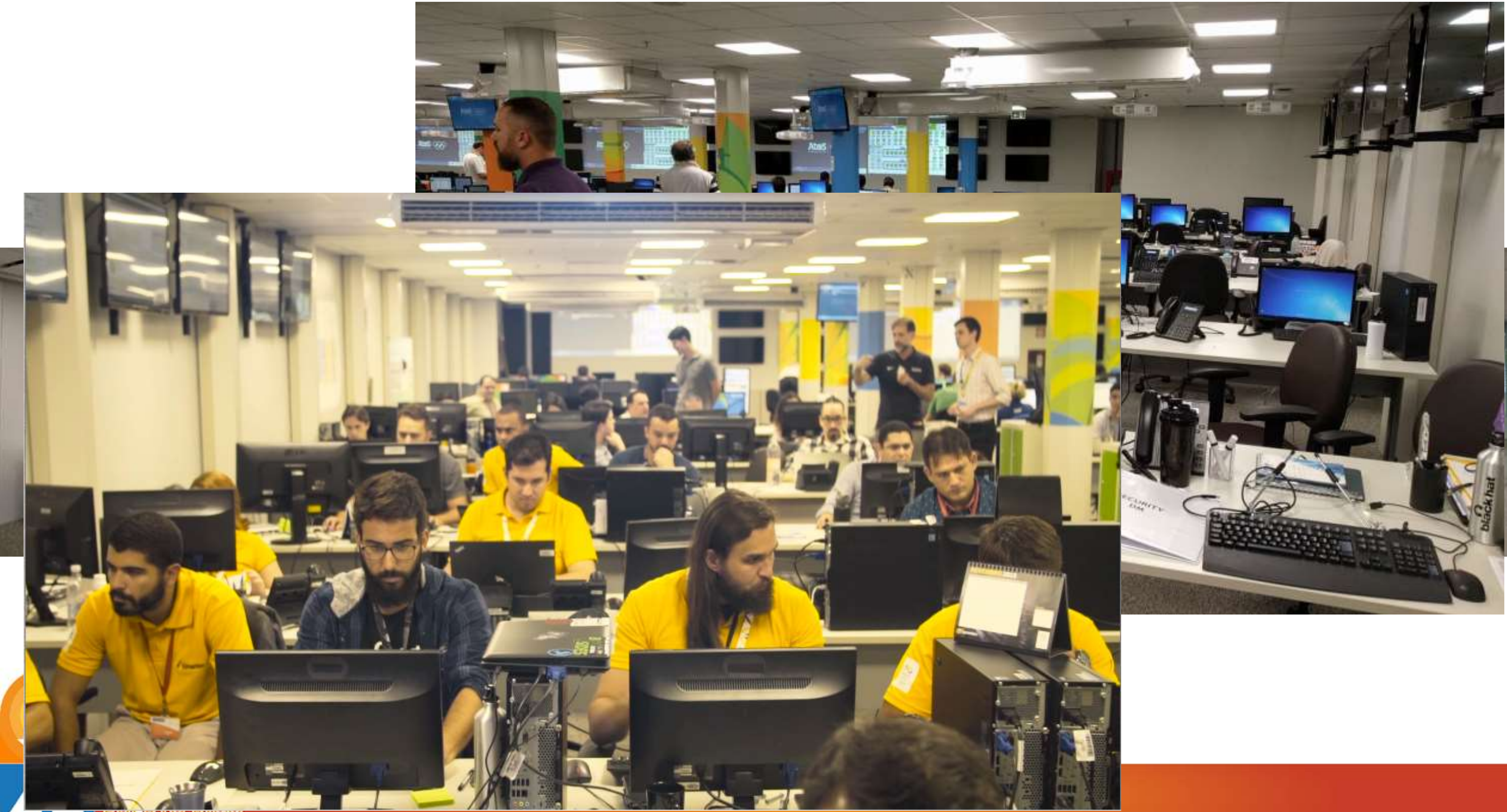
92.875
Workforce

57.256
Press Wifi

18.027
Athletes
(Wi-Fi users)

Wrap up for CSIRT

- Operations initiated 24x7 in 4th July 2016
- Clients: Press, Olympic family, Sponsors and Partners.
- Escope: Rio 2016 infrastructure (on premise and cloud)
- Around 80 people in CSIRT team
- 15 companies
- Red team inside CSIRT team
- Threat intelligence covering more than 9 languages (with help of Japan)
- Cooperation with government agencies
- Remote and on-site IR.


Atos
black hat
SECURITY

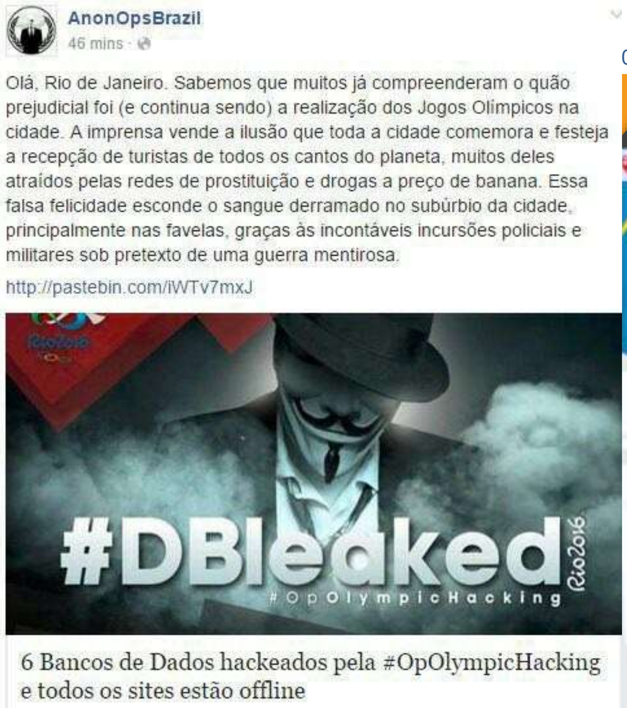
Threat intel timeline

July

August

03 05 06 08 09

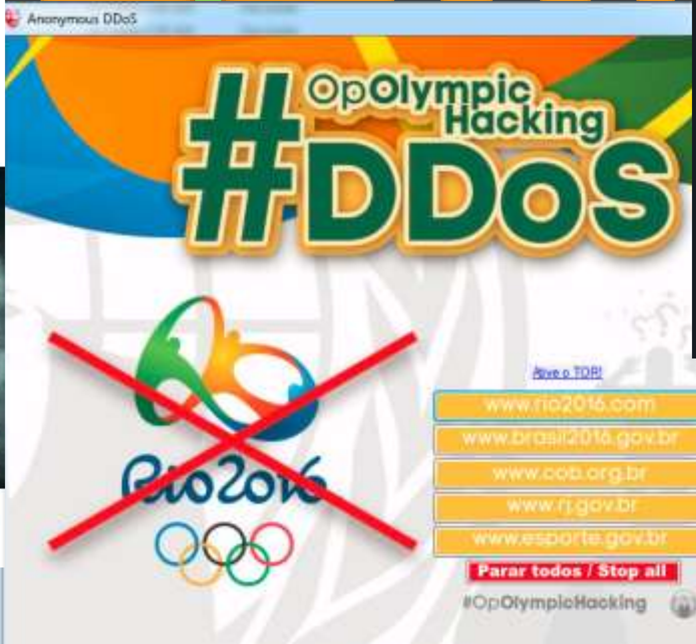
Opening Ceremony

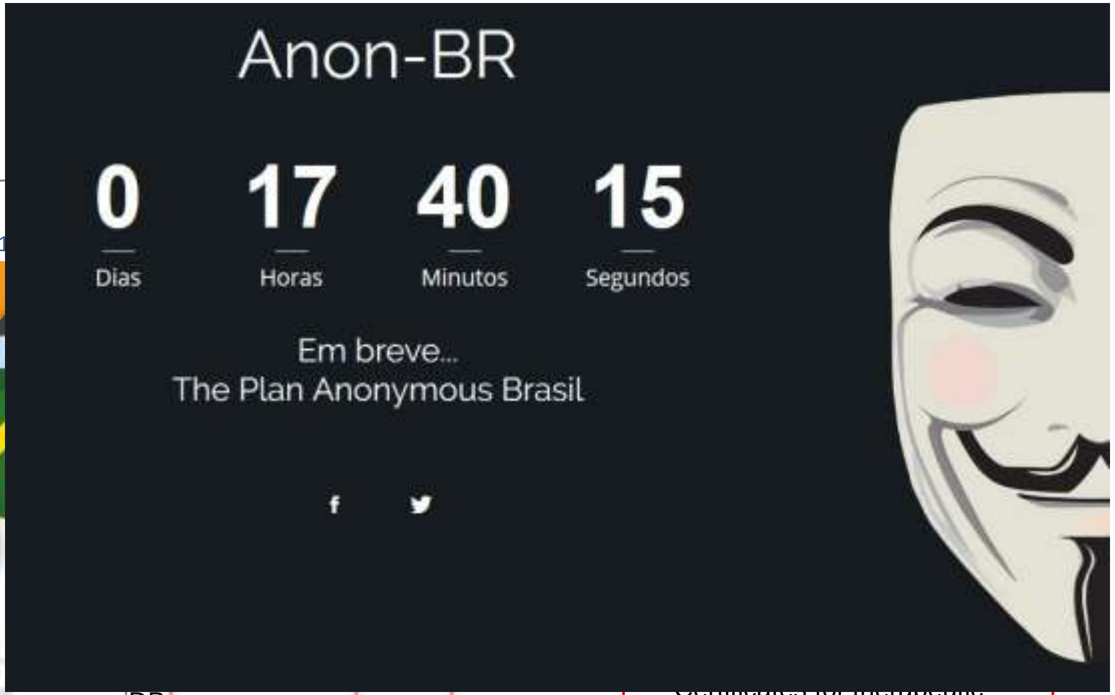

AnonOpsBrazil
46 mins ·

Olá, Rio de Janeiro. Sabemos que muitos já compreenderam o quão prejudicial foi (e continua sendo) a realização dos Jogos Olimpicos na cidade. A imprensa vende a ilusão que toda a cidade comemora e festeja a recepção de turistas de todos os cantos do planeta, muitos deles atraídos pelas redes de prostituição e drogas a preço de banana. Essa falsa felicidade esconde o sangue derramado no subúrbio da cidade, principalmente nas favelas, graças às incontáveis incursões policiais e militares sob pretexto de uma guerra mentirosa.

http://pastebin.com/iWTv7mxJ

6 Bancos de Dados hackeados pela #OpOlympicHacking e todos os sites estão offline





- IOC
- COB
(Brazilian OC)

Spanish

DB leaks of several sports confederations

- DDoS attacks against website "www.rj.gov.br"
- Leaked personal data of heads of RJ Gov. offices

DB
r Sport

t received
early Aug
Yuliya
ussian
ount was
ed

AnonOpsBR hacked OBS (Olympic Broadcasting Services) main website and leaked an associated DB

Anon Poland criticizes Olympic Games and promises new attacks against WADA

- Anon Poland says the group attacked "teamusa.org" and "paralympic.org"
- Our assessment classified that as false claims

Certificates for therapeutic usage of prohibited drugs.

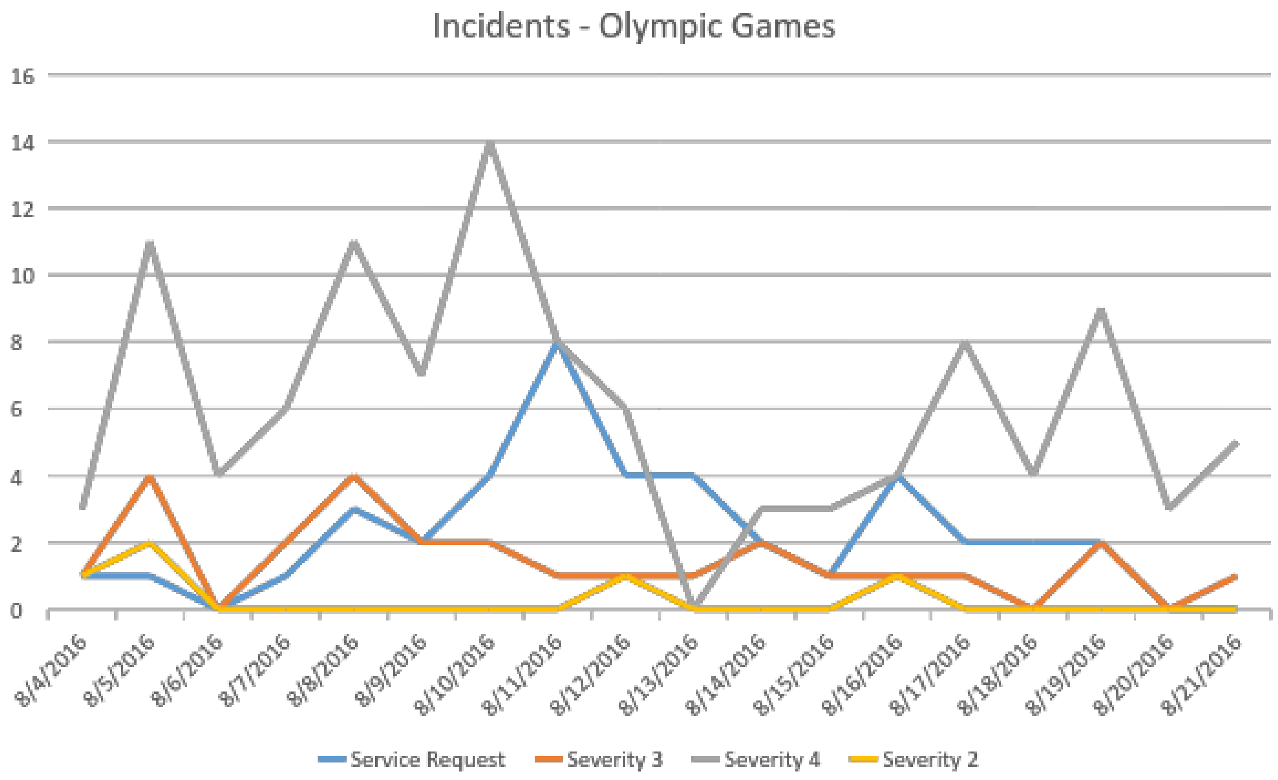
WADA confirmed the hack

Caption

- ★ Main activities
- ◆ Other Hacktivism activities

Security Numbers

- +20m of alerts
- 181 incidents
- 50.000 authentications using 2FA (around 5800 users)
- Around +800 malware blocked on AntiSpam.
- +50 takedowns during the games time period
- +30m WAF blocks (website e mobile app)
- +100k connected equipments
- Major incidents: Anon ransomware, Wada attacks detected on our network



Lessons learned from whole experience

- Understand you public, scope and start small
- Know your communication channels, exercise them regularly
- Brief and contact external partners before critical periods
- Fine tuning forever
- Triage is key, cannot be underlooked as someone without experience
- Centralize your documentation, make it easy for newcomers
- Attention to shift hand-off, contextual information can be lost. (overlaying is a good option)
- Avoid at all cost, the “ticket closing” behavior, incidents should be investigated until the end. TTPs and IOCs must be determined and returned to monitoring
- Situational awareness meetings/reports is nice to have, set team in the mood and prepare for difficult situations
- Automatize everything as possible

Thank you