IT Security for the Olympics
London 2012 experience

ATEC

Atos – Major Events

09/10/2013

>Agenda

- Introduction
- IT Security scope
- Methodology and processes
- Risk assessment
- Examples of Security controls:
  - Security Information and Events Management
  - Identity Management
  - Integrity Monitoring

- Long-term relationship based on trust and proven performance since Barcelona 1992
- Worldwide IT Partner since 1999 to 2016

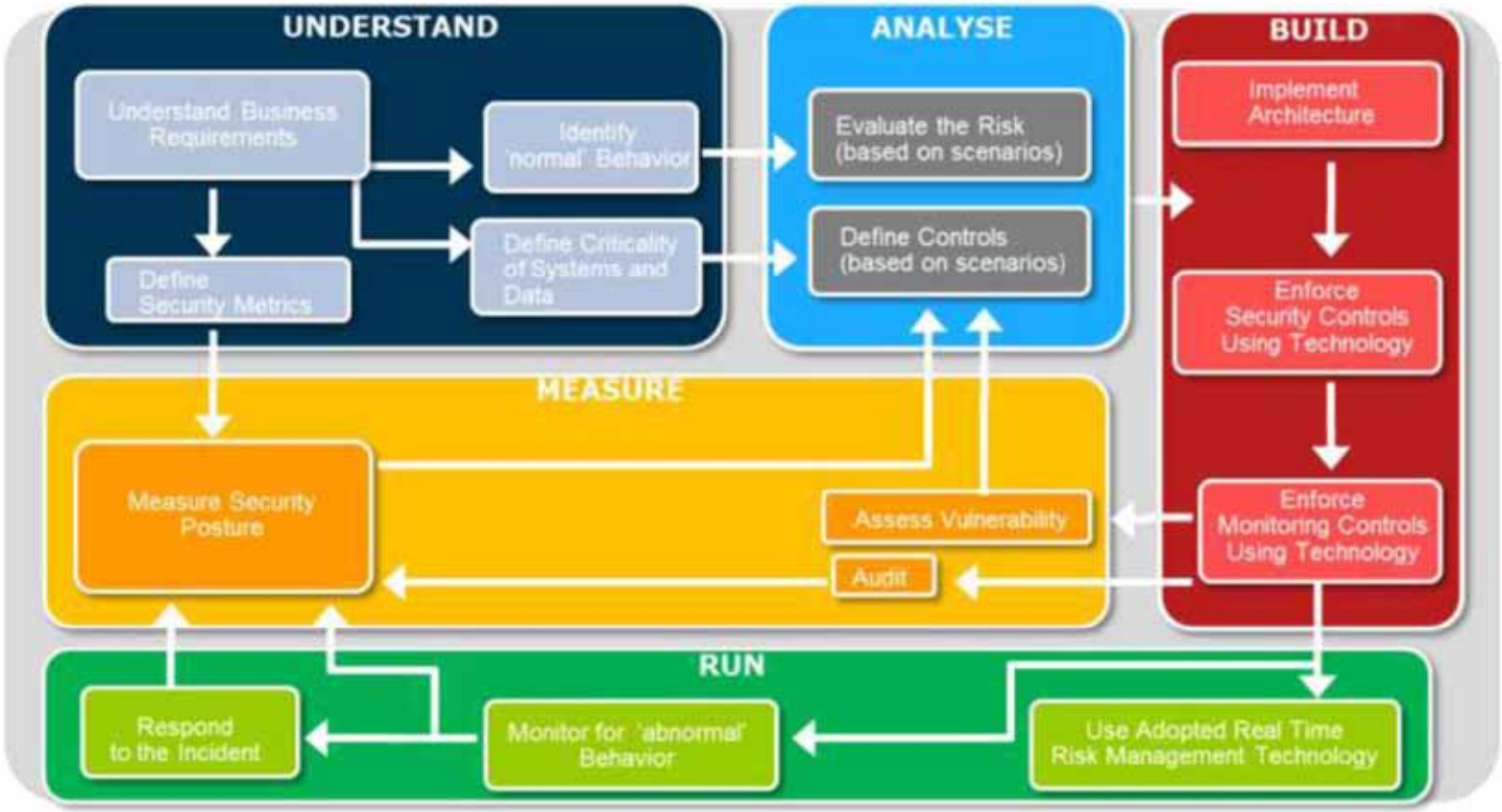
>What we deliver?

Timing and Scoring		▶ Real time applications (Scoreboard)	**100% Availability** **Integrity** **100% Accurate**
Information Diffusion Systems		▶ Near real time ▶ Feed to the Press & Broadcasters ▶ Remote Services	**Availability** **Integrity**
Games Management Systems		▶ Olympics Resource Planning Applications ▶ (ACR, SIS, TRA...)	**Personal data** **Confidentiality** **Integrity**

BACK FORWARD

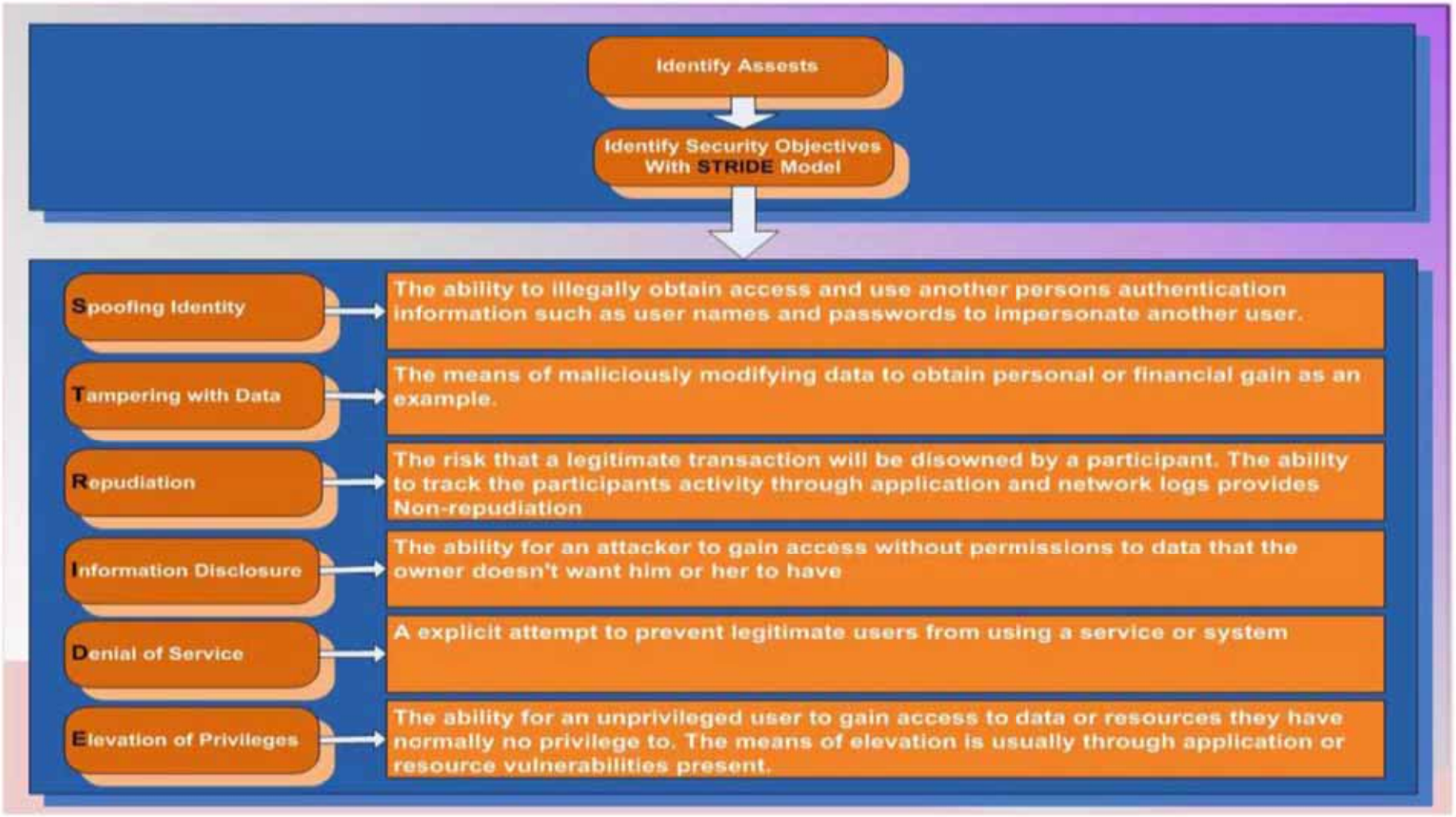
- Usual Olympic project challenges:
  - -Deliver on-time and on-budget
  - -New environment every 2-years
  - -Large scale deployment (in short time windows)
  - -Complex integration (different partners and technologies)

>IT Security methodology



>Pre-Operations scope

- IT Risk Assessments
- IT Security Controls definition and implementation:
  - -Policies & Procedure
  - -IT Architecture
  - -Infrastructure hardening
  - -Security Awareness Trainings
- IT Security Tests:
  - -Vulnerability testing
  - -Penetration testing
- IT Security posts measurement:
  - -Security Audits

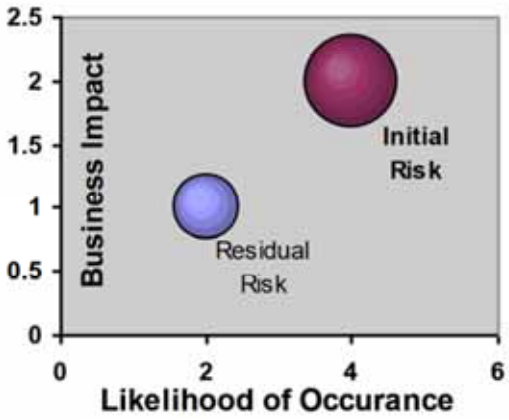

Identify Assests
Identify Security Objectives With STRIDE Model
Spoofing Identity
The ability to illegally obtain access and use another persons authentication information such as user names and passwords to impersonate another user.
Tampering with Data
The means of maliciously modifying data to obtain personal or financial gain as an example.
Repudiation
The risk that a legitimate transaction will be disowned by a participant. The ability to track the participants activity through application and network logs provides Non-repudiation
Information Disclosure
The ability for an attacker to gain access without permissions to data that the owner doesn't want him or her to have
Denial of Service
A explicit attempt to prevent legitimate users from using a service or system
Elevation of Privileges
The ability for an unprivileged user to gain access to data or resources they have normally no privilege to. The means of elevation is usually through application or resource vulnerabilities present.

- Scenarios: "What – **How** – **What for**"
  - **What:** describe the threat
  - **How:** define which vulnerability is exploited to break into the targeted system
  - **What for:** describe the purpose of the attack: corruption, disclosure, denial of service…
- Example of scenario:
  - Break into the OVR server through OS vulnerability to modify data on the Scoreboard.
- Validation of the scenarios:
  - Technical Rehearsals
  - Penetration Testing
  - Periodic Security Reviews

Title: INFO Server DoS
Description: Intruder plugs a laptop in INFO VLAN to perform DoS attack against INFO server

>Risk scenario example

Initial Evaluation:
Business Impact: Multi-Catastrophic **Likelihood:** High
Risk Level: 9



Impact Mitigation Controls:

- Info Application Tuning
- Load Balancer bandwidth limitation
- Web Server hardening

Likelihood Mitigation Controls:

- Port Security
- Laptop Security Policy
- OS Hardening procedures
- Network Segmentation

Monitoring Controls:

- Monitor Web attack IDS signature
- Monitor server CPU
- Monitor Bandwidth utilization

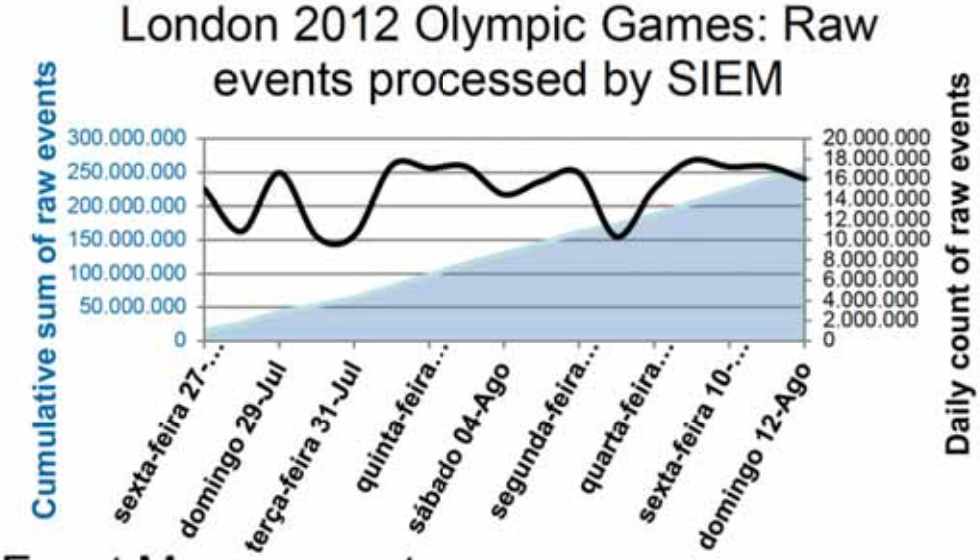
Residual Evaluation:
Business Impact: Major **Likelihood:** Low
Risk Level: 5

- Real time security monitoring:
  - -Intelligent processing
  - -Prioritization
  - -Real time security auditing
- Incident Management:
  - -Incident response procedures
  - -24x7 incident response support
- System Maintenance:
  - -Network & OS access rules

>SIEM

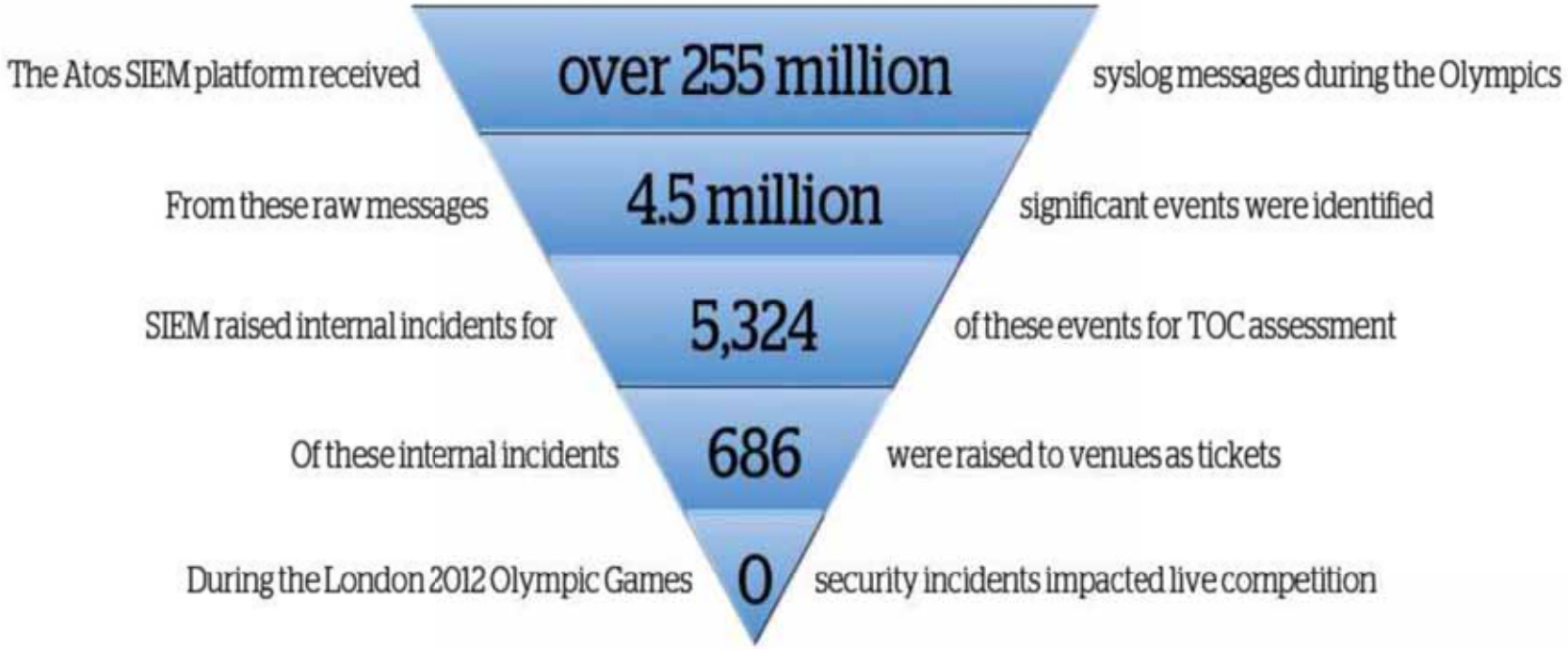
- How to understand over 255,000,000 security related syslog messages?
- How to recognize real threats in over 4,000,000 security events?

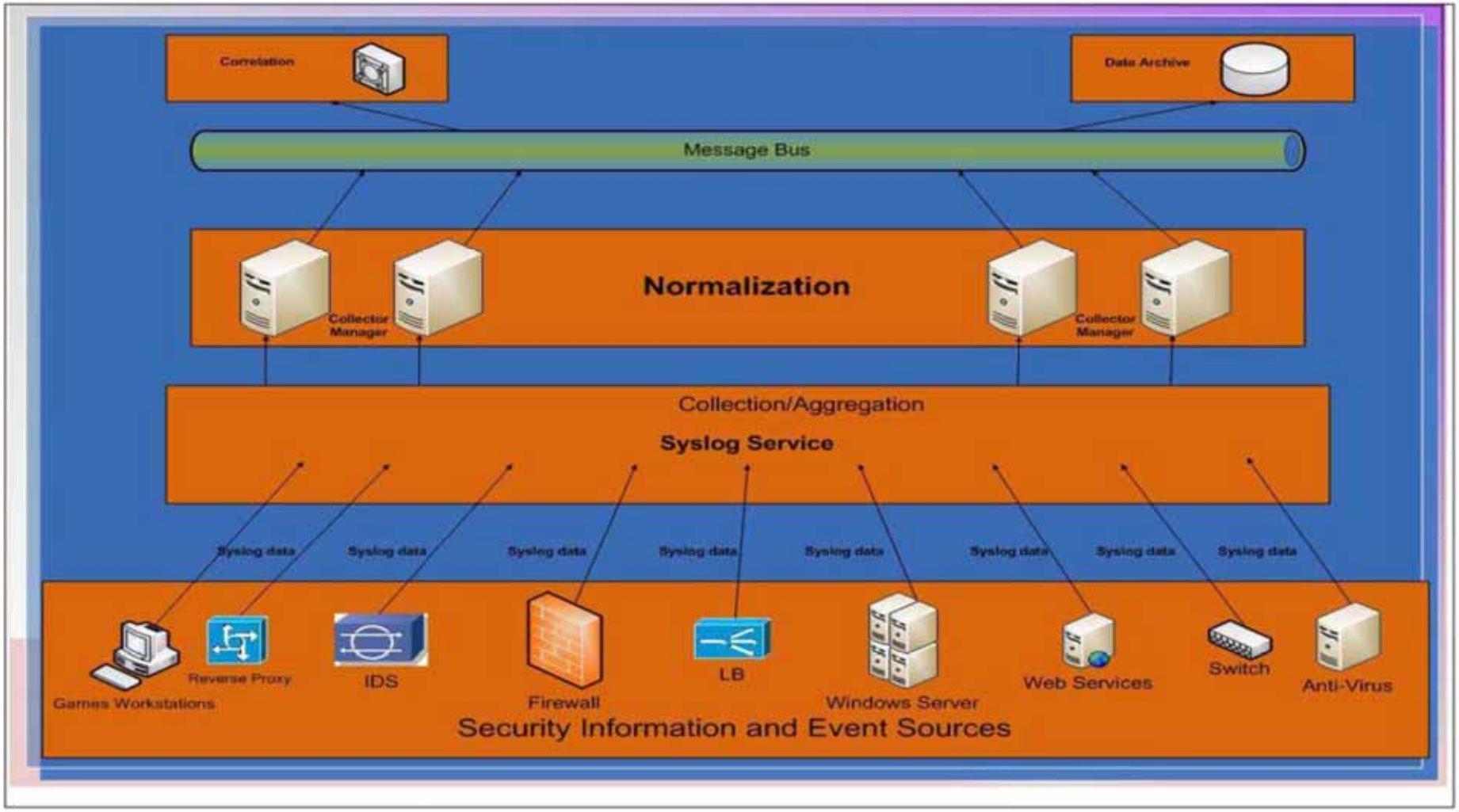
- The solution: **MEV Real Time Security Risk Management**

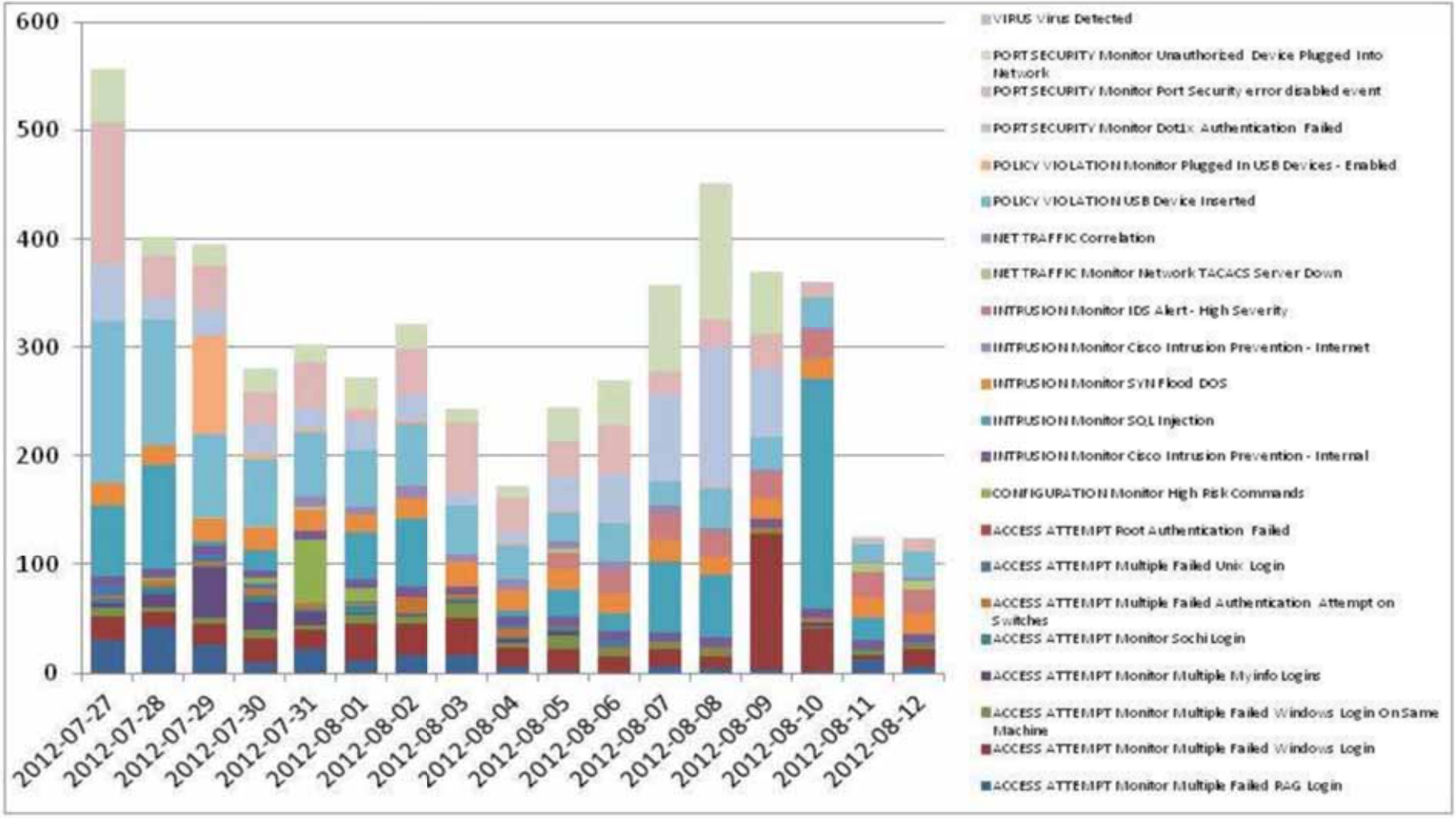


- Implement a Security Information and Event Management (SIEM) solution
  - Perform Intelligent Event Processing
  - Aggregation & Correlation
  - Prioritization
  - Real Time Auditing
  - Predefined Incident Management Process

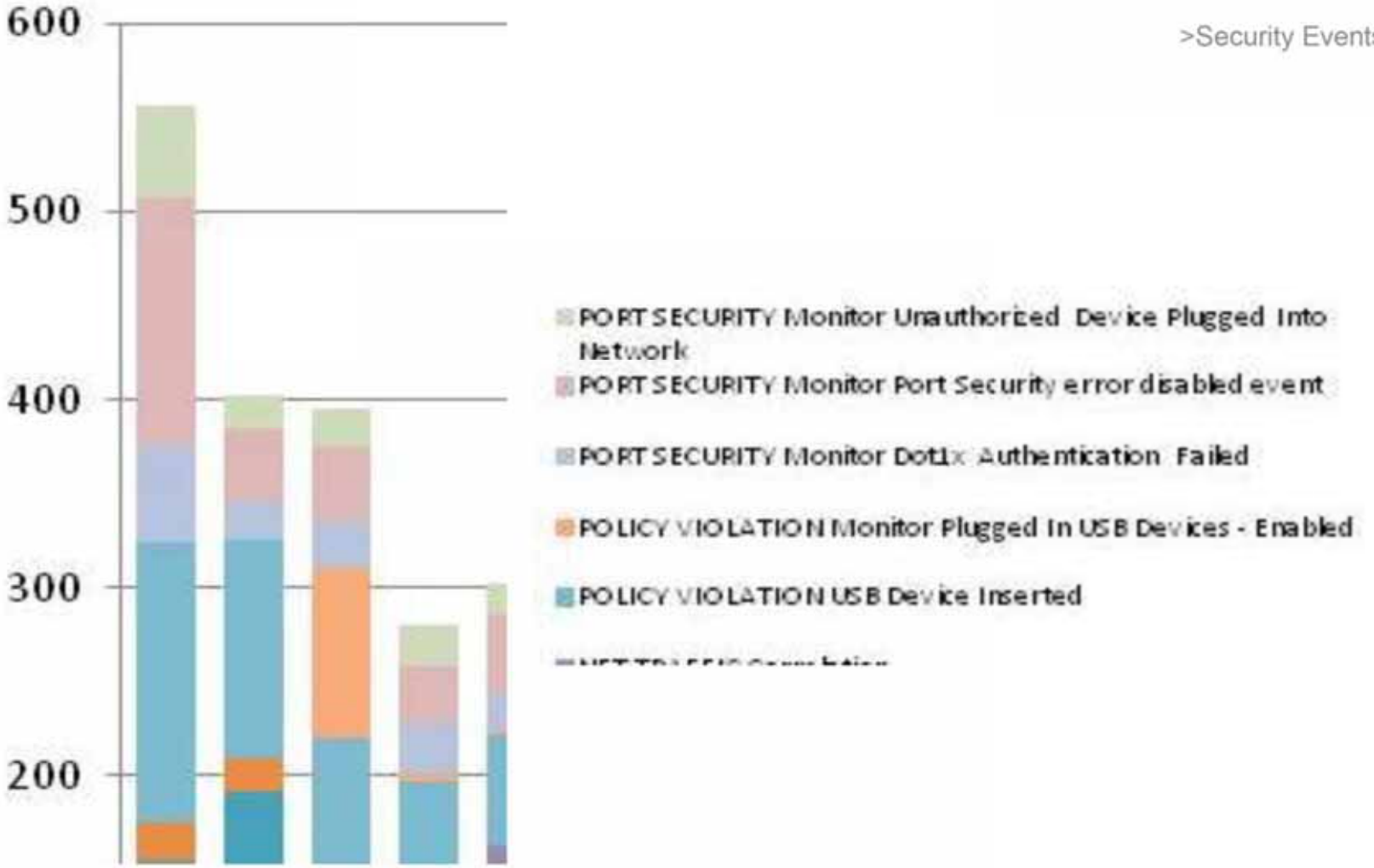
BACK FORWARD


The Atos SIEM platform received
over 255 million
syslog messages during the Olympics
From these raw messages
4.5 million
significant events were identified
SIEM raised internal incidents for
5,324
of these events for TOC assessment
Of these internal incidents
686
were raised to venues as tickets
During the London 2012 Olympic Games
0
security incidents impacted live competition


Correlation
Data Archive
Message Bus
Normalization
Collector Manager
Collector Manager
Collection/Aggregation
Syslog Service
Syslog data
Syslog data
Syslog data
Syslog data
Syslog data
Syslog data
Syslog data
Syslog data
Games Workstations
Reverse Proxy
IDS
Firewall
LB
Windows Server
Web Services
Switch
Anti-Virus
Security Information and Event Sources


600
500
400
300
200
100
0
2012-07-27
2012-07-28
2012-07-29
2012-07-30
2012-07-31
2012-08-01
2012-08-02
2012-08-03
2012-08-04
2012-08-05
2012-08-06
2012-08-07
2012-08-08
2012-08-09
2012-08-10
2012-08-11
2012-08-12
VIRUS Virus Detected
PORT SECURITY Monitor Unauthorized Device Plugged Into Network
PORT SECURITY Monitor Port Security error disabled event
PORT SECURITY Monitor Dot1x Authentication Failed
POLICY VIOLATION Monitor Plugged In USB Devices - Enabled
POLICY VIOLATION USB Device Inserted
NET TRAFFIC Correlation
NET TRAFFIC Monitor Network TACACS Server Down
INTRUSION Monitor IDS Alert - High Severity
INTRUSION Monitor Cisco Intrusion Prevention - Internet
INTRUSION Monitor SYN Flood DOS
INTRUSION Monitor SQL Injection
INTRUSION Monitor Cisco Intrusion Prevention - Internal
CONFIGURATION Monitor High Risk Commands
ACCESS ATTEMPT Root Authentication Failed
ACCESS ATTEMPT Multiple Failed Unix Login
ACCESS ATTEMPT Multiple Failed Authentication Attempt on Switches
ACCESS ATTEMPT Monitor Sochi Login
ACCESS ATTEMPT Monitor Multiple Myinfo Logins
ACCESS ATTEMPT Monitor Multiple Failed Windows Login On Same Machine
ACCESS ATTEMPT Monitor Multiple Failed Windows Login
ACCESS ATTEMPT Monitor Multiple Failed RAG Login

>Security Events



BACK FORWARD

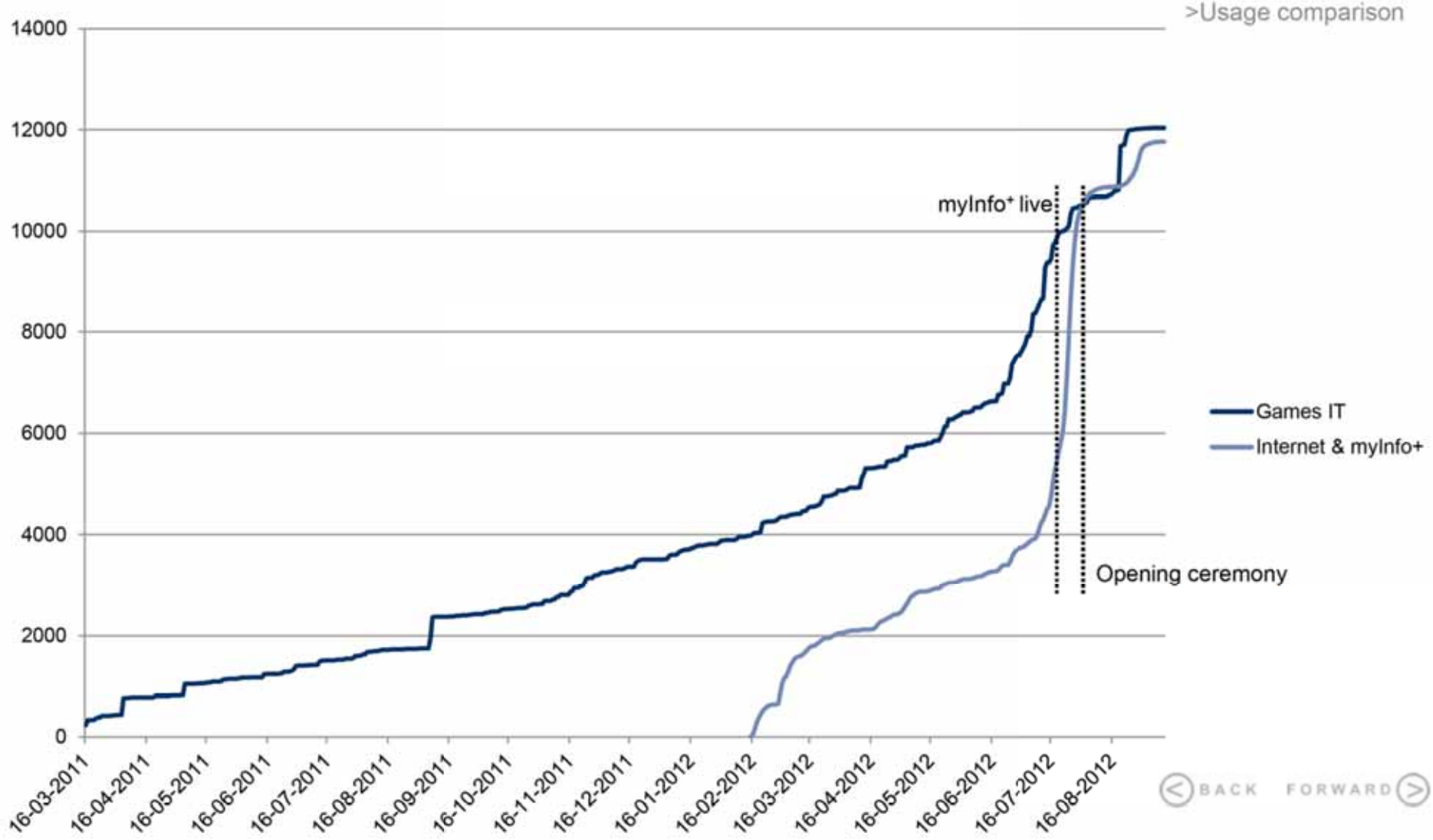
Games IT

- Large number of privileges and systems
- Supports end-to-end process
- Requires manual approval

Internet & myInfo+

- Few privileges
- Covers only provisioning
- High provisioning performance

>Usage comparison

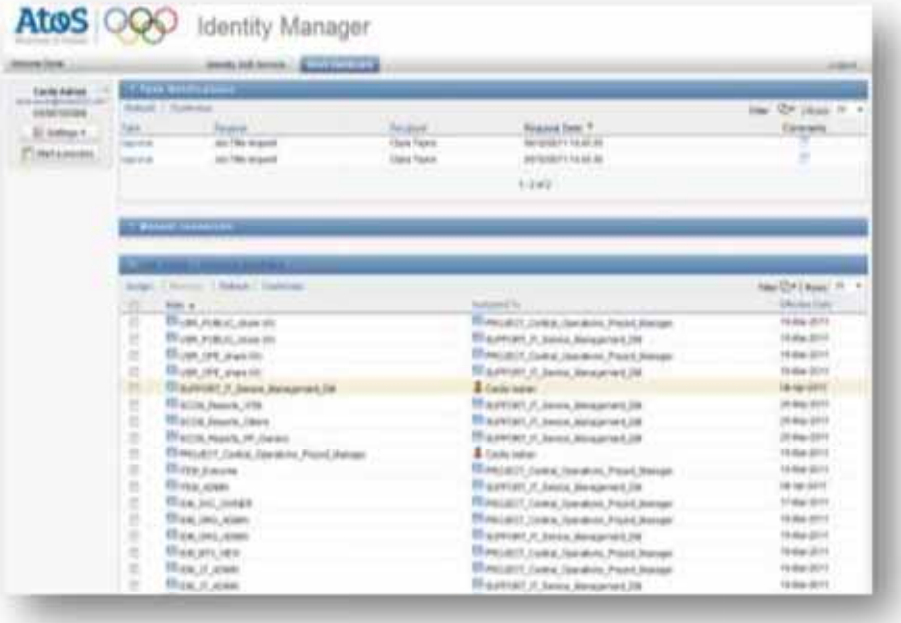


BACK FORWARD

>Games IT IDM

- Formalization and documentation of all privileges in Games services: **Service profiles**
- Definition and maintenance of **Job titles**
- Assignment of Service profiles to Job titles: **Access Matrix**
- Assignment of Job titles to identities: **Access requests**
- Password management

- Key success factors:
  - Streamline the process by facilitating Self-service
  - Dynamic privileges management
  - Integrated implementation follow-up

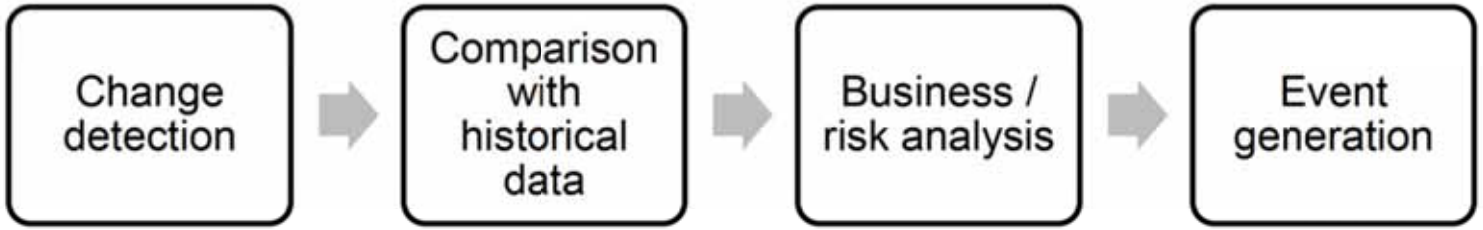


- Provide Internet and myInfo+ access to media
- Peak usage around opening ceremony: lightweight solution designed for provisioning performance
- Self-registration using pre-bought “access passes”
- Time based provisioning

- Other use cases: manage a corporate guest Wi-Fi service

- Detection and analysis of changes:
  - Software update
  - Configuration change
  - Malicious attack
  - Mistakes

- Scope:
  - Binaries (checksum, privileges, timestamps, etc.)
  - Configuration files and parameters (content, timestamps, etc.)



- Key success factors
  - -Support Configuration management through auditing
  - -Validate application behaviors
  - -Integration with SIEM

- Main challenge: understanding of the internals of monitored applications to avoid false-positives

Thanks

For more information please contact:
T+ 34 605 745 606
adrien.montfaucon@atos.net

- Accreditation Applications

-Electronic Accreditation Form System (ECR):

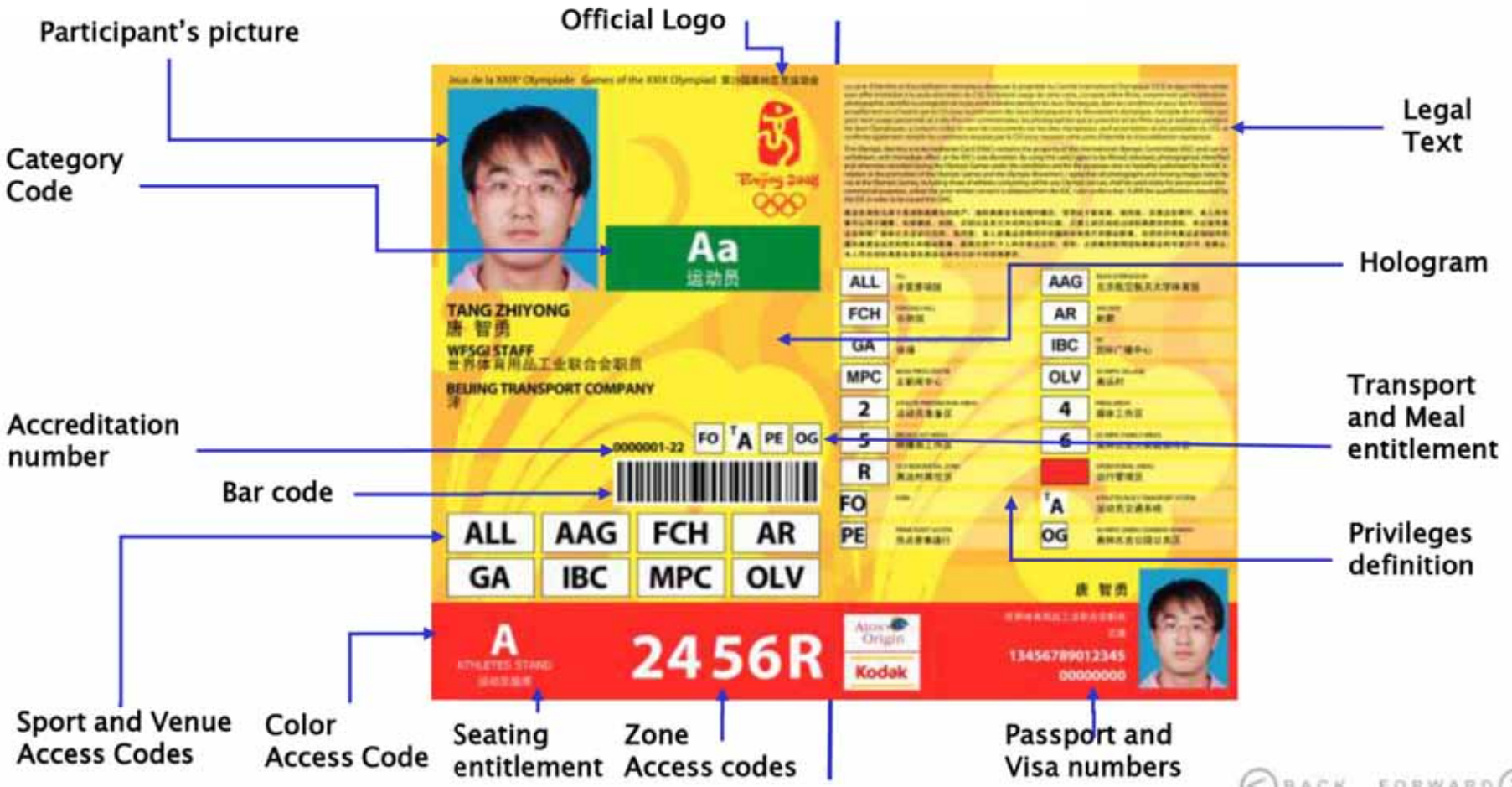
- Multilanguage Registration Forms for Event Staff, Teams, Media…
- Different mechanisms to register participants to one/several event/s
- Detection process of duplicated registration forms
- Effortless registration
- Tracking the Participant Accreditation status changes

-Accreditation System (ACR):

- Registration of participant's personal data
- Assignation of privileges
- Sophisticated provision of clearly visible accreditation badges
- Management of Participants' Data including the Participant Badge production history

-Access Control System (ACS)

- Real-time verification of the accreditation badges against the ACR database at security checkpoints
- Fixed and mobile communication devices
- Supporting Barcode, RFID or NFC technologies


Participant's picture
Official Logo
Legal Text
Category Code
Hologram
Transport and Meal entitlement
Accreditation number
Bar code
Privileges definition
Sport and Venue Access Codes
Color Access Code
Seating entitlement
Zone Access codes
Passport and Visa numbers
Aa
运动员
TANG ZHIYONG
唐 智勇
WFSGI STAFF
世界体育用品工业联合会职员
BEIJING TRANSPORT COMPANY
0000001-22
FO
A
PE
OG
ALL
AAG
FCH
AR
GA
IBC
MPC
OLV
2456R
Kodak
13456789012345
00000000