



Security Operation Centers

V.Todorovic

Agenda

- ▶ Where to start?
- ▶ How project implementation looks like?
- ▶ SOC Organizational Structure
- ▶ SOC Positions and their definition
- ▶ SOC Procedures with examples
- ▶ Incident Management
- ▶ Multi Regional SOCs
- ▶ Technical Rehearsal
- ▶ Disaster Recovery
- ▶ Critical Services Real Life Example



Service Levels Drive Everything

Operations Service Levels (1)

Incident Response & Resolution

	Target Response Time	Target Fix Time
Severity 1	5 minutes (95%)	1 hour (95%)
Severity 2	5 minutes (95%)	2 hours (95%)
Severity 3	30 minutes (95%)	4 hours (95%)
Severity 4	60 minutes (95%)	8 hours (95%)

1. Service Availability

	Downtime over 30 days for 24 x 7 operations	Downtime over 30 days for 20 x 7 operations
99.9%	43.2 minutes	36 minutes

It is recommended to define criticality level by measurable parameters (number of hosts affected, service criticality, escalation level...)



Service Levels Drive Everything

Operations Service Levels (2)

System Performance

Examples	Target Performance Level
Commentator Information System	-300 msec from Results System to client -for 96% of all messages
INFO2008 Reports Publishing	-Less than 1 minute -for 90% of all messages.
INFO2008 Navigation	-4 seconds -for 90% of all navigation



Security & Technology Operations Centre

- » 24 x 7 Operations
- » 2 x 12 hour shifts per day
- » 150 Positions (IT, Telecom, Facilities)
- » Incident Management
- » Change Management
- » Disaster Recovery and Crisis management
- » Monitoring



Not just a support team, but the core of the incident management system



SOC Building Blocks

Processes

Ensure operational procedures are properly

- defined,
- trained and
- practiced

► People

- Ensure staff readiness through
 - Training and awareness
 - Professional skills
 - Stress test



Technology

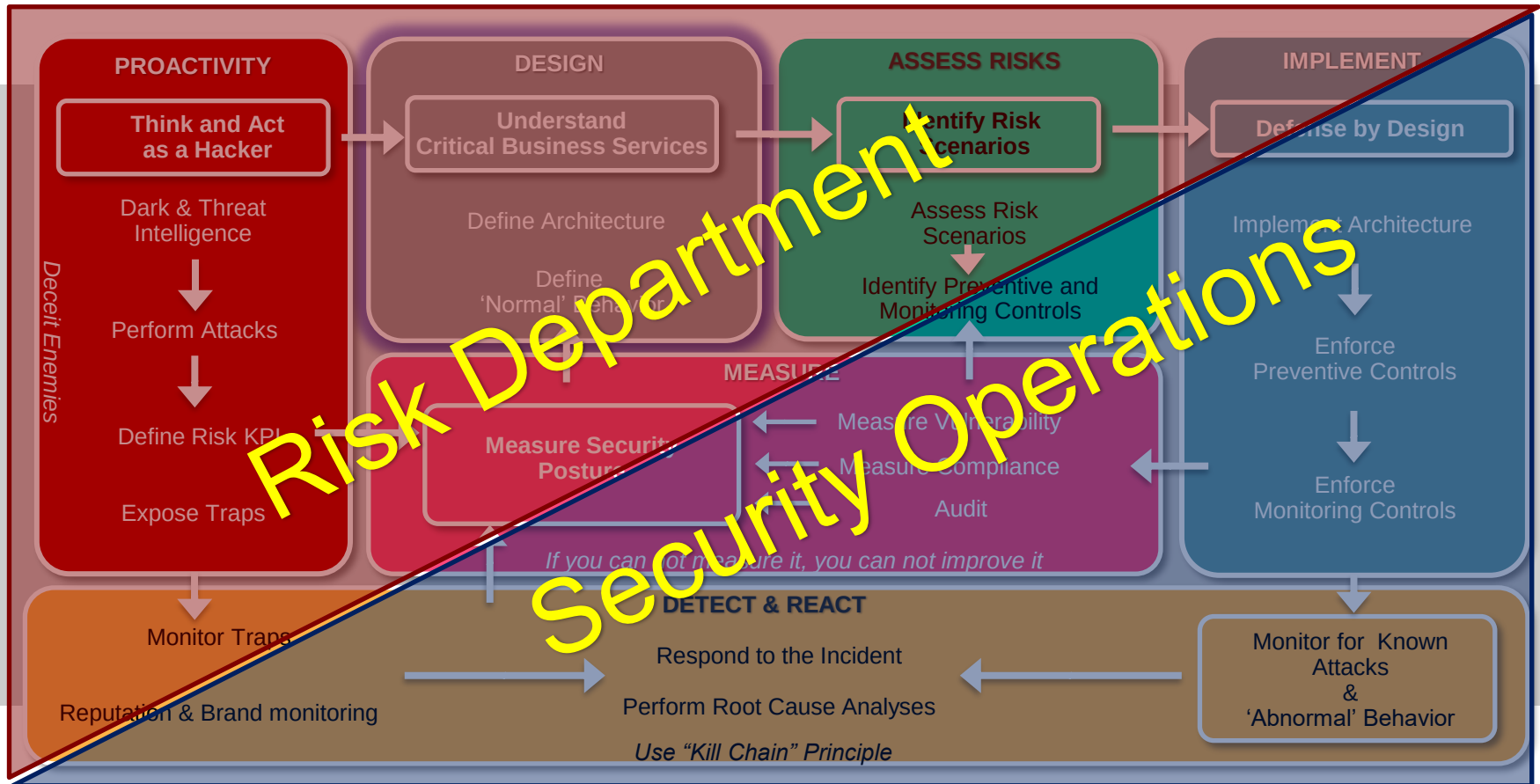
Ensure technology excellence by

- End-to-end testing
- Fail over tests
- Automated KPI

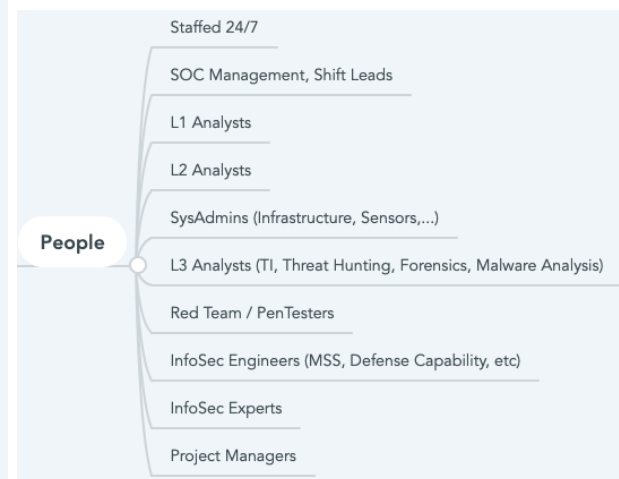
we ensure SOC operational readiness excellence using tech rehearsals



Split of Responsibilities for Internal Competition Effect



Example of a Mature SOC / CSIRT - Processes, Technology, People



Tasks Overview

- ❖ IT Security controls definition and implementation
 - ❖ Policies & Procedures definition
 - ❖ Security Architecture definition
 - ❖ Network hardening
 - ❖ OS hardening
 - ❖ DB hardening
 - ❖ Application hardening
 - ❖ Security Awareness Trainings
 - ❖ SIEM implementation
 - ❖ Advanced Security Controls Implementation

- ❖ IT Security Tests
 - ❖ Network services testing
 - ❖ Vulnerability assessments
 - ❖ Penetration testing
- ❖ Operational Test
 - ❖ Test Events
 - ❖ Test Rehearsals
- ❖ IT Security posts measurement
 - ❖ Risk Assessments
 - ❖ System Tests
 - ❖ Security Audits



General SOC / CSIRT Capabilities

1. Providing Office Space, Equipment, Technological Platform
2. Implementing Operation & Maintenance Capability: Infrastructure O&M, Sensor Tuning & Maintenance
3. **Building Demonstration Capability:** (8/5), Webinars, Presentations, Demonstrations, Reports, Pilots (partly)
4. Building Basic Detection Capability: Call Center, Basic Monitoring, Incident Detection, Triage, Notification
5. Implementing Extended Detection Capability: Vulnerability Scanning/Assessment, PenTest, Custom Signature Creation, Threat Hunting, Behavior Analytics
6. Implementing Threat Intelligence Capability: Cyber News Analysis, Trending, Threat assessment, Forensics, Malware Analysis, Fusion, Tradecraft Analysis, Distribution
7. Implementing Response Capability: Incident Investigation, Response (On-Site/Remote), Automation
8. Implementing Defense Capability: MSS, Blue Team
9. Implementing Proactive Defense / Offense Capability: Red Team
10. Implementing Engineering Capability: Tool Development & Customization, Scripting & Automation
11. Building Full SOC/CSIRT Capability: (24/7), All Competencies maintained In-house, Self-Sufficient, Self-Optimizing



Building *Demonstration Capability* for Indorama SOC

- Goals
 - Developing Capability Necessary for Demonstrating SOC Functionality to Potential Clients
 - Minimizing the Project Cost by Leveraging Use of a Free of charge, or Low cost software
 - Dependencies
 - Office Space, Equipment, Technological Platform
 - Adequate Real-Time Flow of Log-Data
 - Established Operation & Maintenance Capability
 - Infrastructure O&M
 - Sensor Tuning & Maintenance
 - Competences to be Developed in the Project
 - Conducting Online Webinars
 - Conducting Online and Live Presentations
 - Conducting Online and Live Demonstrations
 - Generating and Explaining Standard Reports
 - Presenting Results of Pilot Projects
- ## Indorama SOC after the project completion
- People
 - Staffed 8/5
 - L1 Analysts: (2)
 - L2 Analysts: (1)
 - SysAdmins (Infrastructure, Sensors,...): (Linux+Network+Windows OR Outsourced)
 - Processes
 - required: SOC Infrastructure Admin & Support (including Infrastructure Monitoring)
 - required: Security Event Sources Management
 - Security Event Monitoring / Incident Detection
 - KPI Control & Reporting
 - Technology
 - required: SIEM
 - Incident Management
 - Vulnerability Management
 - Reporting (including Dashboards)
 - Deception Platform
 - Visual Analytics



Project Phases and Schedule - 1

I. Project Preparation 2 weeks

- Analysis of information provided by the client
 - SOC Vision, Mission, Strategy, Requirements (ext, int), Products & Services (if available)
 - Information on Space, Equipment, Technological Platform
 - Current Operation & Maintenance Capability
 - Existing Employee Competence and Experience, Phone Interviews (If organized In-house)
 - Contracts and SLAs (If Outsourced)
 - Current Detection / Demonstration Capability
 - Information on Existing Employee Competence and Experience, Phone Interviews
- Technological Platform Audit (Architecture, Performance, Stability, Data Sources, Detection Rules, etc)
- Project Planning

II. Installation/Configuration/Integration of Systems and Tools 2 weeks

- Dependency: remote VPN access to assigned servers, OS installed according to requirements
- Installation & Configuration of the following systems:
 - Incident Management
 - Vulnerability Management
 - Deception Platform
 - Visual Analytics
 - Reporting (including Dashboards)
 - Infrastructure Monitoring (if not implemented)
- Integration of Incident Management with Aspen



Project Phases and Schedule - 2

III. Process Implementation (remote), 1 week

- Security Event Monitoring / Incident Detection
 - Workflow Implementation
- KPI Control & Reporting
 - KPI Configuration
 - Reporting Configuration
 - Process “Training” (Creating Cases for Report Generation)

IV. Staff Selection and Hiring (remote & On-site), 1 week (depending on a number of candidates)

- Candidate Resume Review (remote), 1-2 days
- Candidate Interviews (On-site), 2-3 days

V. Live Demonstration Preparation (remote & On-site), 1 week

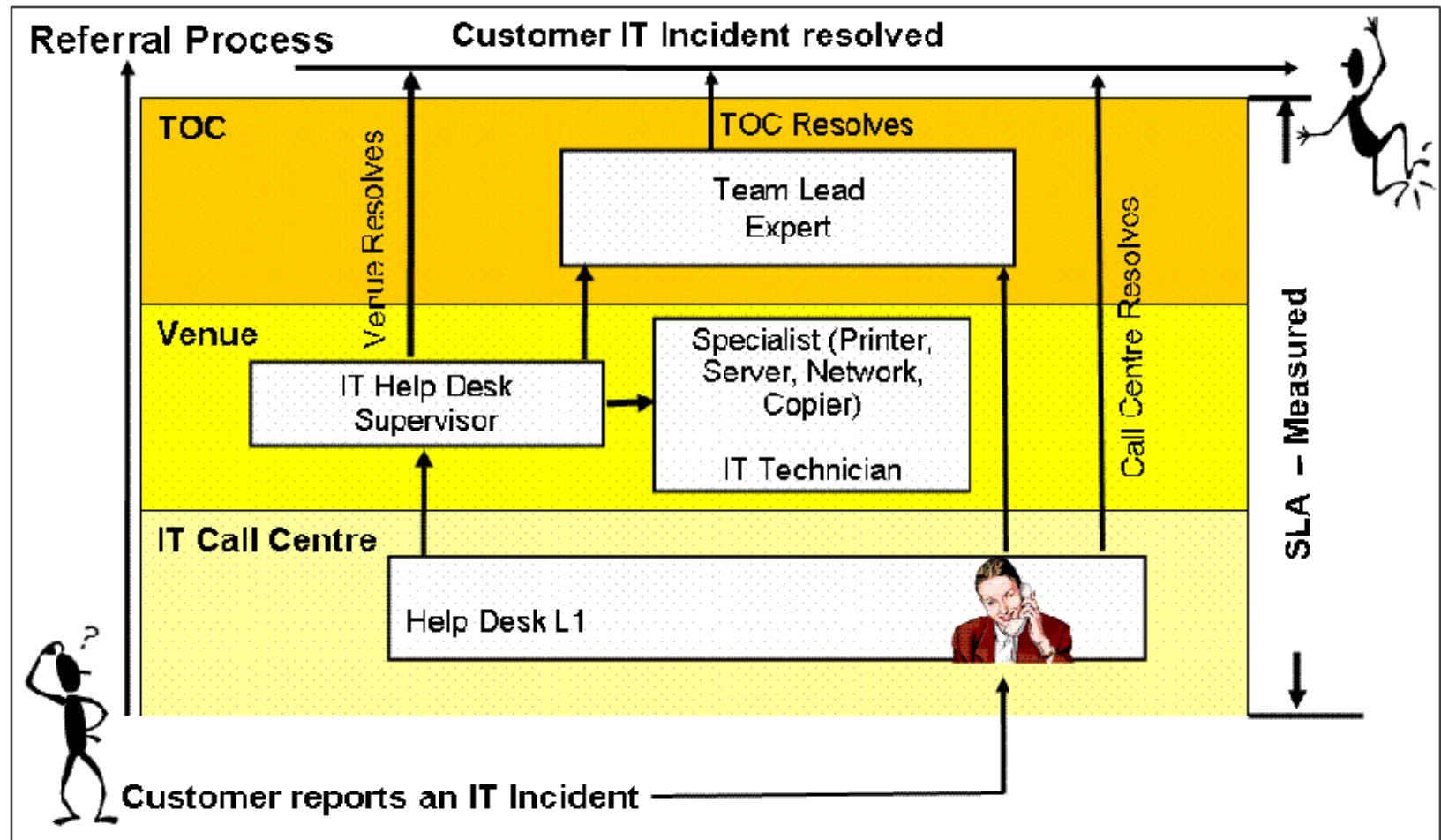
- Designing the Use-cases and Preparing the Demonstration Scenario
- Technical Preparation of the Use-cases
- Use-cases Rehearsals

VI. Training (remote & On-site), 1-2 weeks (depending on the level of competence of the personnel)

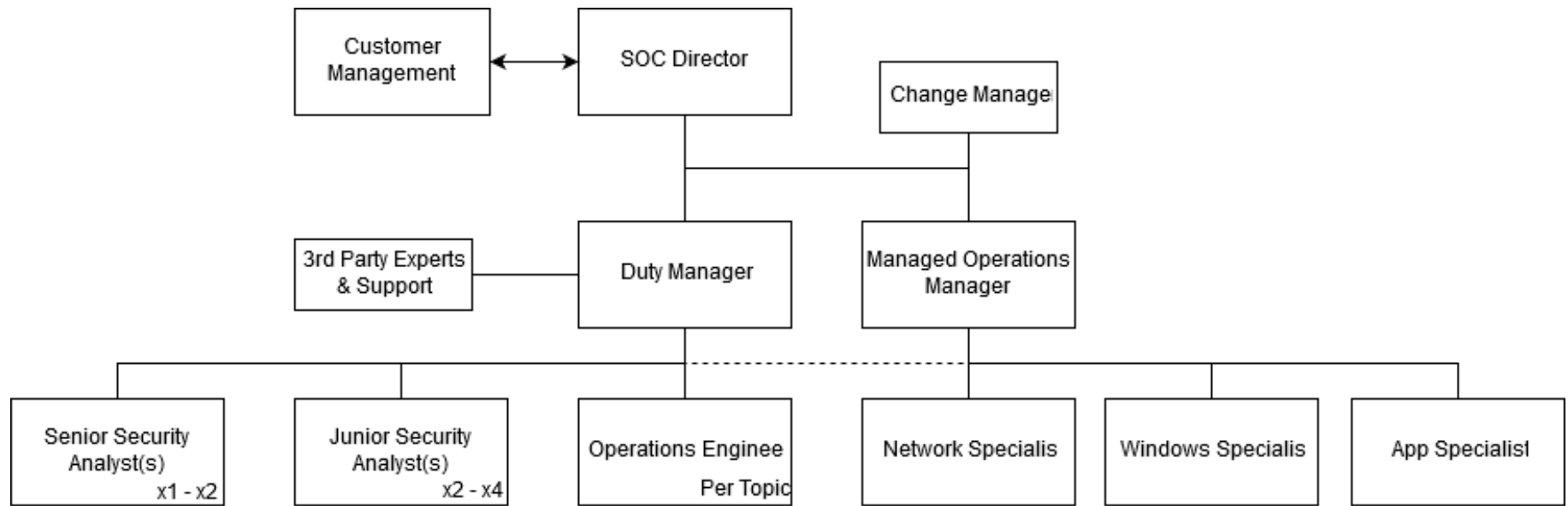
- Aspen: Event Monitoring and Incident Detection (to the level necessary for the Pres / Demo)
- Incident Management: Incident Workflow, KPIs, Reports (Incidents, KPIs, Vulnerabilities, etc)
- Live Demonstration: Training & Rehearsals



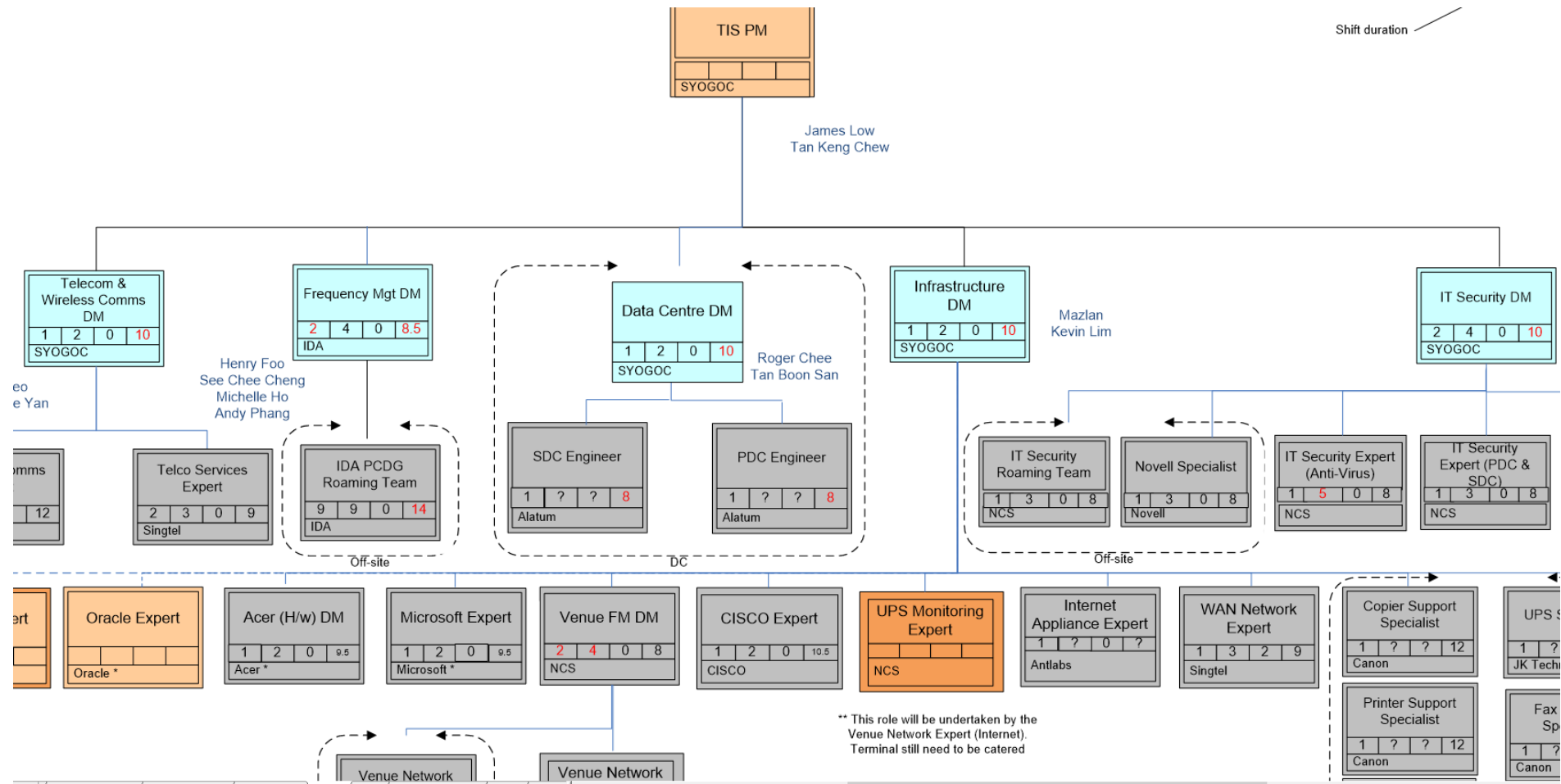
Incident Management



Example of Organizational Structure



Real Life Example



Roles – Junior Security Analyst

Junior Security Analysts provide a first line of defence against security threats in the SOC. They react to known alarms from the inputs into the data centre, and respond.

Major Tasks:

- ▶ Monitor the SIEM and Dashboards for possible clear, frequent incidents
- ▶ Respond to security incidents identified by SOC appliances
- ▶ Follow SOC policies, procedures, and documentation regarding events
- ▶ Review public threat bulletins, warnings, and advisories
- ▶ Escalate events to the appropriate group
- ▶ Communicate with 3rd parties

Major Skills:

- ▶ Familiarity with Windows and Linux operating systems
- ▶ Familiarity with Security Incident & Event Management Systems (SIEM)
- ▶ Familiarity with network perimeter technologies, like firewalls and proxies
- ▶ Familiarity with the operation of Intrusion Detection or Prevention Systems (IDS/IPS)
- ▶ An understanding of networking concepts (TCP/IP, network architecture and topology)



Roles – Senior Security Analyst

Senior Security Analysts provide a second line of defense against security threats in the SOC. They perform advanced real-time analysis of the inputs into the data center, and respond or route response.

Major Tasks:

- ▶ Monitor, manage, and analyse logs generated by SOC appliances and sources
- ▶ Respond to non typical security incidents identified by analyses
- ▶ Monitor the events and dashboards for possible abnormal behaviours
- ▶ Follow SOC policies, procedures, and documentation regarding events
- ▶ Review public threat bulletins, warnings, and advisories
- ▶ Route/Escalate events to the appropriate group

Major Skills:

- ▶ Familiarity with advanced events data analyses by different tools (Security Incident & Event Management Systems (SIEM), IDS/IPS, custom tools)
- ▶ Familiarity with Windows and Linux operating systems
- ▶ Familiarity with network perimeter technologies, like firewalls and proxies
- ▶ Familiarity with the operation of Intrusion Detection or Prevention Systems (IDS/IPS), NGFW
- ▶ The ability to analyze network traffic packets and protocols
- ▶ An understanding of networking concepts (TCP/IP, network architecture and topology)



Roles – Duty Manager

Major Tasks:

- ▶ Manage cross-functional SOC teams, which may include analysts, engineers, and supervisors, as well as outsourced specialists
- ▶ Ensure operational excellence, coordination, and quality throughout the SOC
- ▶ Serve as the formal business owner of information security processes and policies
- ▶ Serve as a leader in teams across functions, clients, and employees during SOC-related projects or incidents
- ▶ Manage coordination and escalation for critical incidents
- ▶ Develop, maintain, and present security analysis metrics for the SOC

Major Skills:

- ▶ The ability to manage and lead people
- ▶ Familiarity with operating enterprise security and threat management technology
- ▶ Familiarity with information security frameworks and general best practices
- ▶ An understanding of contractual, legal, or regulatory requirements like PCI DSS (depending on the environment)
- ▶ Experience developing detailed metrics, reporting, and presentations for audiences



Roles – Director/Supervisor

Major Tasks:

- ▶ Oversee a functional, shift-based, or geographical team in a SOC environment
- ▶ Prioritize, direct, and monitor workflow
- ▶ Coordinate and schedule coverage for the SOC, and assign resources to critical incidents or projects
- ▶ Monitor and meet triage, quality metrics, and service level agreements
- ▶ Provide coaching, feedback, training, and mentoring to SOC team members
- ▶ Manage the escalation of incidents, ensuring they're addressed by appropriate team members
- ▶ Help develop, implement, and maintain SOC policies, procedures, and processes

Major Skills:

- ▶ General technical knowledge and experience with security technologies and concepts
- ▶ Interpersonal skills for team building and coordination with other groups
- ▶ Project prioritization, management, decision-making and organizational skills
- ▶ Skilled at explaining complex technical issues to non-technical business employees
- ▶ Competencies similar to those of the members of the team being supervised, if not better



Procedures

General Operation Procedures

- Shift Start/Stop per role
- Ticketing system usage
- 3rd party communication
- Technical failures
- Human failures
- Escalation process
- Critical situations

Incident Related Procedures

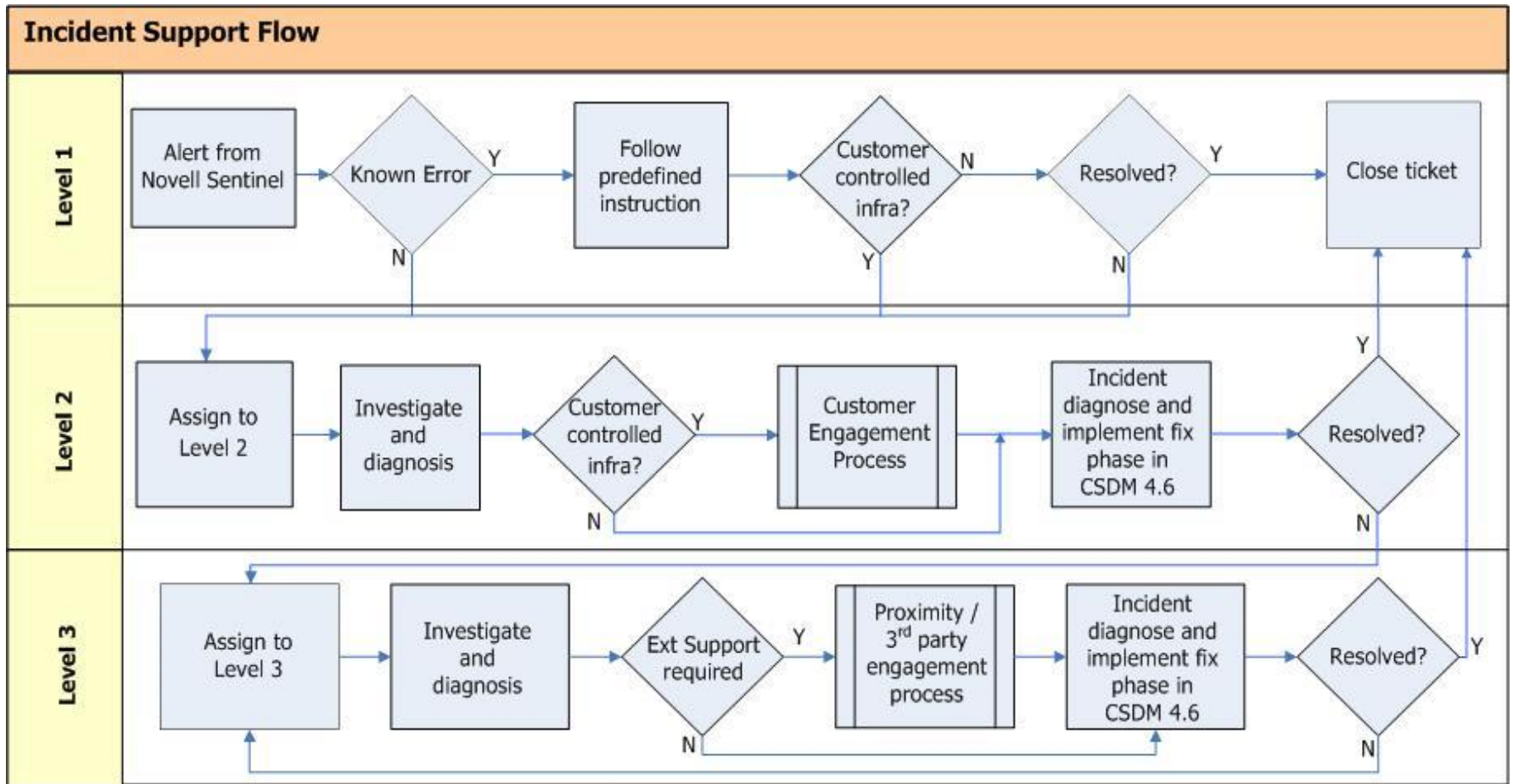
- General Incident Workflow
- Known Incident types procedure
- Unknown Incident type procedure
- Analyst regular procedures



INCIDENT RESPONSE



3 Levels Workflow Example



Incident Proc Template Phases

1. Preparation:

Establish contacts, define procedures, and gather information to save time during the incident handling

2. Identification:

Detect the incident, determine its scope, and involve the appropriate parties.

3. Containment:

Mitigate the attack's effects on the targeted environment.

4. Remediation

Take actions to remove the threat and avoid future incidents.

5. Recovery

Restore the system to normal operations.

6. Aftermath

Document the incident's details, discuss lessons learned, and adjust plans and defences.



Incident Proc Templates

- ▶ WormInfection
- ▶ WindowsIntrusion
- ▶ UnixLinuxIntrusionDetection
- ▶ DDOS
- ▶ MaliciousNetworkBehaviour
- ▶ Website-Defacement
- ▶ WindowsMalwareDetection
- ▶ Blackmail
- ▶ SmartphoneMalware
- ▶ SocialEngineering
- ▶ InformationLeakage
- ▶ Insiderabuse
- ▶ Phishing
- ▶ Scam
- ▶ Trademark infringement
- ▶ Ransomware
- ▶ Abusive content
- ▶ Information Gathering
- ▶ Availability
- ▶ Information Confidentiality
- ▶ Fraud
- ▶ Policy Violation
- ▶ Thief Incidents
- ▶ Other Security Incidents
- ▶ Notification template



Security Analysts Procedures

- ▶ Priority 5 events analyses
- ▶ Multiple failed logon attempts
- ▶ Port Security Violation
- ▶ Hosts without AV
- ▶ Network scans detected
- ▶ Multi vector attacker detection
- ▶ Honeypot triggered
- ▶ Hash trap triggered
- ▶ Hosts not on domain
- ▶ Tracing non standard processes per user
- ▶ 50+ Western and eastern AV checks for each process started ever
- ▶ Successful connections and/or mail accepted from dangerous IPs (Dangerous IP is IP reported as attacker by PA,Snort, Imperva)
- ▶ TSBANK Privileges Tracking
- ▶ Critical Assets access tracking
- ▶ Suspicious processes started
- ▶ Suspicious service installed
- ▶ New scheduled tasks installed
- ▶ User off hour login
- ▶ IDS Alarms
- ▶ Review and elimination of noise events (known, repeatable false positives)
- ▶ Tracing in live all administrators activity
- ▶ Verification of every web site accessed against Top 1 million sites (Alexa + Cisco)



Incident Management Key Points

1. Importance of Proactive Monitoring
2. Knowledge of Procedures
 - Incident Management
 - Communications
 - Change Management
 - Configuration Management
3. Role of the Crisis Situation Manager
4. SOC Concept where all the right people are in the same room
5. Communications to external stakeholders
6. Communications to venues
7. Roles & Responsibilities...not kids playing football
8. Objective is no impact to the operation so workarounds are proposed together with permanent solutions
9. Even in emergency situations, changes still need to follow the CM process
10. A new situation can cause stress (& panic). However a support team which has been trained to follow a process and methodically resolve problems has a better chance to succeed.
11. Move towards a no blame culture...responsibility but not finger pointing



Turin Internal Employee Inc

1. Internal employee has grabbed windows administrator account at ADMIN network
2. By multiple logins to few servers from atypical host he was discovered by our SIM solution
3. Arrested, interviewed
4. We got list of more than 90 people potentially involved
5. Potential resolutions:
 1. Disable all this accounts?
 2. Pray to god?
6. Dynamic change:
 1. Re-assign roles and process (2 person assigned only on suspicious accounts activity tracking)
 2. Prioritize any event related to those 90 suspicious people
 3. One click to disconnect them



Accreditation Incident

1. Internal employee tried to export face accreditation outside of Games network
2. He used encrypted zip file through FTransfer
3. Suspicious activity detected
4. Employee arrested
5. Challenges:
 1. AV does not report issue with encrypted files
 2. Content is not malicious



Corporate Incident

Incident information:

There was a FAILED logon attempt of user us001\configsoft from host BOMWKGTS006 [10.17.136.114] to server masd002a.US001.CORPORATION.NET [155.45.60.12] and username "admineric"

- Admineric is account discovered to be compromised in early august incident.
- Server masd002a.US001.CORPORATION.NET [155.45.60.12] is server stationed in US, managed by YYY for CORPORATION customer.
- us001\configsoft is username being used for patch tool named configsoft, having high privileges
- BOMWKGTS006 [10.97.136.114] is server stationed in India, Mumbai. It is used as a test server for "tat project" for a customer called ICICI.
- Logon attempt has been done using Logon mode 10, meaning that it is remote interactive logon attempt, used in RemoteDesktop protocol or remote session protocol.



Corporate Incident

UPDATE [15-Oct]

- **New incident:** The failed logon attempts were observed on the core switches in Philippines. The source IP is 10.96.154.172, which seems to be assigned to the workstation mc080uec registered to BUSTOS, Rodrigo [A403817] in Argentina. Investigation with Argentina CSO is going on.
- A set of clarifying questions has been sent to India forensics company in order to ensure full understanding of their future report and proactively enforce that all important information is included. This action has been done as some problems have been already identified in initial information provided.
- Tasso performed requested analyses of internal domain accounts. Result shows that there were no attacks against domain admin accounts. **This removes the risk of having compromised domain administrator accounts on internal domain.** Provided result details are:



DomainName	TargetUsername	exists	Dom admin
WW930.MY-IT-SOLUTIONS.NET	a132290	yes	no
WW930.MY-IT-SOLUTIONS.NET	a527314	yes	no
WW930.MY-IT-SOLUTIONS.NET	a539321	yes	no
WW930.MY-IT-SOLUTIONS.NET	de14650	yes	no



Best Practices

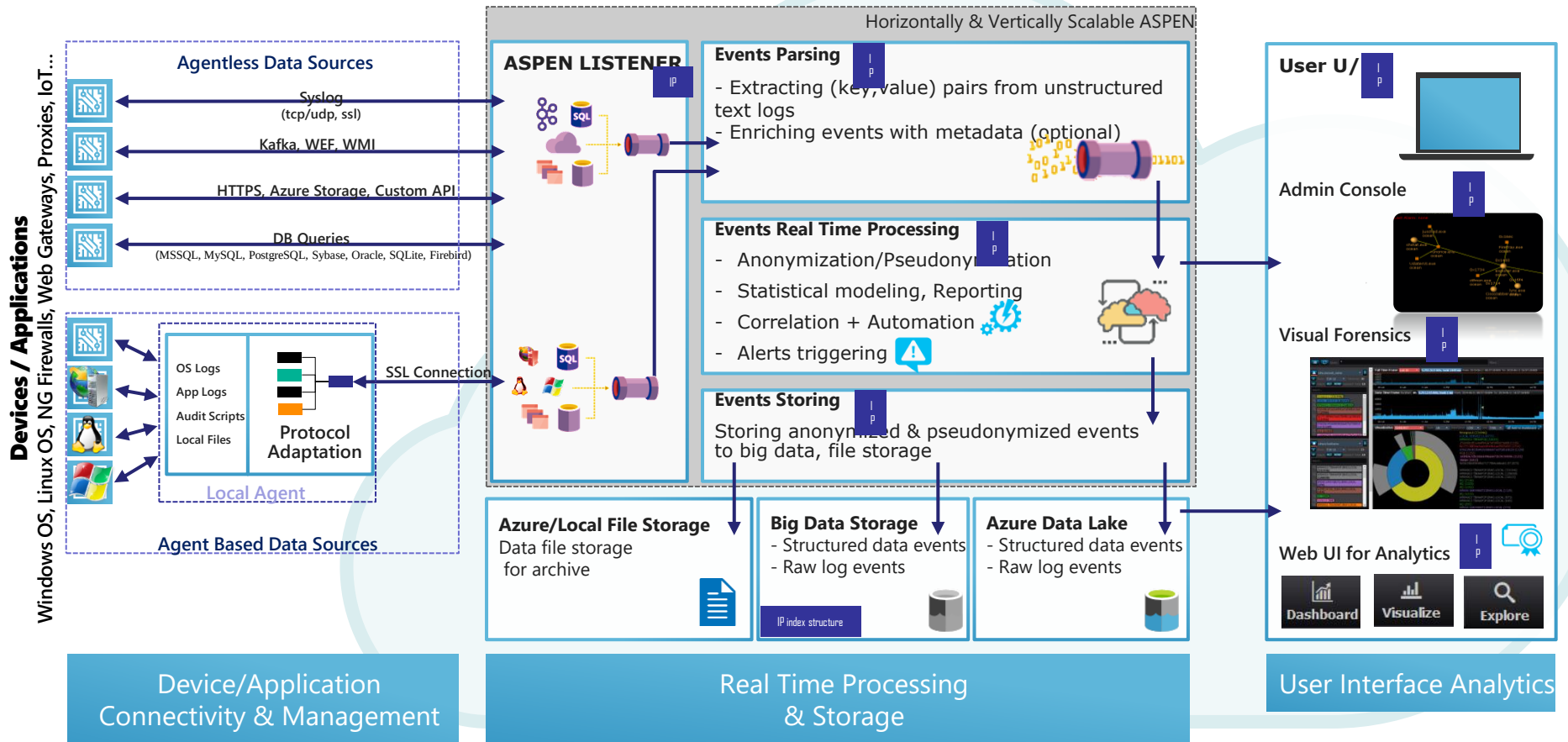
- » Scheduled Security audits with automatic reconfiguration of not properly configured devices
- » Real time security audits providing information about errors immediately after change has been made
- » Automation of all processes to avoid probability of human errors and increase team capability in supporting rapid deployment
- » Multiple antivirus solution can only guarantee full AV protection in high risk zones
- » Early deployment of all security controls ensures early detection of problems.



SECURITY MONITORING CHALLENGES



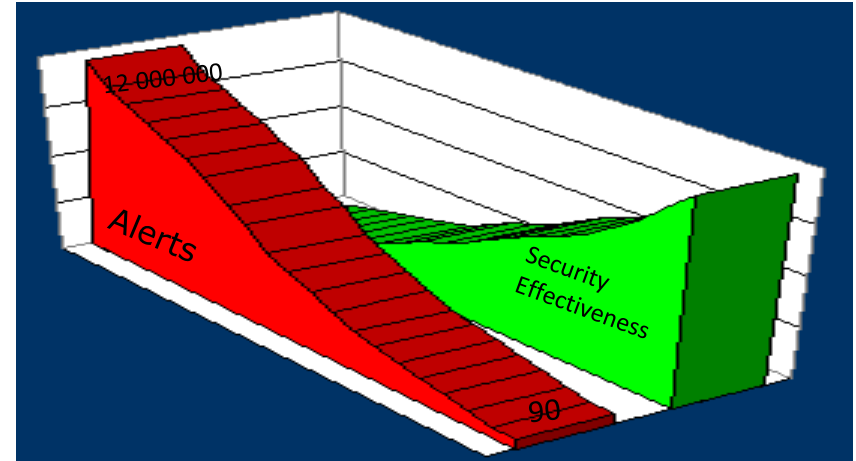
SIEM Big Picture



Proactive Crises Management

Incident Management Challenge:

- » How to understand over 20,000 security event types?
- » How to recognize real threats in 12,000,000 alerts per day?



Solution is Real Time Risk Management Technology:

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



Risk Scenarios

- 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:

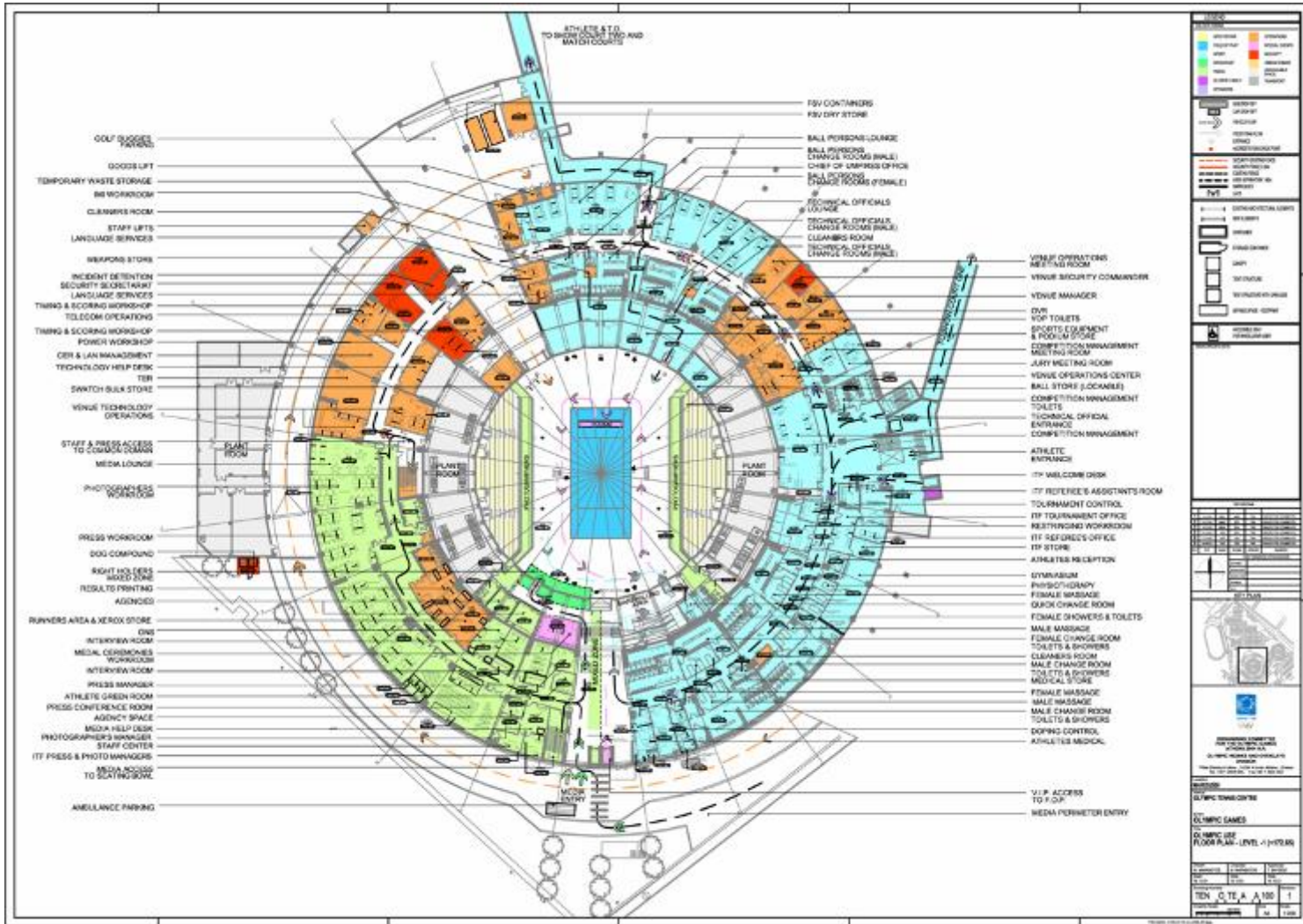
- » Break into the OVR server through OS vulnerability to modify data on the Scoreboard.

- Validation of the scenarios:

- » Technical Rehearsals
- » Penetration Testing
- » Periodic Security Reviews



Physical Security Risk Integration



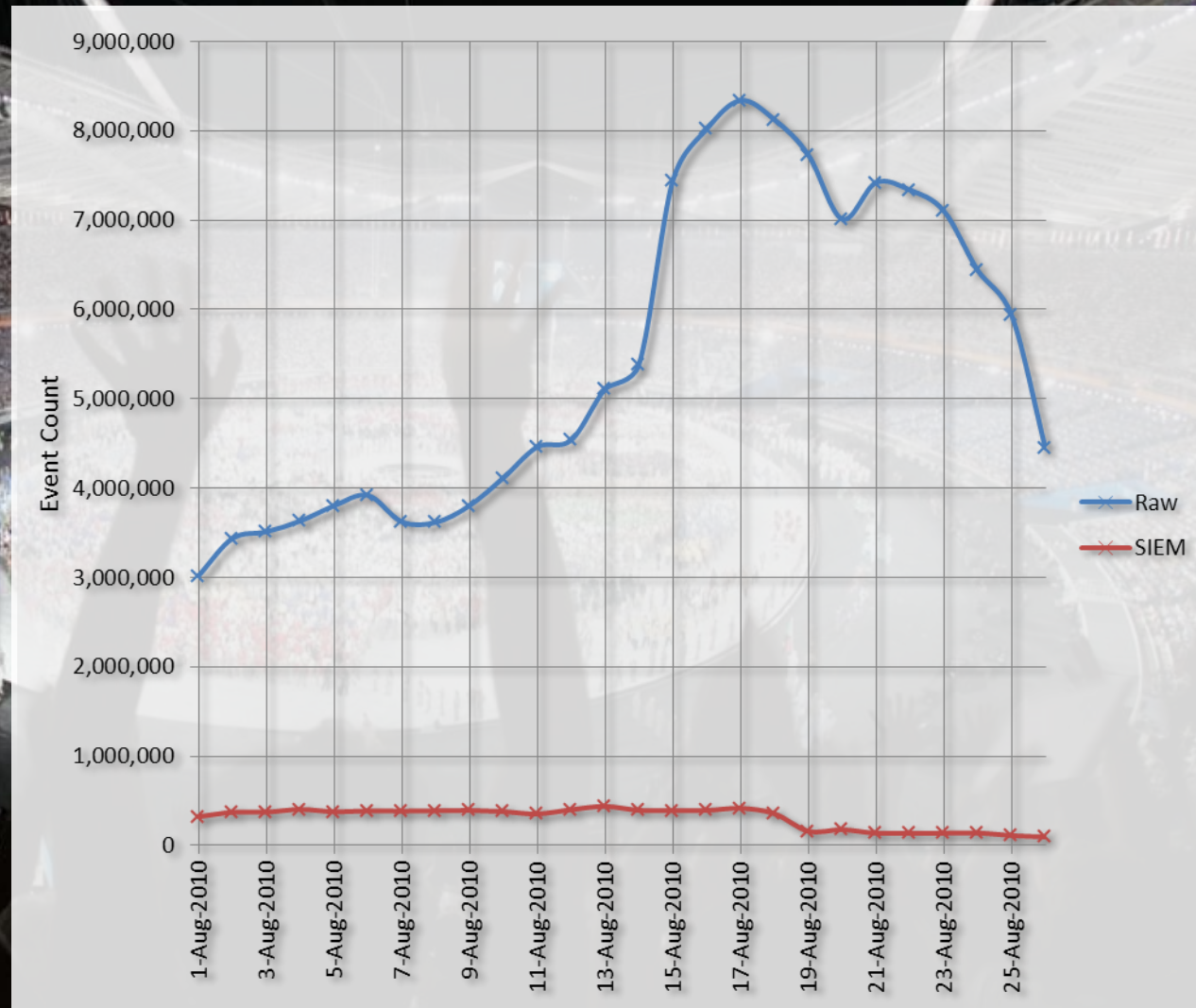
Correlation & Threat Hunting addressing information flood



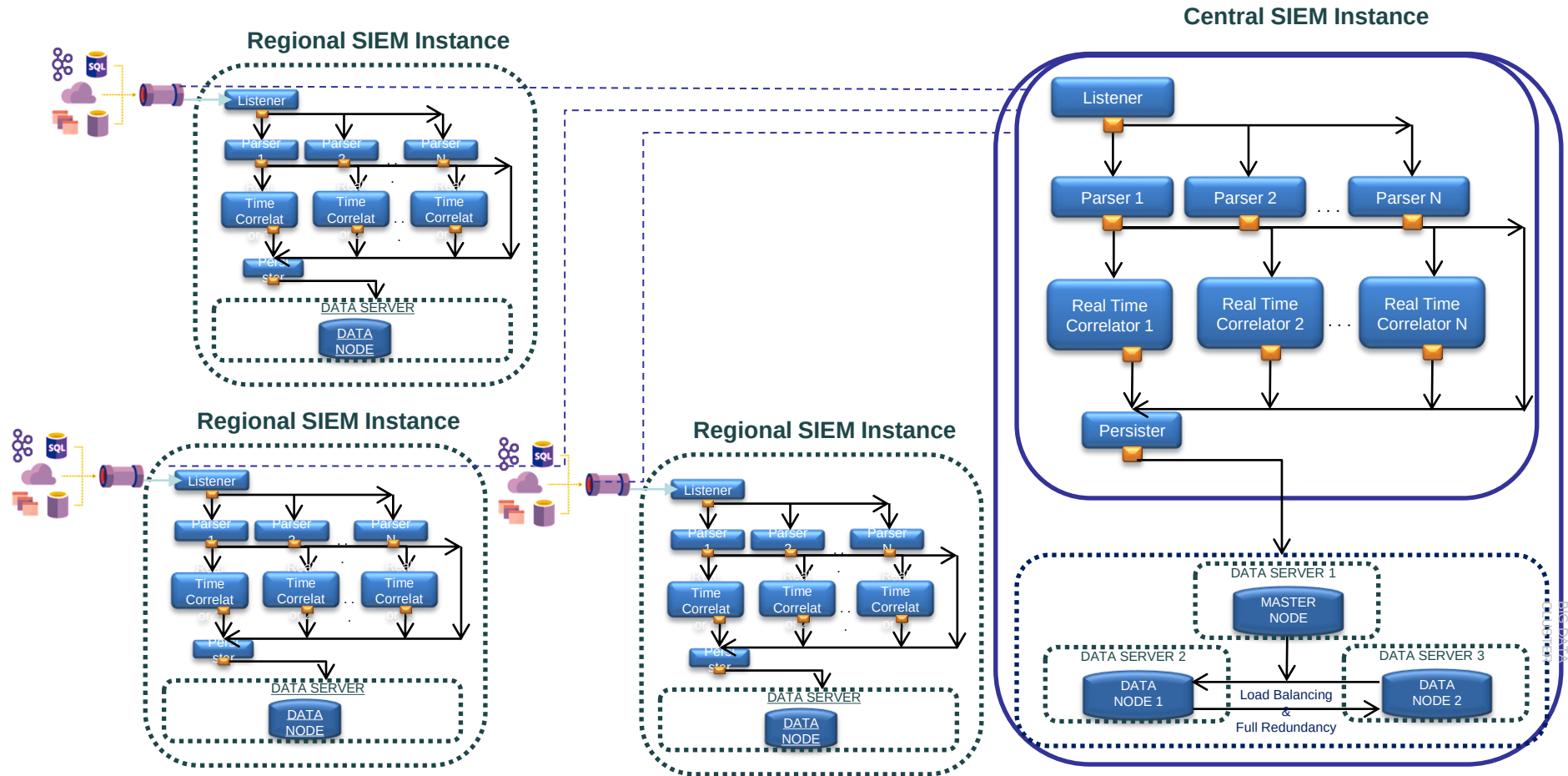
Singapore Statistics:

The >100% increase in raw event count did not increase the number of correlated events.

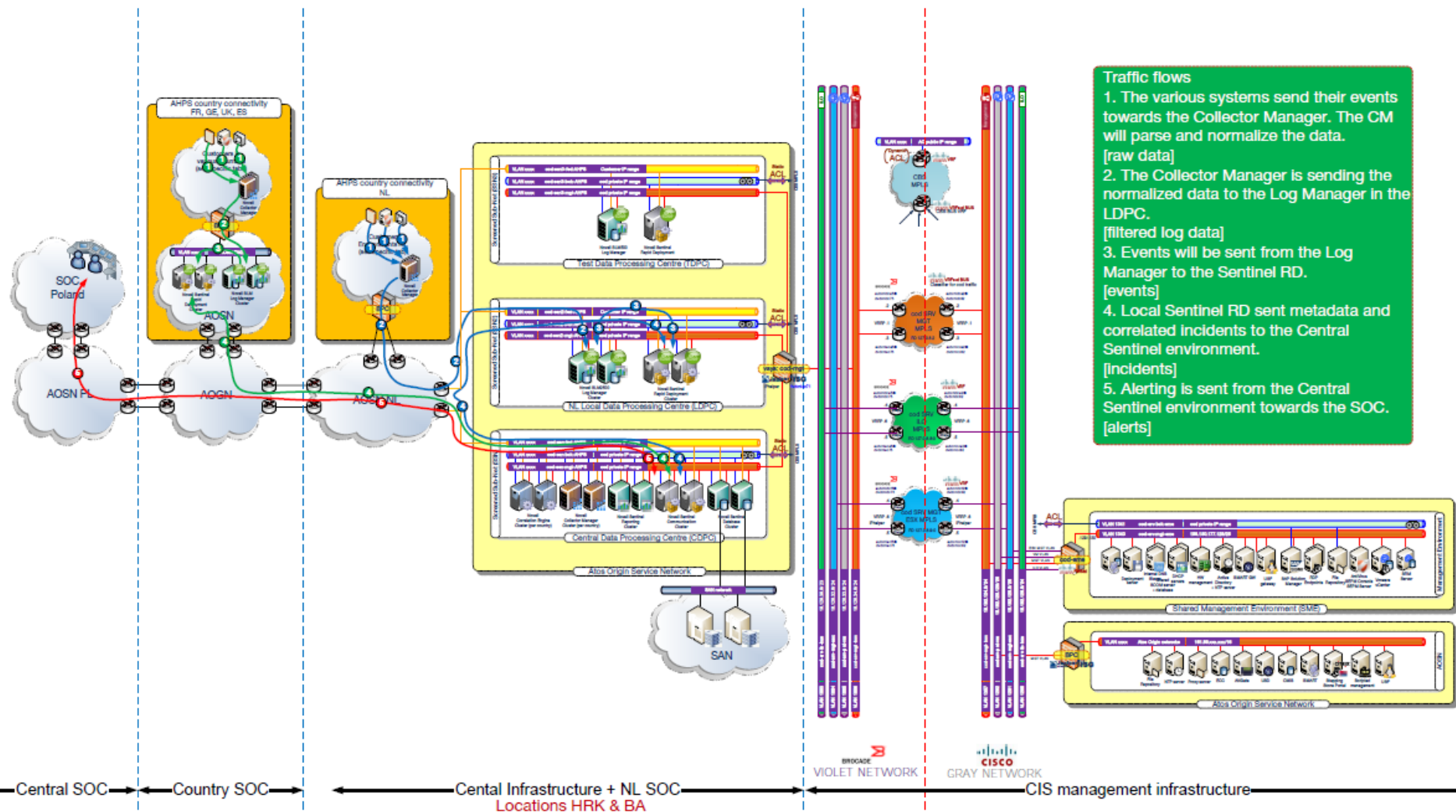
This approach drastically increases the processing capacity (EPS) of the SIEM solution.



Multi Regional SIEM Architecture



Round the Globe SoCs



Building experience on real incidents is very expensive and risky

BUILDING OPERATIONAL EXCELLENCE



TECHNICAL REHEARSALS



SOC Building Blocks

Processes

Ensure operational procedures are properly

- defined,
- trained and
- practiced

► People

- Ensure staff readiness through
 - Training and awareness
 - Professional skills
 - Stress test



Technology

Ensure technology excellence by

- End-to-end testing
- Fail over tests
- Automated KPI

we ensure SOC operational readiness excellence using tech rehearsals



Ensure Your Operational Level by Tech Rehearsals

- ▶ Technical Rehearsals are 'simulations' of the challenging, real life situations that allows testing of people, processes and technology.
- ▶ During these tests, some unexpected scenarios are triggered **interfering** with the regular real life tasks.
- ▶ TR scenarios are unknown to the SOC team and team has to react according to the operational policies and procedures they have been trained in.



Types of TR Scenarios

Table Top

- Usually used for very first time execution, with draft processes and technology partially deployed
- Simple scenarios used

Manual

- Performed periodically, as a targeted attack against some critical service
- Parallel simple scenarios executed in order to test basic human skills and supporting technology and processes

Automated

- Fully automated scenario execution performed regularly (e.g. on a weakly bases)
- Single attack vector scenarios exploring all possible ways of attack using that attack vector



Example 1: Email based OWA external link vector attack

- ▶ **Description:** External URL link should be sent by email to many employees to test if technology is properly blocking them and if people do not try to access external bad URL and do not provide their credentials.
- ▶ **How:** URL for OWA login page should be sent to random group of 100 employees using following methods:
 - Plain text email that contains `http://externalserver.tbd.com`
 - HTML email that contain HTML text `http://externalserver.tbd.com`
 - HTML email that contain external image link `http://externalserver.tbd.com/image.jpg`
 - HTML email with script opening external link after a click to a button
 - HTML email that is performing scrambling of source code in order to hide external links
 - BAR code URL link
- ▶ **Expected preventive control results:**
 - All link references should be removed by email gateway (100%)
 - Direct access should be blocked by web gateway
 - If link passes cleaning control, no employee should click on link (0%)
 - If employee click on link, he/she must not provide corporate credentials to fake OWA site
- ▶ **Expected monitoring control results:**
 - Large number of DNS requests toward never used domain detected
 - Large number of DNS request toward recently registered domain name detected
 - Employees should report URL in email
 - Web gateway should report unverified SSL web certificate site access attempt
 - BRO should report unverified SSL web certificate site accessed
- **Expected SOC reaction:**
 - SOC analyst should detect all alarms in less then 15 minutes
 - SOC analyst should identify all affected assets and control weaknesses, if any
 - SOC DM should create incident with appropriate priority based on the predefined policy
 - SOC analyst should block access from attacker IPs to all services



Example 1: Email based OWA external link vector attack

- ▶ **Description:** External URL link should be sent by mail to many employees to test if technology is properly blocking them and if people do not try to access external bad URL and do not provide their credentials.
- ▶ **How:** URL for OWA login page should be sent to random group of 100 employees using following methods:

- Plain text email that contains `http://externalserver.tbd.com`
- HTML email that contain HTML text `http://externalserver.tbd.com`
- HTML email that contain external image link `http://externalserver.tbd.com/image.jpg`
- HTML email with script opening external link after button click
- HTML email that is performing script tambling of source code in order to hide external links
- BAR code URL link

Results:

> 100 emails passed preventive controls

> 15 corporate credentials obtained, including even administrator credentials 😞

▶ Expected preventive controls

- All link references should be removed by email gateway (100%)
 - Direct access should be blocked by web gateway
 - If link passes cleaning control, no employee should be allowed to click on it. If employee must not provide credentials. A site must not provide credentials.
- ## ▶ Expected monitoring controls
- Large number of DNS requests toward never used domain detected
 - Large number of DNS request toward recently registered domain name detected
 - Employees should report URL in email
 - Web gateway should report unverified SSL web certificate site access attempt
 - BRO should report unverified SSL web certificate site accessed

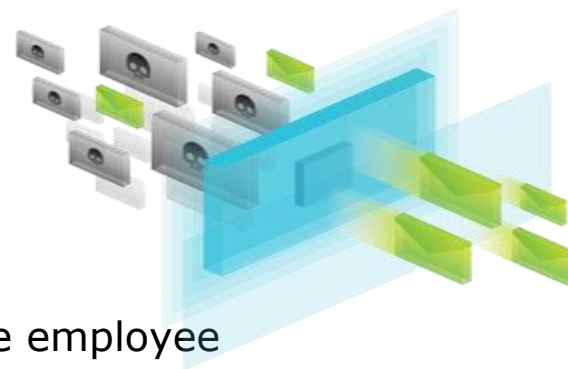
Expected SOC reaction:

- SOC analyst should detect all alarms in less than 15 minutes
- SOC analyst should identify all affected assets and controls weaknesses, if any
- SOC DM should create incident with appropriate priority based on the predefined policy
- SOC analyst should block access from attacker IPs to all services



Example 2: Known malware in email

- ▶ Can you guess how many ways are there to send a malware through e-mail, so employee can open it by double-click?
- ▶ If corporation has following controls:
 - Last version of MS Exchange with AV,
 - Last version of McAfee email GW,
 - ClamAV at MTA,
 - Last generation NG Firewall
- ▶ How many of infected emails should pass through to corporate employee
- ▶ How many of blocked emails will be reported as “infected”?



Example 2: Automated malware cleaning in emails KPI

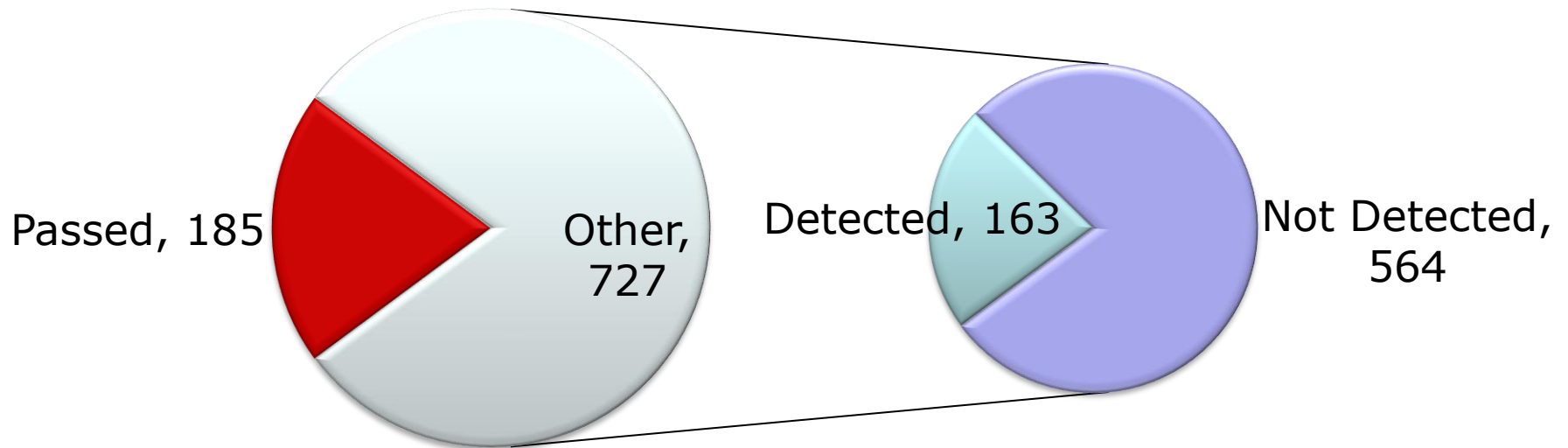
- ▶ **Description:** Use all possible ways of sending EICAR malware using email and measure number of files passed, blocked or detected
- ▶ **How:** Prepare all possible format of executable files with EICAR malware string to be sent by email:
 - Directly attached executable files
 - Archived executable files attached
 - Files archived with password
- ▶ **Expected preventive control results:**
 - NGFW should reject mail communication when malware attachment is sent (100%)
 - All passed mail attachments must be removed by
 - Mail gateway AV
 - ClamAV on Unix MTA in DMZ,
 - Exchange AV
 - Endpoint AV
- ▶ **Expected monitoring control results:**
 - NGWF should report on every mail rejected
 - AV instances should report every malware removal (100%)
 - ASPEN correlation should detect large number of malware email send from same IP
 - ASPEN correlation should detect large number of malware email send from same domain
 - ASPEN correlation should detect large number of alarms related to same SourceIP
- **Expected SOC reaction:**
 - SOC analyst should detect all alarms in less than 15 minutes
 - SOC analyst should identify all affected assets and **controls weaknesses**, if any
 - SOC DM should create incident with appropriate priority based on the predefined policy
 - SOC analyst should block access from attacker IPs to all services



1st Run Results

Infected emails

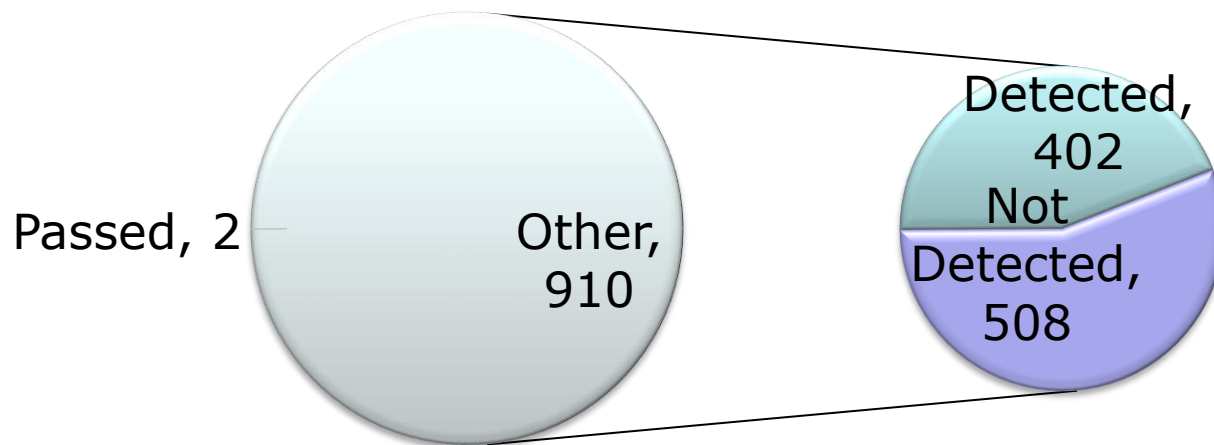
■ Passed ■ Detected ■ Not Detected



2nd Run results, 2 months later:

Infected emails

■ Passed ■ Detected ■ Not Detected



Technical Rehearsal (1)

► Objectives

- Test the team in an environment which is more intensive than the games, to ensure operational excellence during the Olympic Games

► Scope

- Simulate competition results the 3 busiest days of the the Olympic Games
- End-to-end systems. All venues and systems in use
- Operations polices, procedures and support tools must be in place
- Implement “abnormal” scenarios to complement “normal” operations
- Observe the behavior of the operations support team.
 - Do they know their procedures?
 - Do they follow them?
 - Do they communicate properly?
 - Do they know how to resolve problems?
 - Can they deal with stress?



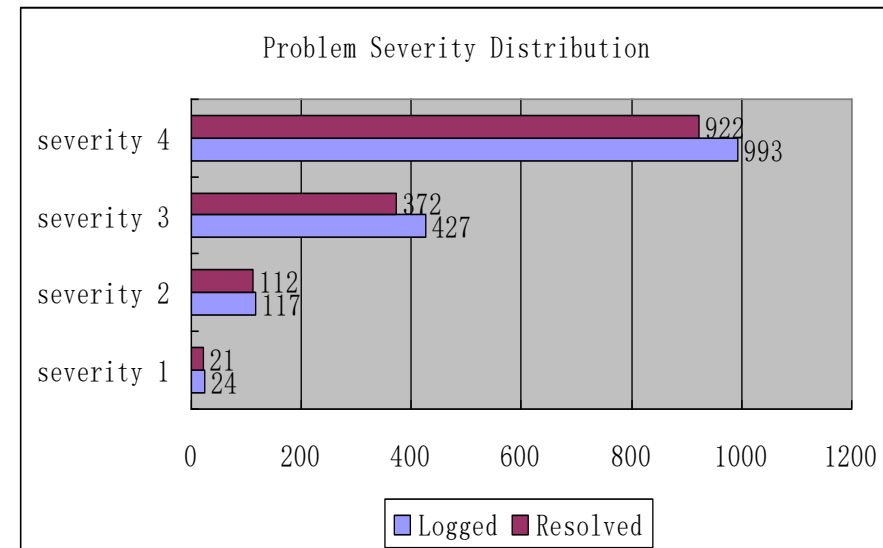
Technical Rehearsal (2)

► Critical Services Rehearsals

- Simulated days 5,8 & 13 of the Olympic Games
- 33 Competition and 6 Non-Competition venues involved
- 2546 People involved from 16 different organizations
- 78 Technical Rehearsal Officials
- 480 Scenarios executed
- 2554 Incidents logged
- 2298 Incidents resolved

► Outcomes

- Improved knowledge of procedures
- Improved teamwork and spirit
- Improved monitoring in TOC & venues
- Improved Communication
- Improved ability to resolve high severity incidents
- Identified conflicts between control and flexibility
- Identified critical areas of operational weakness
- Identified system issues not found during testing



Operational Readiness - others

► Disaster Recovery Rehearsals

- Rehearse the Disaster Recovery Plan for:
 - Disaster in Data Centre
 - Disaster in Technology Operations Centre
 - 2 DR exercises performed
 - Target Maximum Acceptable Outage Duration of 2 hours
- Lessons Learned
 - Scheduling is difficult, plan early
 - Procedures must be written and checked before starting exercise

► Training & Table Tops

- E-Learning, 17 courses
- Hands On, 4 courses
- Presentation: 8 courses on venue, 15 courses on central facility
- Table Tops: > 40 sessions
- Lessons Learned
 - A mix of training is required (presentation, e-learning, tabletops)
 - Training must be compulsory – block access to services if not completed
 - Table Tops are the most effective form of training



Disaster Recovery

2 DRR2 Objectives and Scope Definition

Primary goal for DRR2 is to ensure the Disaster Recovery Plan and main failover procedures can be executed smoothly during Games time operations in case of a disaster declaration. Following the outcomes from DRR1, modifications will be carried out in PDC and SDC to properly support the failover, and relevant procedures modified and finalized. Together with this will be address all issues and gaps discovered during DRR1 exercise.

2.1 Objectives

The main objectives of the Disaster Recovery Exercise Two are:

- Validate the critical PDC services can be recovered from alternate facility (SDC) **within target Service Level of two hours**
- Validate the critical TOC command services can be recovered from alternate facilities (ATC) **within target Service Level of two hours**
- Validate that the alternative sites (SDC and ATC) installation and configuration is implemented as per Games Time Solution design and their are able to operate as substitution of the primary sites (PDC and TOC);
- Verify main failover checklists (PDC to SDC and TOC to ATC) and failover procedures for unitary services;
- Validate services and system power off and power on steps at PDC for all critical services in scope
- Validate steps and measure times for IDS services failback to PDC including SDC data restoring at PDC
- To increase staff awareness of implemented disaster recovery strategy;
- Hands-on training for Technology Help Desk Team in managing disaster or critical situations.



Disaster Recovery

2.2 Rehearsal Two Scenario

Only one scenario will be simulated during DRR2: Disaster is declared at VHQ facilities and both TOC and PDC need to be evacuated to alternative facilities. This type of scenario will be "pro-active" disaster declaration – because of high risk or life threat / equipment damage situation services will be discontinued from PDC and systems must be shut down before starting failover to SDC. Main exercise phases will be:

- Stopping PDC services and systems (stop services for end users, stop interfaces, verify last data replication between PDC and SDC, power down PDC systems)
- TOC Failover to ATC is executed following DR Plan and TOC to ATC failover procedure
- When ATC is declared operational support team will execute critical services failover to SDC following DR Plan and PDC to SDC failover procedure. SDC will be declared as operational and failover will be complete.
- SDC services will be prepared for failback. For IDS services SDC databases will be archived and prepared for data failover to PDC
- At the end of the exercise all services in scope will be restored from PDC. For IDS services data failback from SDC will be executed at PDC

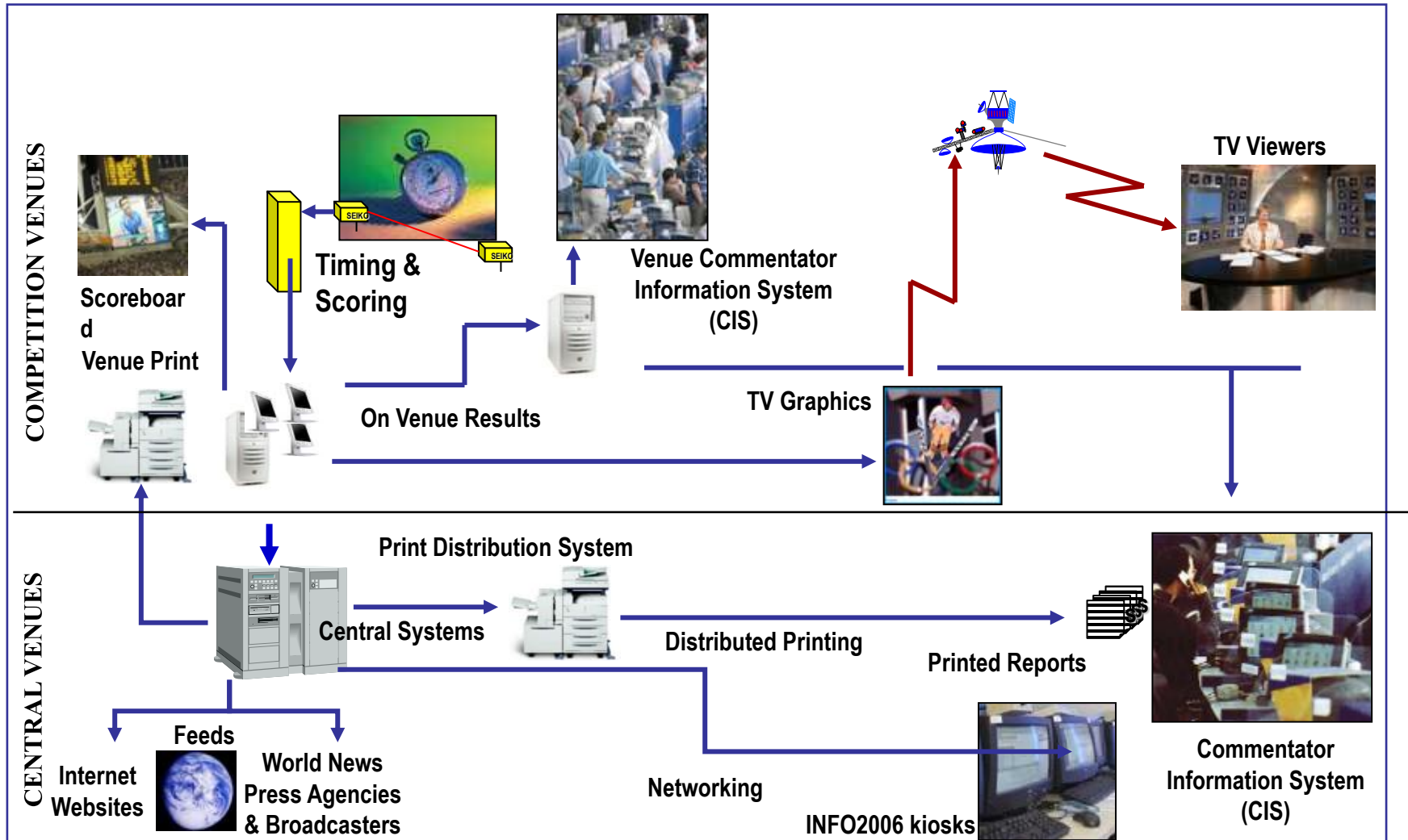


- » BOOST PERFORMANCE
- » REDUCE COST
- » INCREASE AGILITY
- » ENHANCE CRM
- » SHORTEN TIME TO MARKET
- » DRIVE INNOVATION
- » IMPROVE EFFICIENCY
- » INCREASE ADAPTIV



Beijing 2008 Olympics Security the Ultimate Challenge

Information Diffusion Systems



Olympics Security Task

Protect the Games IT infrastructure from any undesired and/or uncontrolled phenomena which can impact any parts of the result chain and associated services

Timing and Scoring



Real time applications
(Scoreboard)

**Availability
Integrity**

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...)

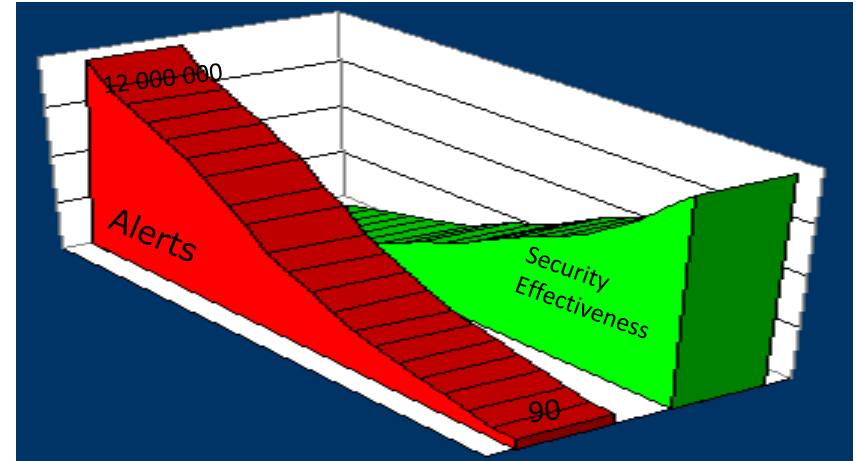
**Confidentiality
Integrity**



Proactive Crises Management

Incident Management Challenge:

- » How to understand over 20,000 security event types?
- » How to recognize real threats in 12,000,000 alerts per day?

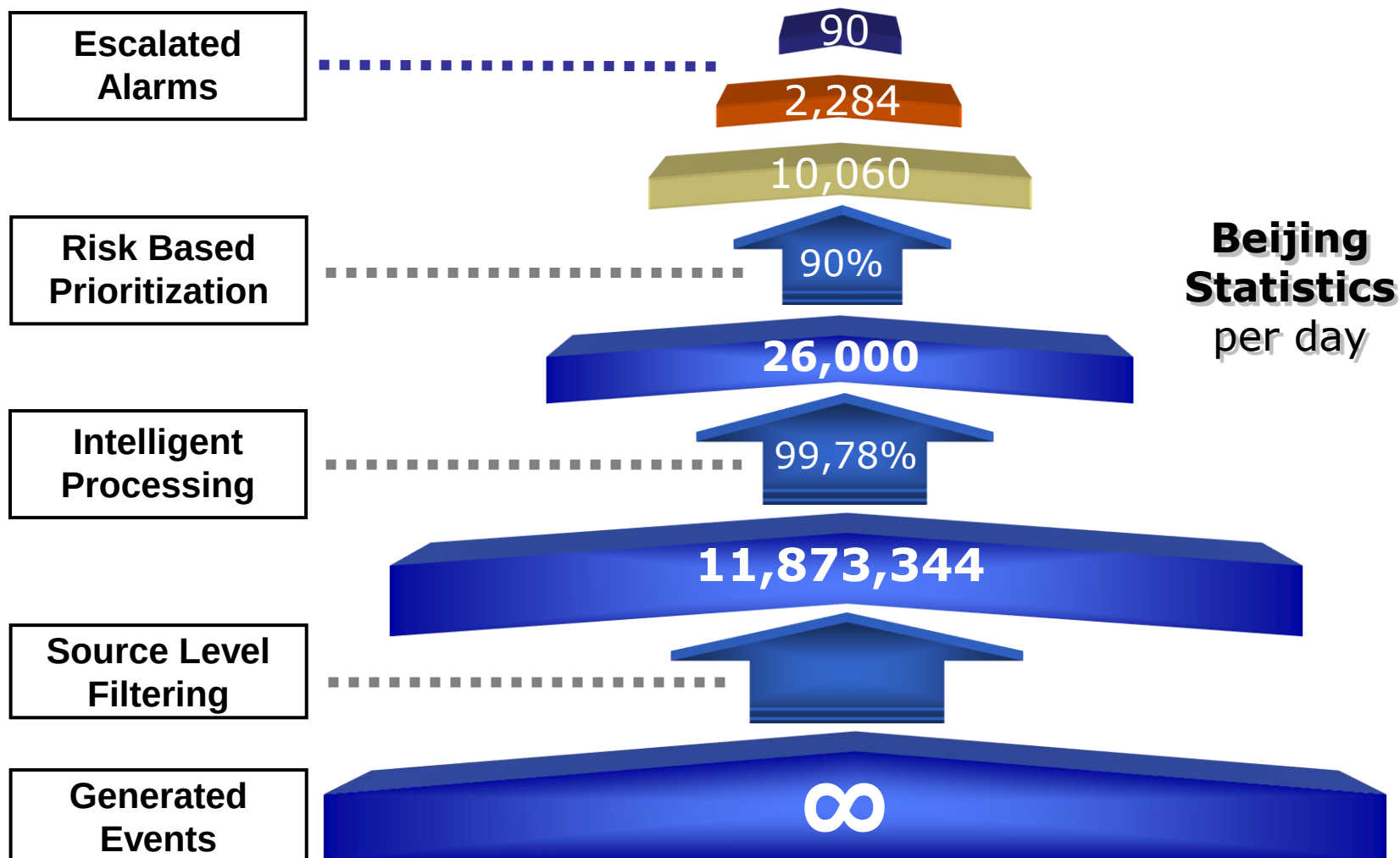


Solution is Real Time Risk Management Technology:

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

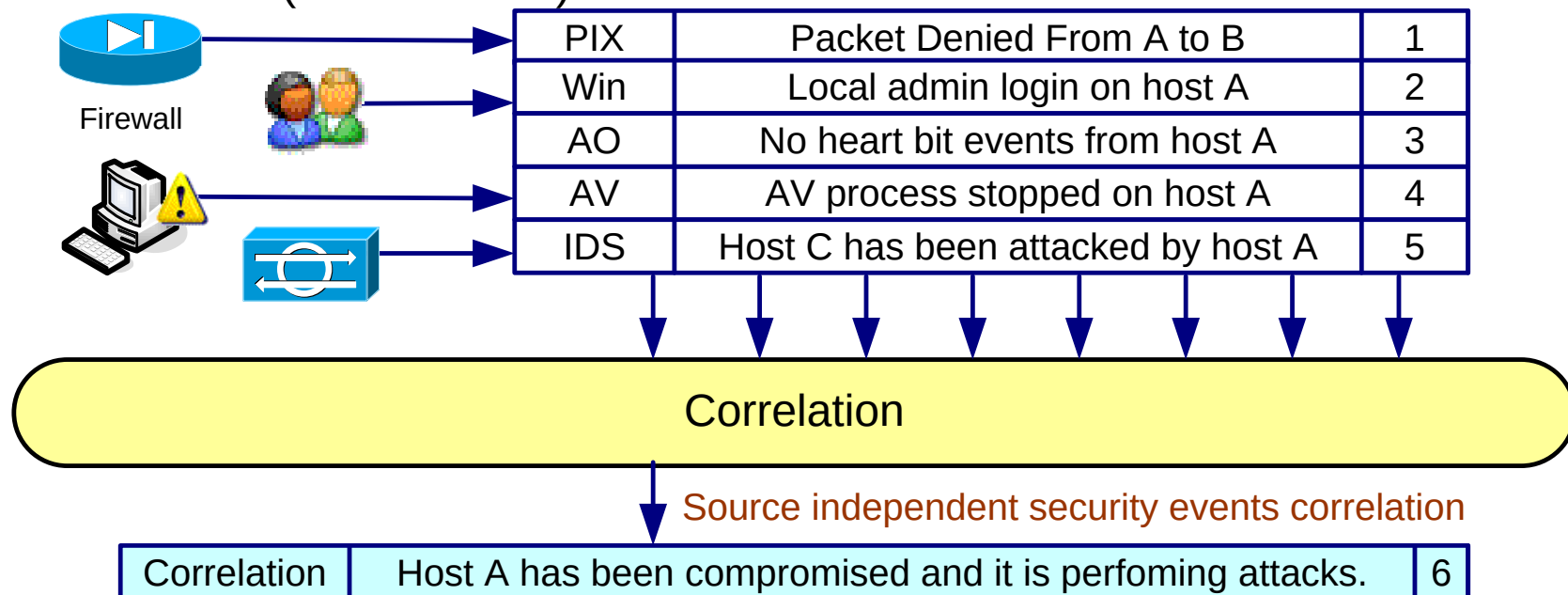


Security Information Reduction



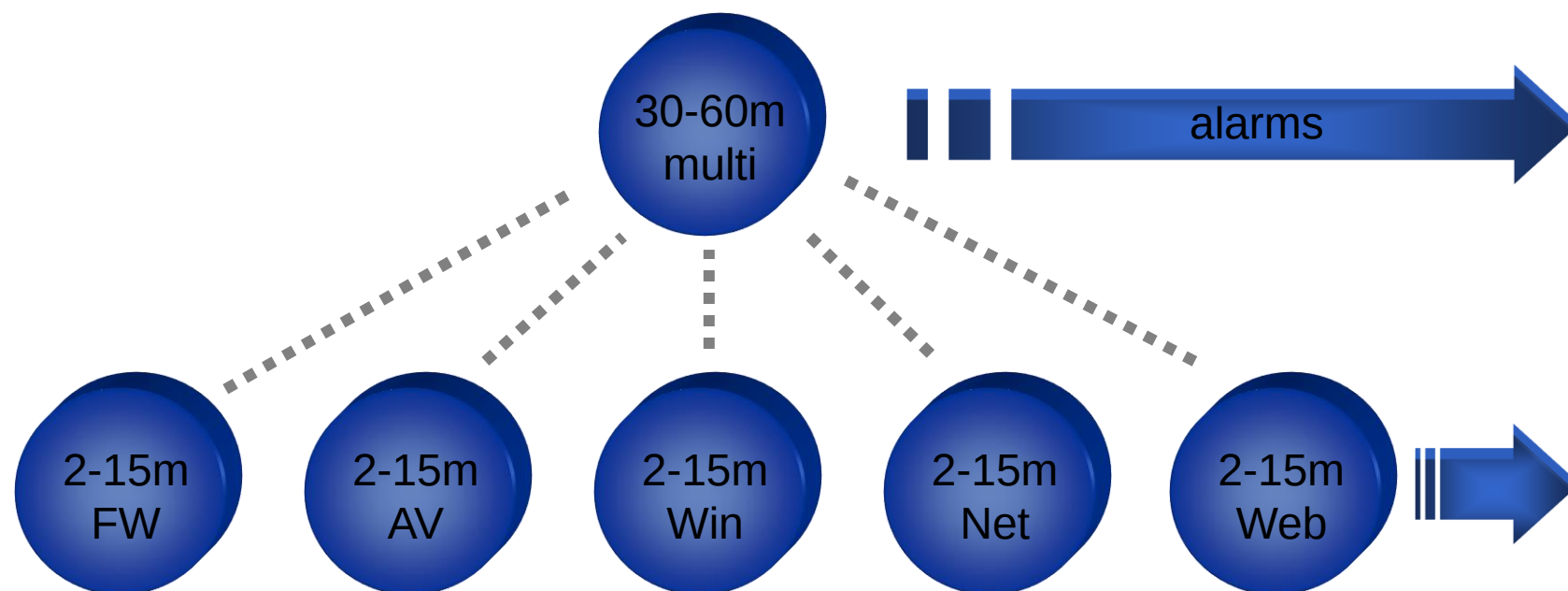
Intelligent Event Processing Multilevel Correlation

- Any event parameter can be used for correlation. Same event is processed through different correlation rules simultaneously
- Any non IT information can be embedded (Physical security information for example)
- Multilevel correlation enables distributed processing and fast (2-15min) and slow (30min-60min) correlation



Distributed & Multilevel Processing

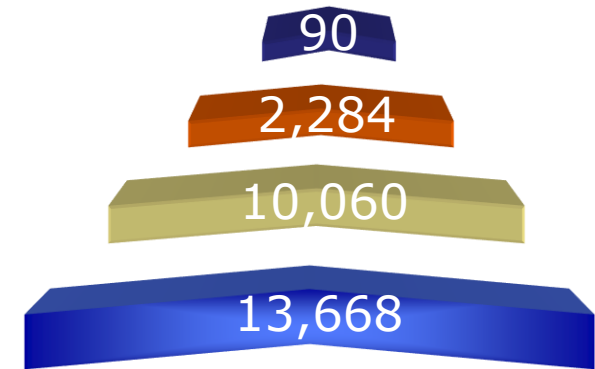
- ▶ Distributed Processing –enables real time data processing in any enterprise environment. This scalable solution can be adopted to any environment size.
- ▶ Multilevel Correlation – enables early multisource detection of both fast (2-15min) and slow (30min-60min) attacks.



Business Risk Based Prioritization

Risk assessment based event prioritization –
which risks/events to focus on?

- ▶ Static Prioritization – an event prioritization level is being determined by predefined rules
- ▶ Dynamic prioritization – an event prioritization based on parameters that can be changed during time
- ▶ Examples:
 - Event prioritization based on the sport events time schedule (we care more about venues with live events going on)
 - Event prioritization based on a number of events correlated
 - Event prioritization based on a number of sources correlated



Real Time Security Audits

Security Compliance Check

Immediately after any configuration change has been made, automatic security audit is performed ensuring security compliance.

ReportedBy	SummaryInfo	CommonParam...	Source	Category
src-n1as48n-013	59.121.2.13: configuration changed on switch 59.121.2.13 by user yangaiping con...	59.121.2.13	Audit	ConfChange
src-n1as24n-032	59.121.2.32: configuration changed on switch 59.121.2.32 by user yangaiping con...	59.121.2.32	Audit	ConfChange
fts-n1as24n-020	60.121.2.20: configuration changed on switch 60.121.2.20 by user zouming conne...	60.121.2.20	Audit	ConfChange
pcf-n1dis3n-001	pcf-n1dis3n-001: 1 switch dos hardening not applied	PCF-N1DIS3N-001	Audit	SwitchConfigRisk
pcf-n1dis3n-001	pcf-n1dis3n-001: 1 s1 management: port security not deployed	PCF-N1DIS3N-001	Audit	SwitchConfigRisk
pcf-n1dis3n-001	pcf-n1dis3n-001: 1 s1 management: port security not deployed	PCF-N1DIS3N-001	Audit	SwitchConfigRisk
pcf-n1dis3n-001	pcf-n1dis3n-001: 1 s1 management: port security not deployed	PCF-N1DIS3N-001	Audit	SwitchConfigRisk
pcf-n1dis3n-001	pcf-n1dis3n-001: 1 s1 management: port security not deployed	PCF-N1DIS3N-001	Audit	SwitchConfigRisk
pcf-n1dis3n-001	pcf-n1dis3n-001: 1 dhcp service enabled	PCF-N1DIS3N-001	Audit	SwitchConfigRisk
pcf-n1dis3n-001	27.121.1.1: configuration changed on switch 27.121.1.1 by user yangaiping conne...	27.121.1.1	Audit	ConfChange
src-n1as48n-013	src-n1as48n-013: 2 h1 newauto: port security not deployed	SRC-N1AS48N-013	Audit	SwitchConfigRisk
src-n1as48n-013	src-n1as48n-013: 1 d1 ids: port security not deployed	SRC-N1AS48N-013	Audit	SwitchConfigRisk
src-n1as24n-032	src-n1as24n-032: 2 c2 cis: port security not deployed	SRC-N1AS24N-032	Audit	SwitchConfigRisk
src-n1as24n-032	src-n1as24n-032: 2 c2 cis: port security not deployed	SRC-N1AS24N-032	Audit	SwitchConfigRisk
src-n1as24n-032	src-n1as24n-032: 2 c2 cis: port security not deployed	SRC-N1AS24N-032	Audit	SwitchConfigRisk
nis-n1as48n-029	41.121.2.29: verification failed on ip:41.11.12.68 (mac:001c.25c9.14fb) on port:fa0/...	41.11.12.68	Audit	Verification
nis-n1as48n-029	41.121.2.29: verification failed on ip:41.11.12.67 (mac:001c.25c8.a316) on port:fa0/...	41.11.12.67	Audit	Verification
yt-n1dis1n-003	50.121.1.3: configuration changed on switch 50.121.1.3 by user saukilo connectin...	50.121.1.3	Audit	ConfChange

Actions performed:

- generate risk event and assign priority related to business risk
- perform predefined automatic action (port shutdown?, service startup, accounts removed...)

No misconfiguration is allowed, no matter if it is caused by human mistake or human “misbehavior”.



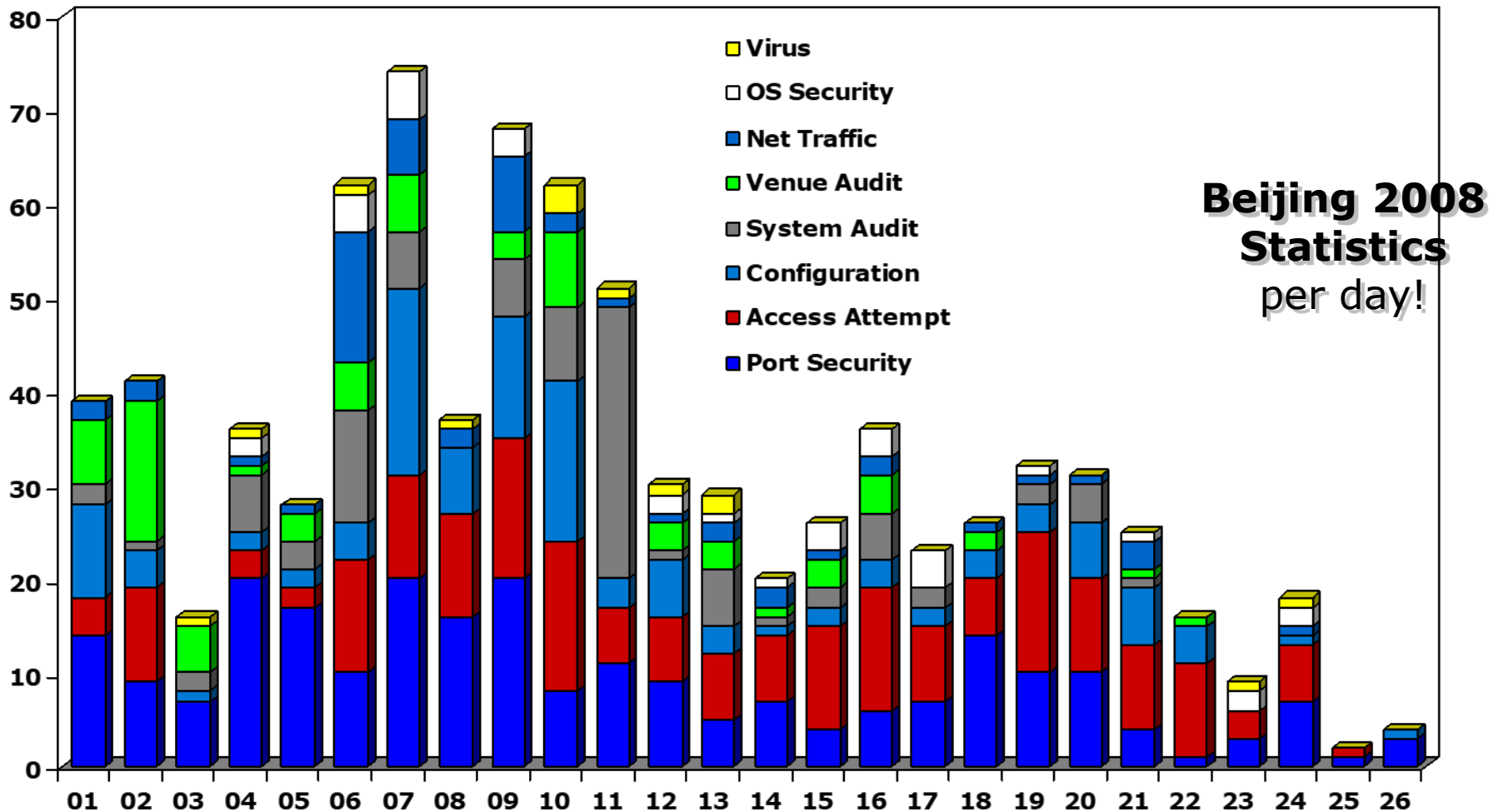
Social strategy

Potential attackers recognizing

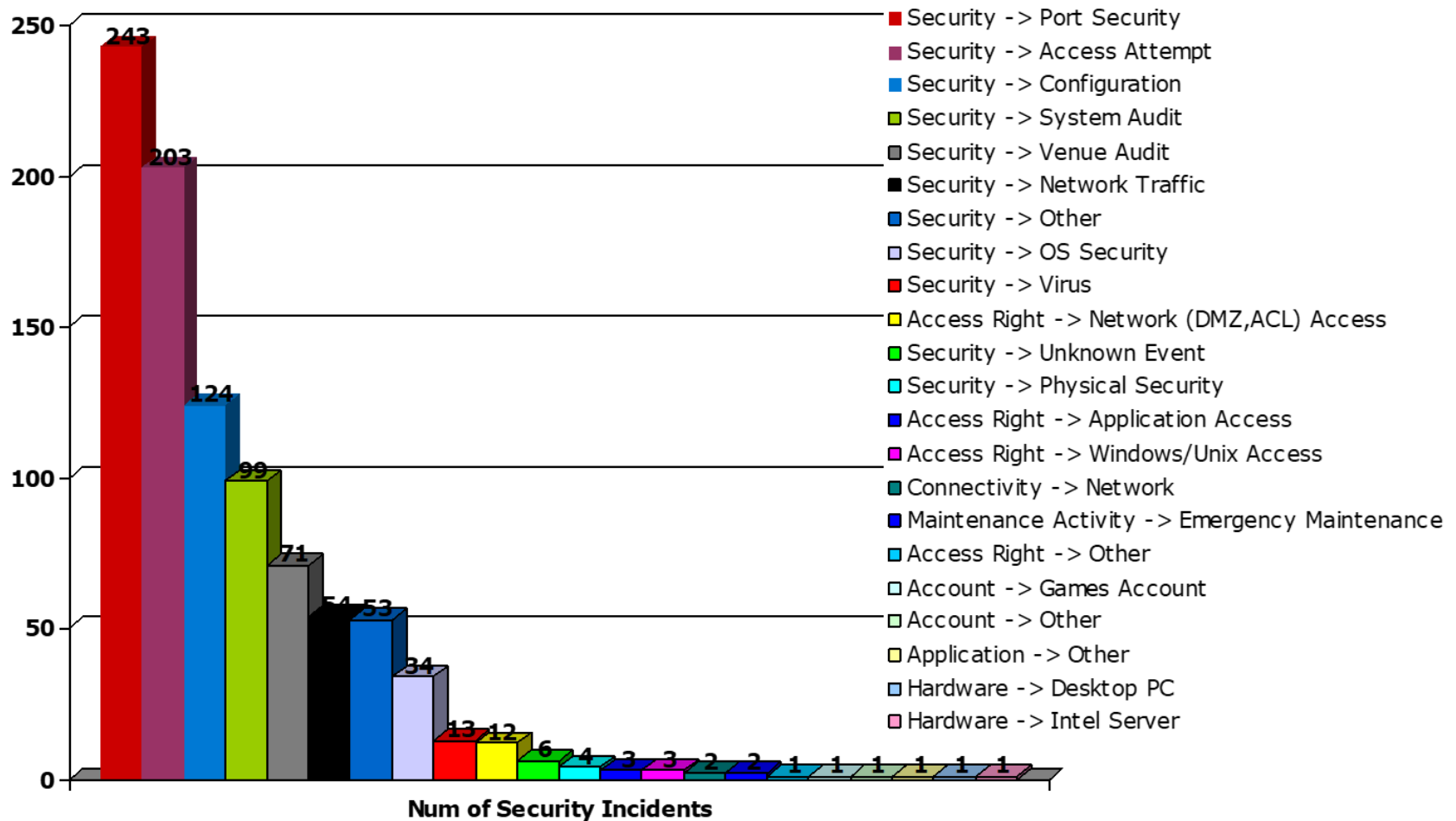
- ▶ During Games time there is high number of volunteers, sport men, journalists, third party employees and additional risks
 - Allow hidden access to some public kiosks without any real impact
 - Track any attempt to access command prompt and immediately perform people arrest of attacker
- ▶ Using honey pots we enable proactive detection of any potential IT attackers.



Security Calls Per Day Statistics



Security Calls Per Profile Statistics



Summary – Beijing 2008 Results

During 17 days of competition :

201,846,847 filtered events

443,745 correlated events

1,527 critical alarms

about 500 incidents

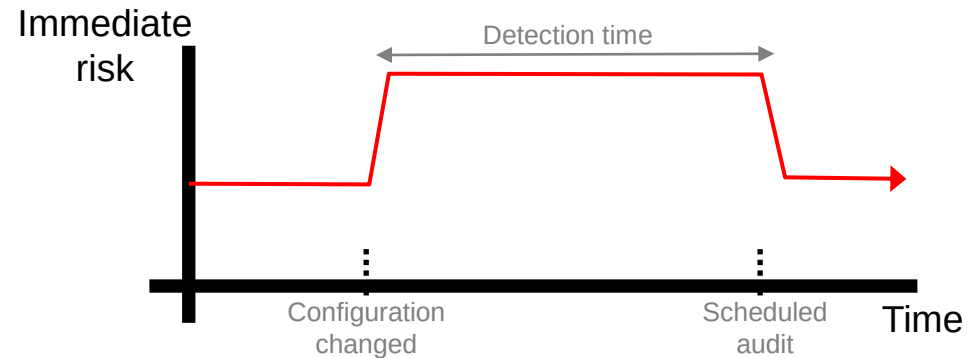
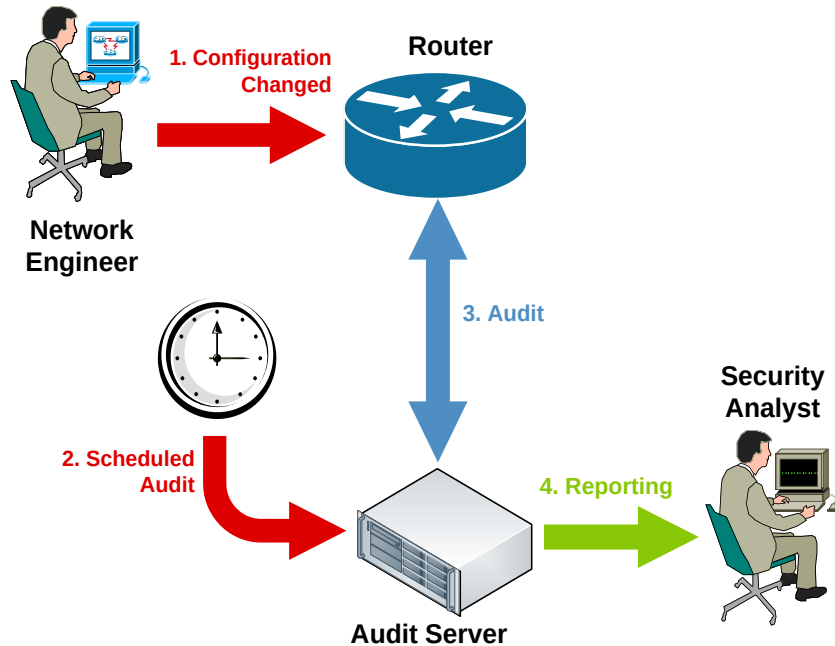
NO IMPACT ON BUSINESS



AUDITING



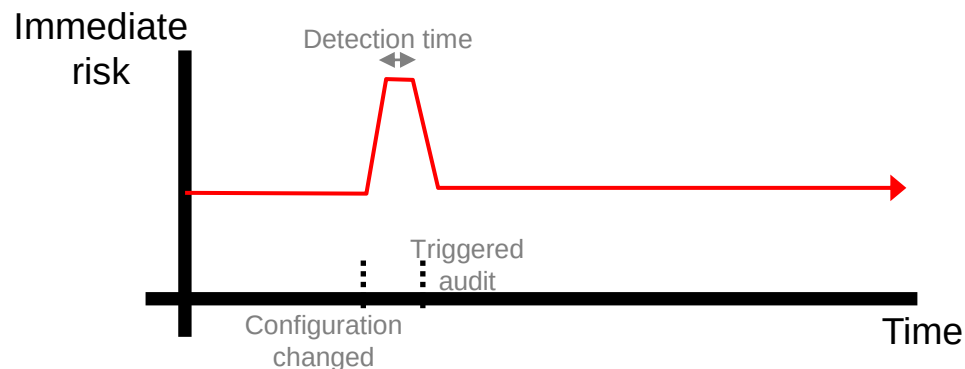
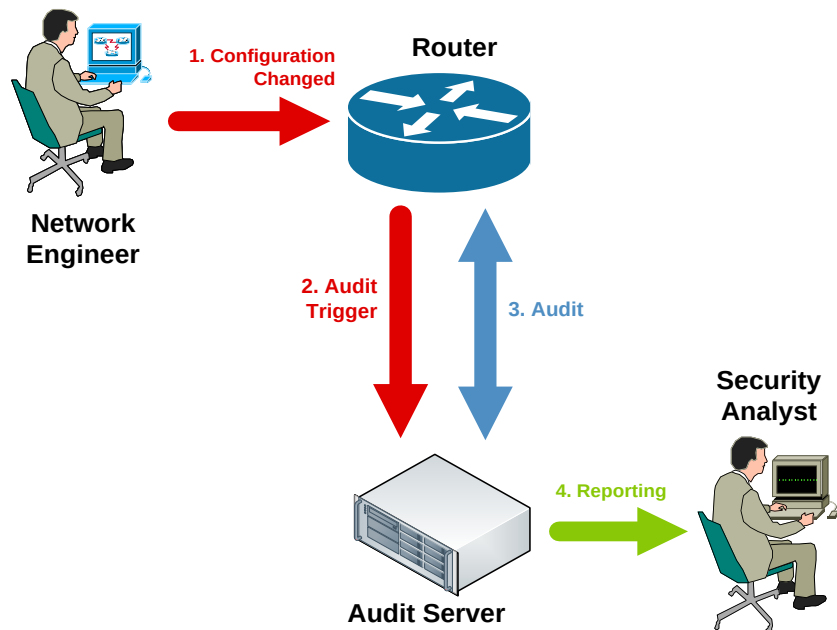
Scheduled Auditing



- » Scheduled audits important for measuring security posture, however, cannot quickly detect non-compliance.
- » Long detection time increases risk exposure.
- » Predictable unless schedule changes regularly; results maybe not true reflection of security posture
- » Examples, USB enabling, local administrator account creation, non-Games devices, etc.



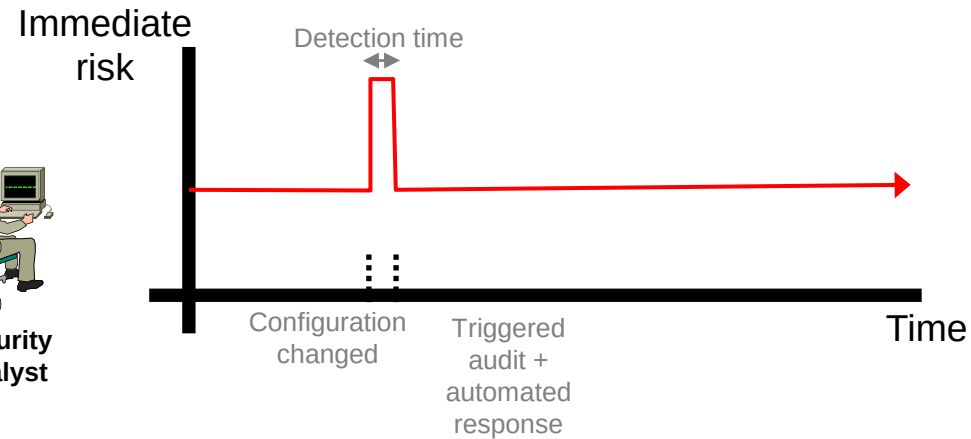
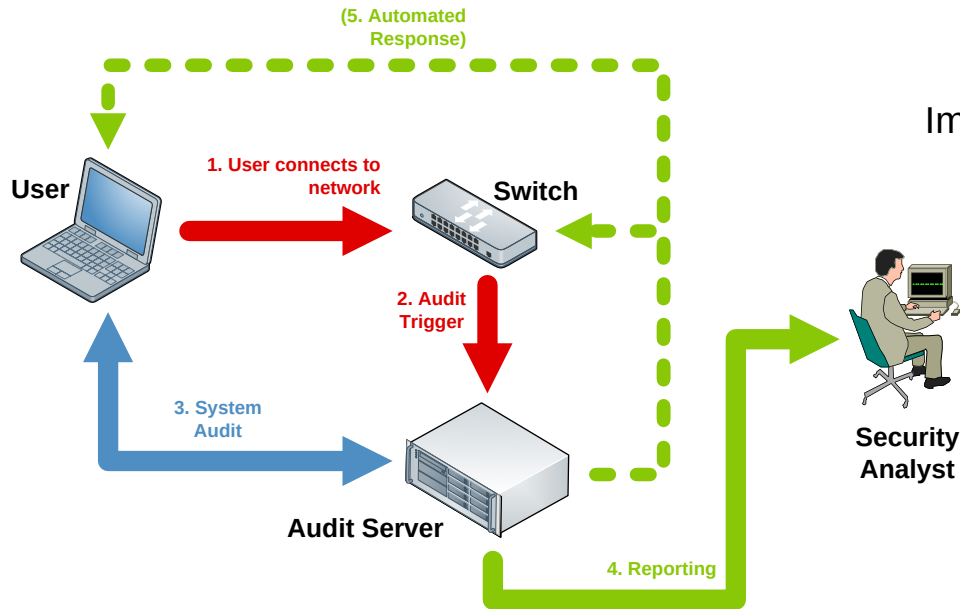
Triggered Auditing



- » Reduced risk exposure since mitigation response time is drastically reduced.
- » Seamless integration with SIEM solution with customisable severity level based on risk assessment.
- » Triggers can be defined for a variety of devices and environments – Windows, UNIX, Cisco, etc.



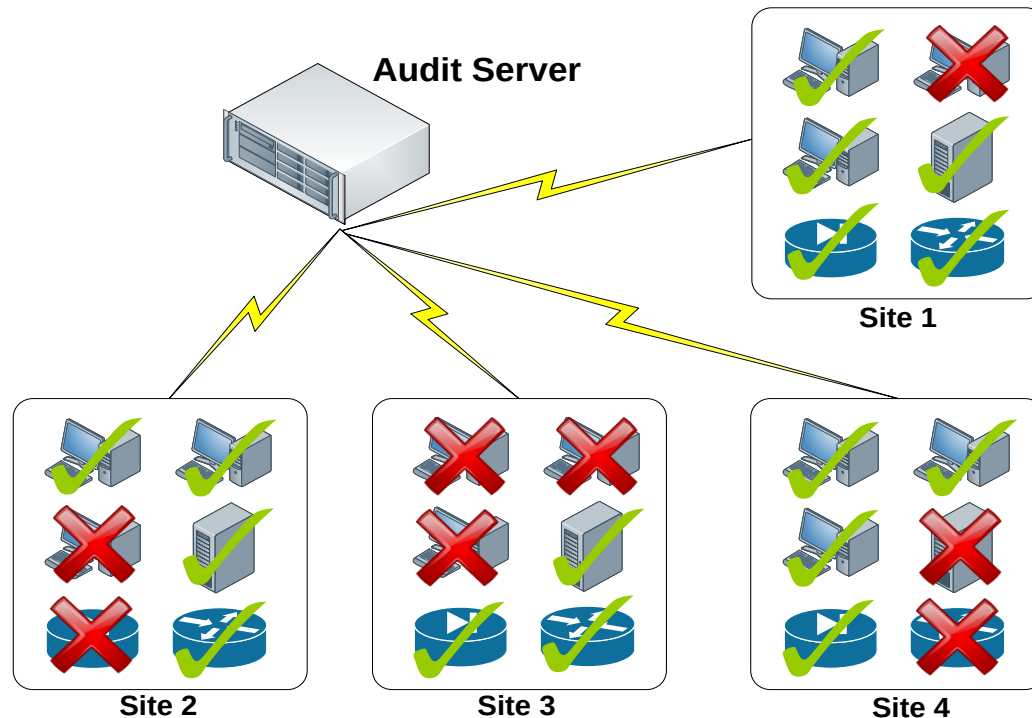
Automated Response



- » If an issue is found following real-time auditing, on-site engineer may take time to respond to event and take action.
- » Real-time audit will report events to SITAR and assign a severity level based on business risk.
- » Unique audit solution can initiate “automated responses”.
- » Audits able to take corrective actions based on results.



Compliance



- » Manual checking of device configurations on a large IT infrastructure – also prone to human error.
- » SITAR can provide **automated auditing** and **corrective actions** to expedite and ensure compliance with pre-defined regulatory standards.
- » Both **customisable** and **scalable** to demands from the business and security.



System: OS Security Audit

- *Verify that domain clients meet and adhere to required security baseline. Ability to take remedial actions when non-compliance found.*
- Checks:
 - Security services (AV, event forwarding agent) are running and configured correctly
 - OS hardening compliance
 - Rogue or unauthorised local administrator privileges
- Reports:
 - Risks and non-compliance
 - Informational messages
 - Integration with SIEM solution
 - Fully customisable events and severities.
- Actions:
 - Initiate remedial action if non-compliance found.
- When:
 - Scheduled
 - Triggered



System: Network Adapter Audit

- *Monitor for unauthorised or incorrectly configured network adapters.*
- Checks:
 - Enumerate all network adapters and settings into database
 - Compare results against pre-defined whitelist.
 - Changes to MAC or IP addresses.
 - Changes to network interfaces
- Reports:
 - Risks and non-compliance
 - Running snapshot of all connected devices and settings
 - Whitelisted/blacklisted network adapters
- Actions:
 - Disable/uninstall rogue network adapters.
 - Change network adapter settings
- When:
 - Scheduled
 - Triggered



Infrastructure: Active Directory Audit and Identity Management.

- *Perform detailed auditing and tracking of Active Directory users, groups and computer objects, leverage results for Asset and Identity Management purposes.*
- Checks:
 - User object configuration, account usage.
 - Group membership whitelisting/blacklisting.
 - GPO's applied on computer objects.
- Reports:
 - User account risks
 - Unauthorised group membership
 - GPO deployment
 - Near-realtime snapshot of Active Directory.
 - Asset and identity management
- Actions:
 - Disable unauthorised/unused user accounts.
 - Assign group memberships as per identity management matrix.
 - Apply GPO.
- When:
 - Scheduled
 - Triggered



Infrastructure: Network Device Audit

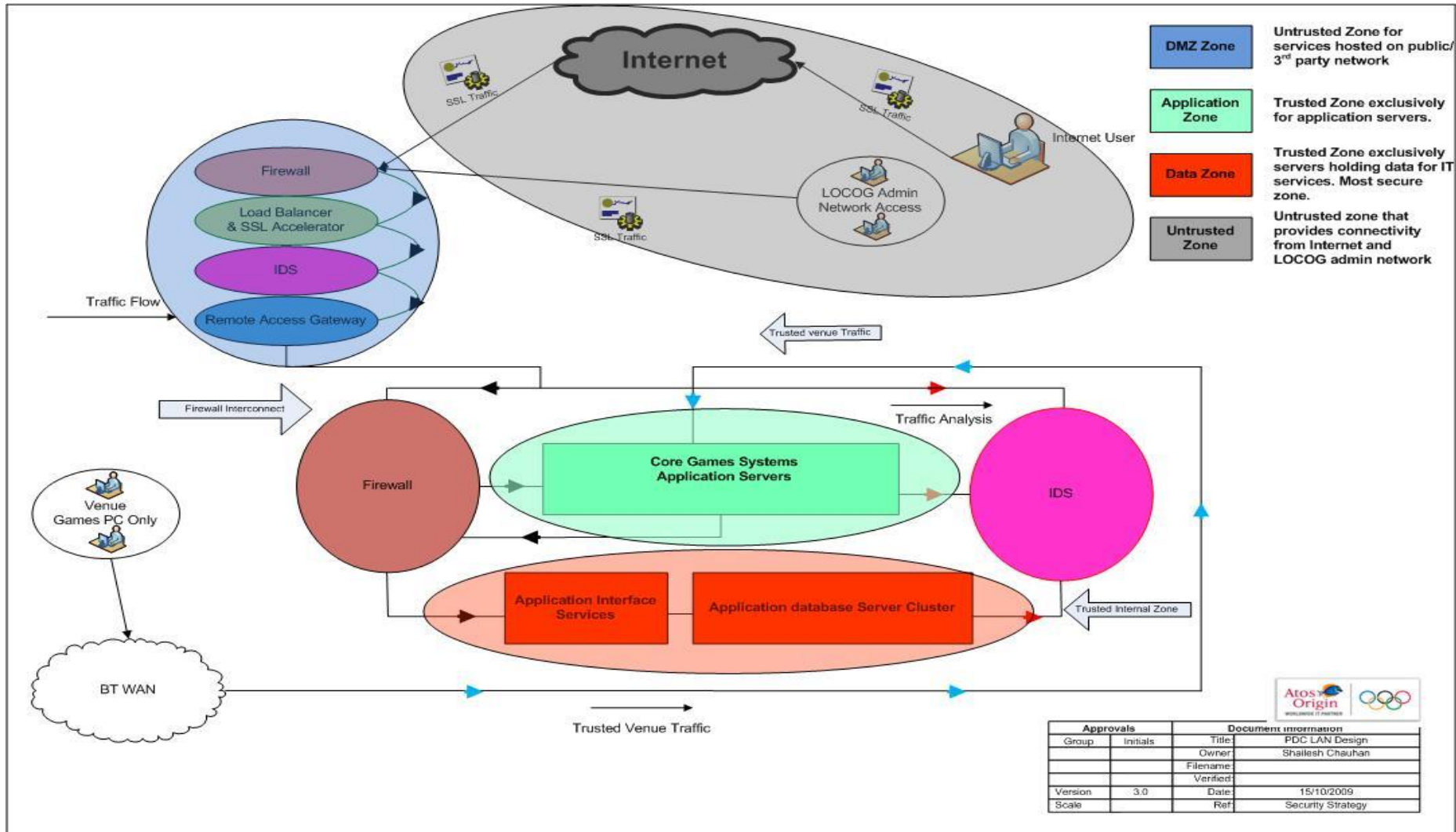
- *Ensure consistent and secure configuration of network devices.*
- Checks:
 - Ensure compliance to security baseline and hardening.
 - Network device discovery based on IP addressing conventions
 - Erroneous or malicious actions by network administrators.
- Reports:
 - Configuration risks.
 - Integration with SIEM solution.
 - Fully customizable events and severities.
- Actions:
 - Automated configuration of network devices to enforce compliance.
- When:
 - Scheduled
 - Triggered

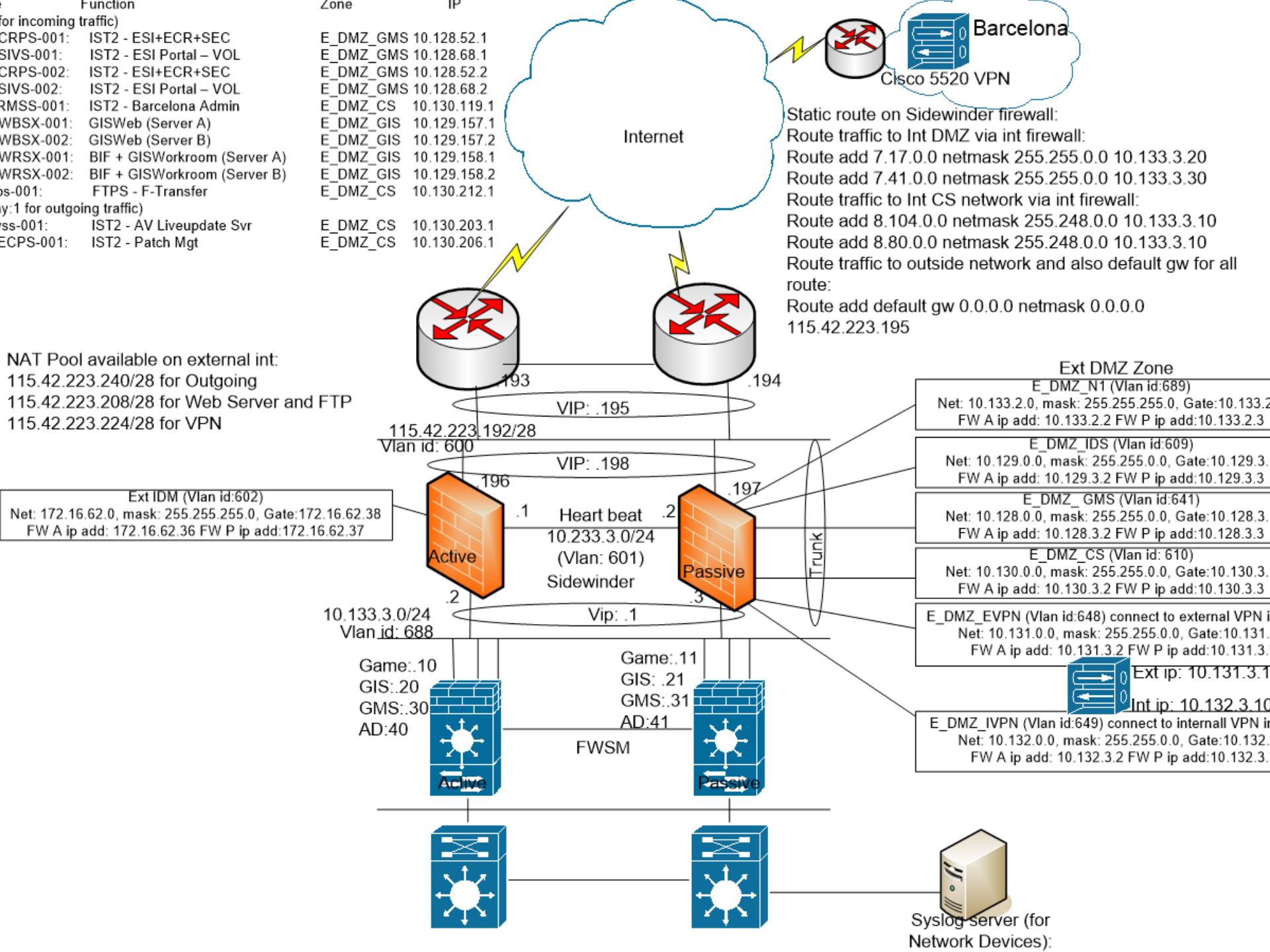


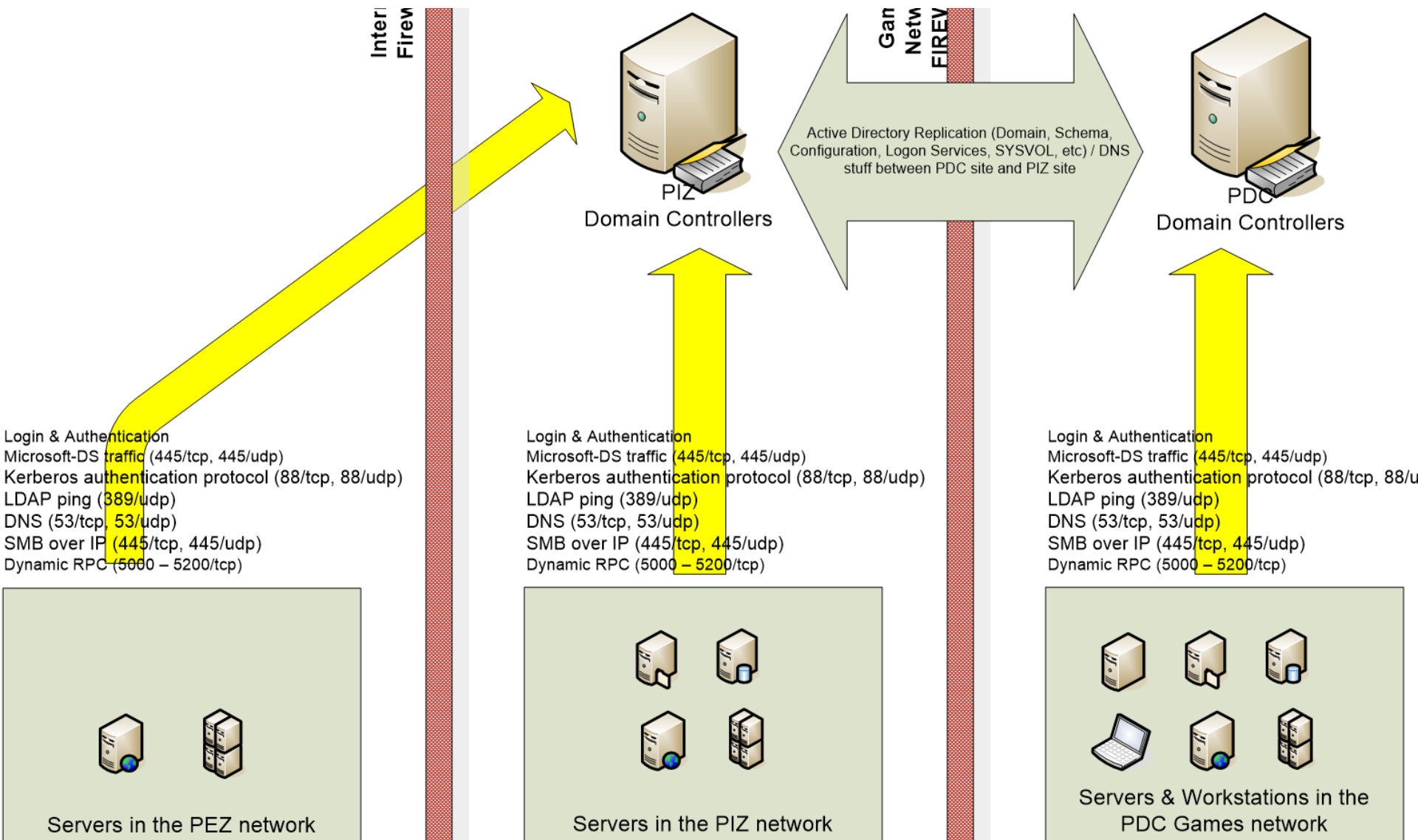
NETWORK SEGMENTATION

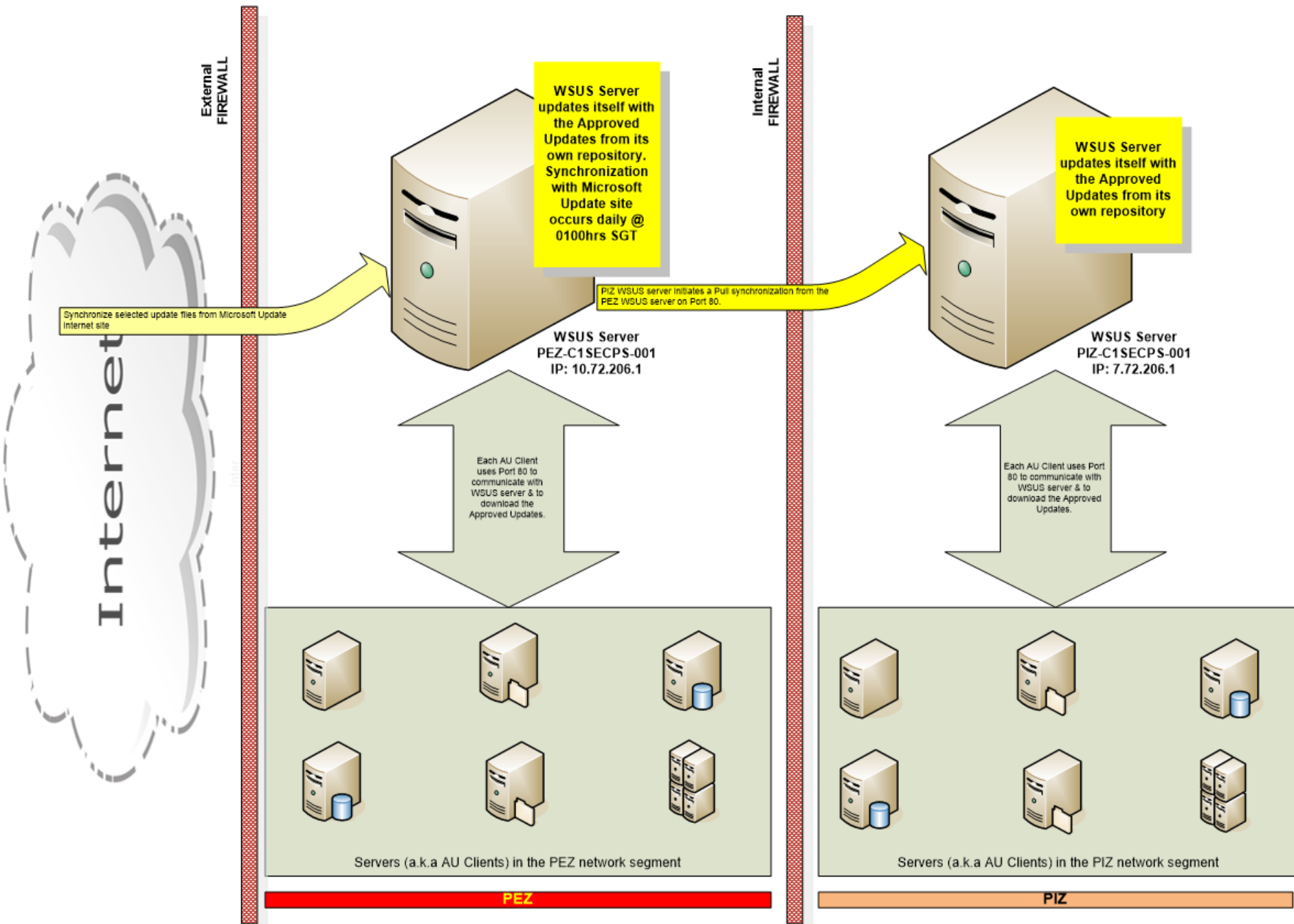


Games Security Zones









ESIREG http 9180 https 9543 (Public accessible)
 ESIADM http 9280 https 9643 (Only Access from KaySiang)
 ECRADM http 9680 https 10043 (Only Access from KaySiang)
 ECRREG http 9580 https 9943 (Public accessible)
 SEC http 8180 https 8543 (Only Access from KaySiang)

VIP: 10.128.255.2 map to
 public: 115.42.223.210

ESI+ECR+SEC
 PEZ-G1ECRPS-001
 10.128.52.1 PEZ-G1ECRPS-002
 10.128.52.2

VIP: 10.128.255.1 map to
 public: 115.42.223.209

ESI Portal – VOL
 PEZ-G1ESIVS-001
 10.128.68.1 PEZ-G1ESIVS-002
 10.128.68.2

Internal DMZ

e-Mail Server/IFTP
 PIZ-G1DFTPS-001
 7.41.80.1 PIZ-G1DFTPS-002
 7.41.80.2

AD + Key Server
 PIZ-G1SADKS-001
 7.41.95.1 PIZ-G1SADKS-002
 7.41.95.2

DB+Interface Server
 PIZ-G1DIDBS-001
 7.41.96.1 PIZ-G1DIDBS-002
 7.41.96.2

7.41.96.11 (MS Cluster IP)
 7.41.96.12 (SQL Virtual IP)

Games Network

VIP: 8.41.255.2
 ACR+ADS+SSC+UMM+SIS+EAC
 PDC-G1ACQWS-001
 8.41.81.1 PDC-G1ACQWS-002
 8.41.81.2

VIP: 8.41.255.3
 RGM+Cclear+Massive Process
 PDC-G1GMSMS-001
 8.41.86.1 PDC-G1GMSMS-002
 8.41.86.2

VIP: 8.41.255.1
 GSC+CORE+WFC+SEC+SEQ
 PDC-G1GWA2S-001
 8.41.77.1 PDC-G1GWA2S-002
 8.41.77.2

AD + Key Server
 PDC-G1SADKS-001
 8.41.95.1 PDC-G1SADKS-002
 8.41.95.2

DB+Interface Server
 PDC-G1GMSIS-001
 8.41.82.1 PDC-G1GMSIS-002
 8.41.82.2

8.41.82.11 (MS Cluster IP)
 8.41.82.12 (SQL Virtual IP)

Internet DMZ Firewalls

Internal DMZ Firewalls

Games Firewall

Subnet Mask: 255.255.0.0
 Default Gateway:
 10.128.3.1 (External DMZ)
 7.41.3.1 (Internal DMZ)
 8.41.1.1 (Games Network)

Supporting Documents

► Dashboards

- KPIs (e.g.:
 - Infections
 - Root logon sources
 - Hosts without AV
- Administrators activity
- Alarms overview
- Rare processes
- Highest risk alarms
- Application related

► Statistics

► Maps

- Network configuration layer(s)
- IT Services layer map for each separate service
 - WSUS
 - Antivirus
 - VoIP
- Business App layer maps
 - Colvir
 - IBanking

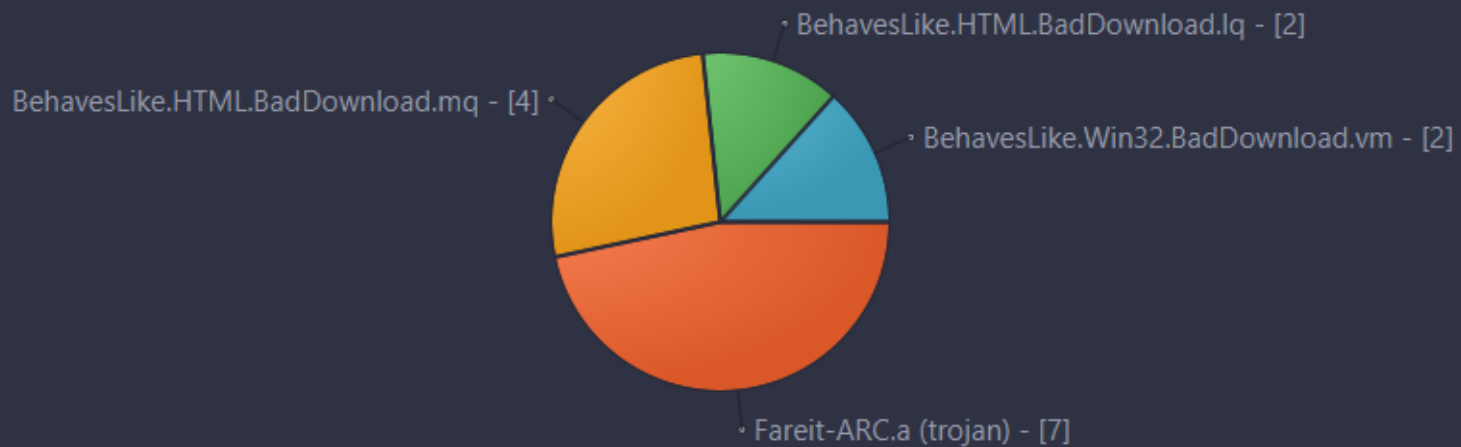


Infections KPI Dashboard

Virus Infections

Last update: 2017-02-17T11:56:40.588+01:00[Europe/Prague]

Virus Infections



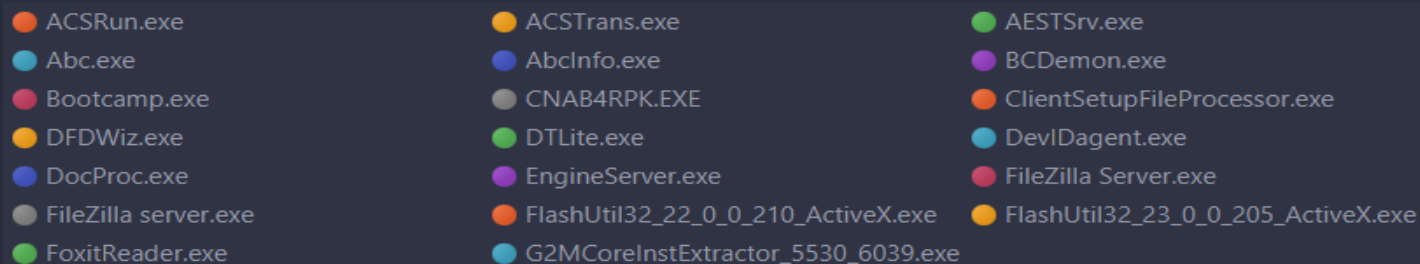
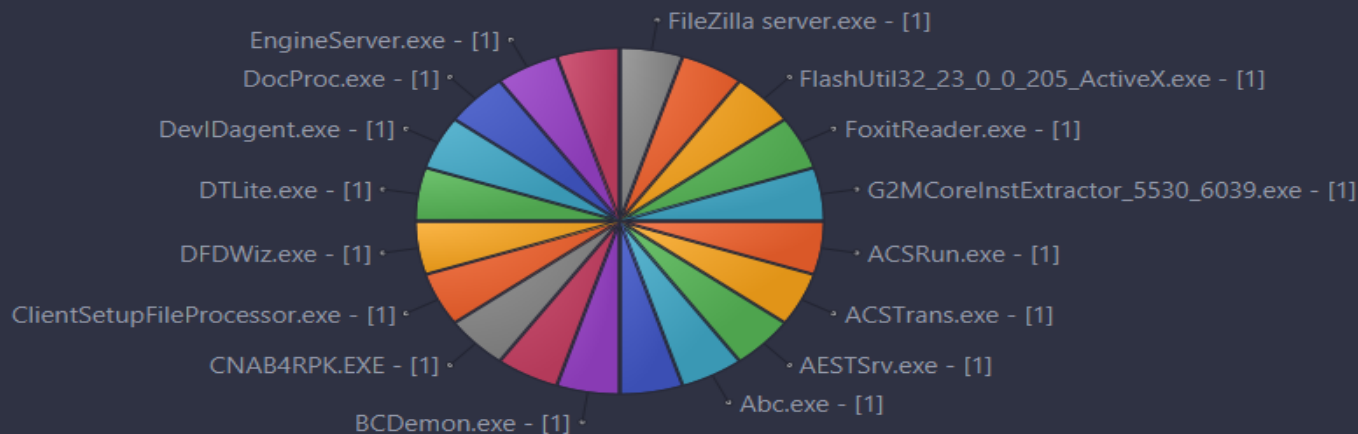
Query: virus_name:["" TO "z"] Field: virus_name



Last update: 2017-02-17T11:54:31.462+01:00[Europe/Prague]



Rarest Processes



Hosts with active Sector

