DTS SOLUTION
smart solution for the smart business

# Building a SCADA Cyber Security Operations Center - PCN

www.dts-solution.com

***Shah H Sheikh – Sr. Security Solutions Consultant***
MEng CISSP CISA CISM CRISC CCSK
shah@dts-solution.com

# Security Operations Center

*Agenda – Building a Security Operations Center*

- Information Security in Depth – put into practice
- Understand overall security architecture
- Identify ingress points of attack vectors
- Physical and Logical Security
- Build a SOC around the above

… and more importantly build it around;

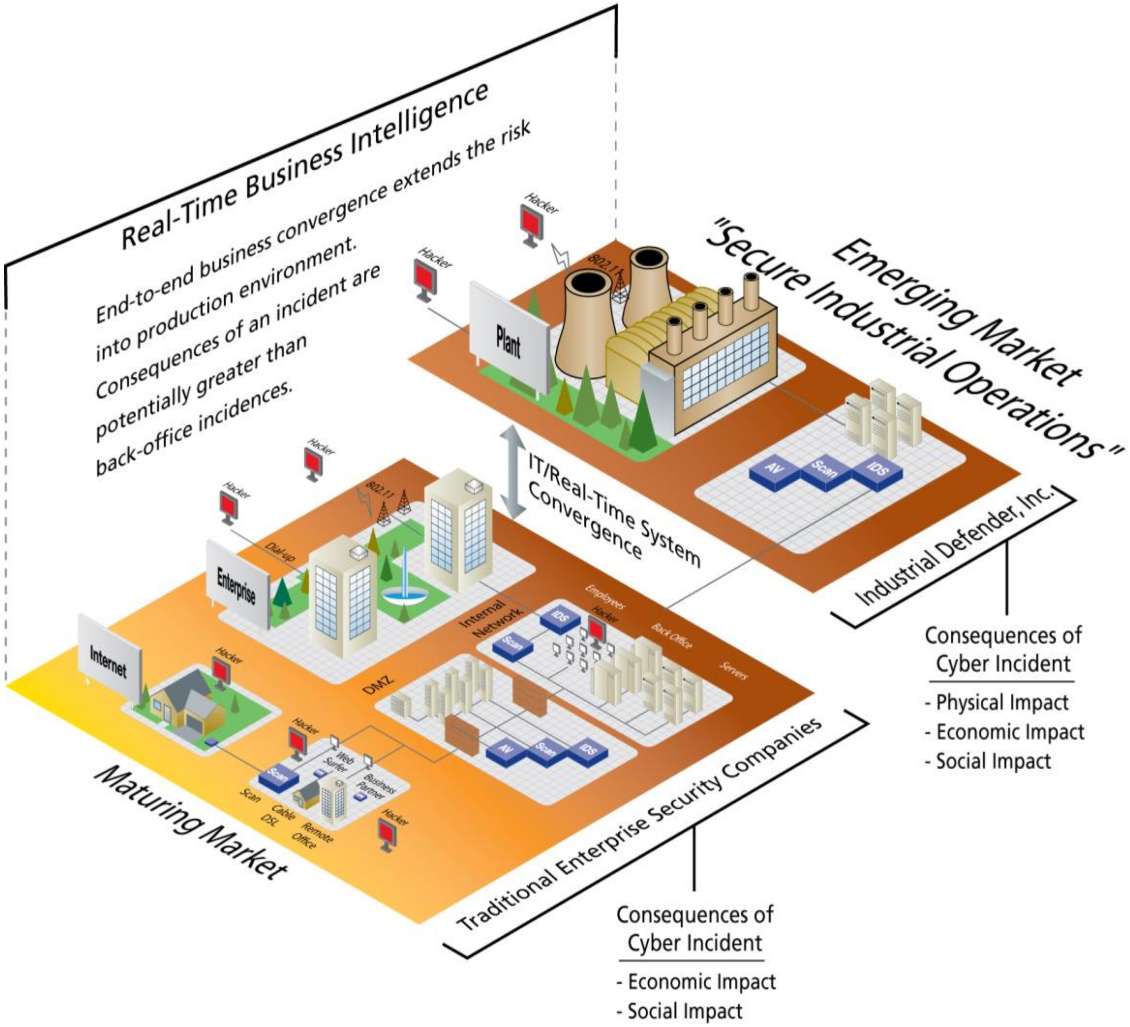
***People, Process and Technology***

# Cyber Security - Defense In Depth

# Why is Cyber Security important?

- **Cost Savings**
  - Reduced down time and maintenance costs
  - Improved productivity
  - Enhanced business continuity
- **Simplified Regulatory and Standards Compliance**
  - FERC / NERC CIP
  - ANSI/ISA-99
  - IEC 62443
  - NIST 800-82
- **Enhanced Security and Safety**
  - Improved safety for the plant, employees and community
  - Improved defense against malicious attacks

# Critical Infrastructure Operations – The Emerging Threat



Real-Time Business Intelligence

End-to-end business convergence extends the risk into production environment. Consequences of an incident are potentially greater than back-office incidences.

Emerging Market "Secure Industrial Operations"

IT/Real-Time System Convergence

Maturing Market

Traditional Enterprise Security Companies

Industrial Defender, Inc.

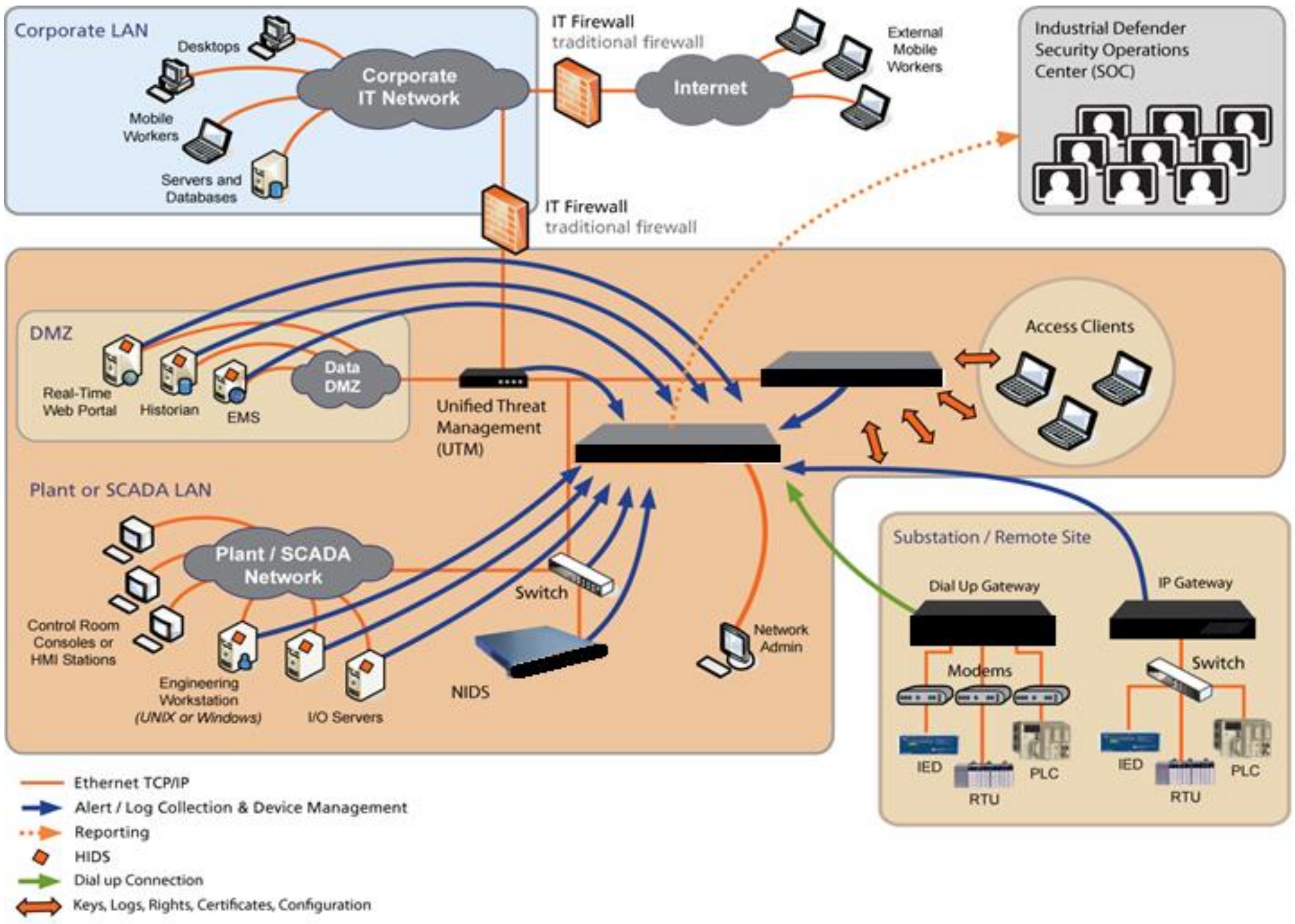
Consequences of Cyber Incident

- Physical Impact
- Economic Impact
- Social Impact

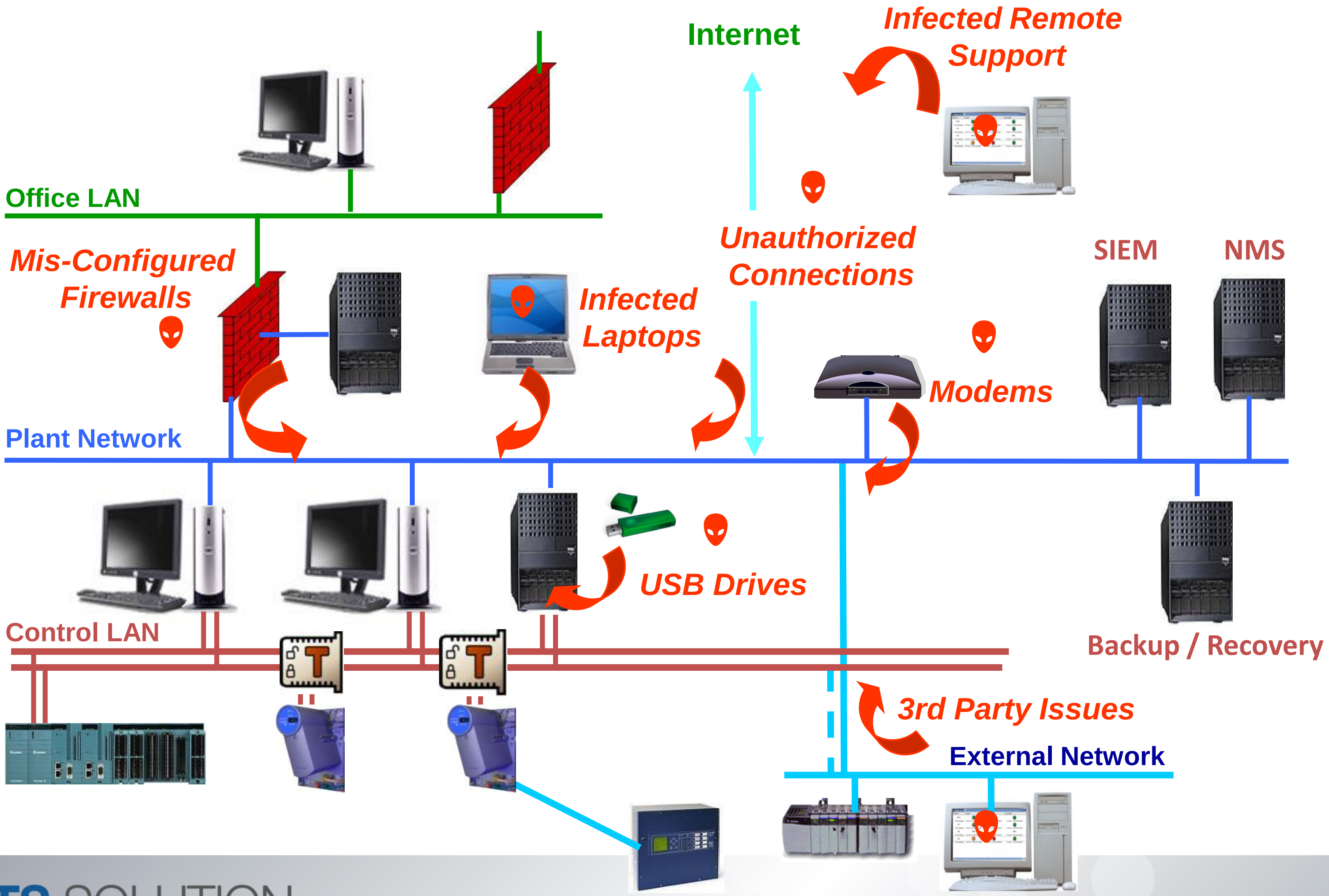
Consequences of Cyber Incident

- Economic Impact
- Social Impact

# ICS Security - Defense-in-Depth



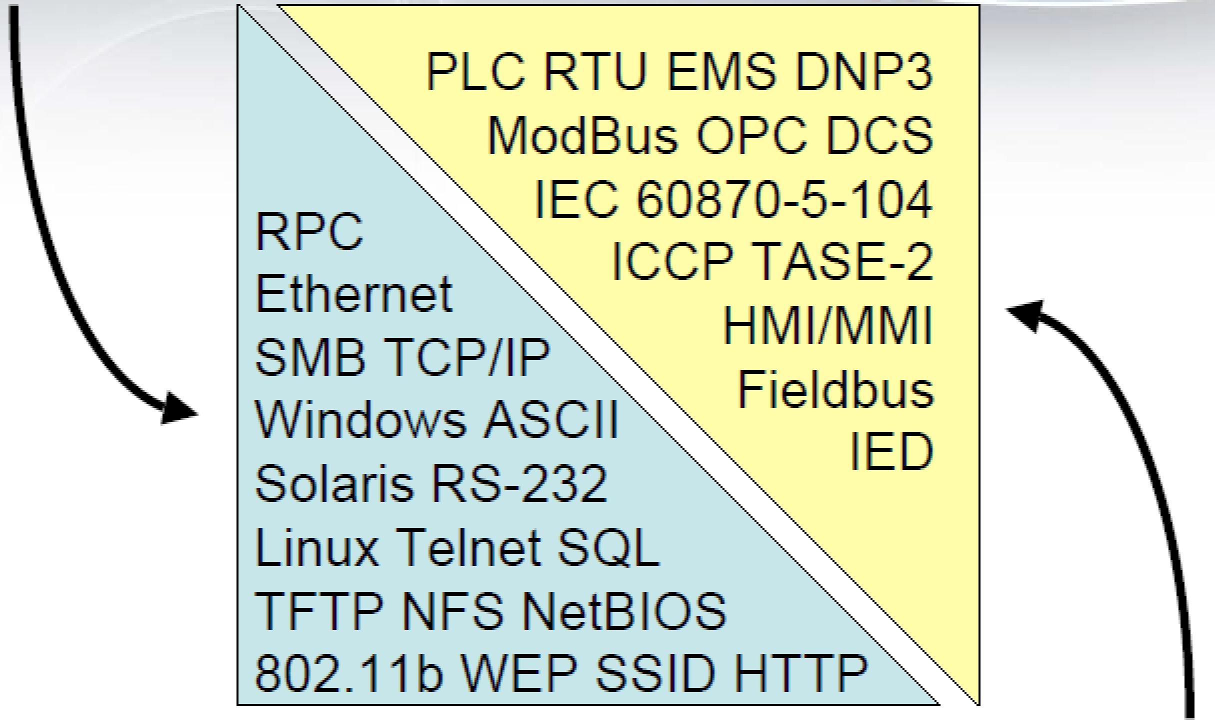
# Pathways into the Plant Floor



# Automation Systems Security Really Unique?

| Corporate IT | Automation Systems IT |
|---|---|
| Not life threatening | Safety first |
| Availability important | Non-interruption is critical |
| Transactional orientation | Real-time focus |
| IBM, SAP, Oracle, ….. | ABB, Emerson, GE, Honeywell, Siemens... |
| People ~= Devices | Few people; Many, many devices |
| PCs and Servers | Sensors, Controllers, Servers |
| Web services model is dominant | Polled automation control model |
| MS Windows is dominant OS | Vendor-embedded operating systems |
| Many commercial software products installed on each PC | Purpose-specific devices and application |
| Protocol is primarily HTTP/HTTPS   over TCP/IP -- widely known | Many industrial protocols, some over TCP/IP – vendor and sector-specific |
| Office environment, plus mobile | Harsh operating plant environments |
| Cross-industry IT jargon | Industry sector-specific jargon |
| Cross-industry regulations (mostly) | Industry-specific regulations |

Just this is sufficient



PLC RTU EMS DNP3
ModBus OPC DCS
IEC 60870-5-104
ICCP TASE-2
HMI/MMI
Fieldbus
IED

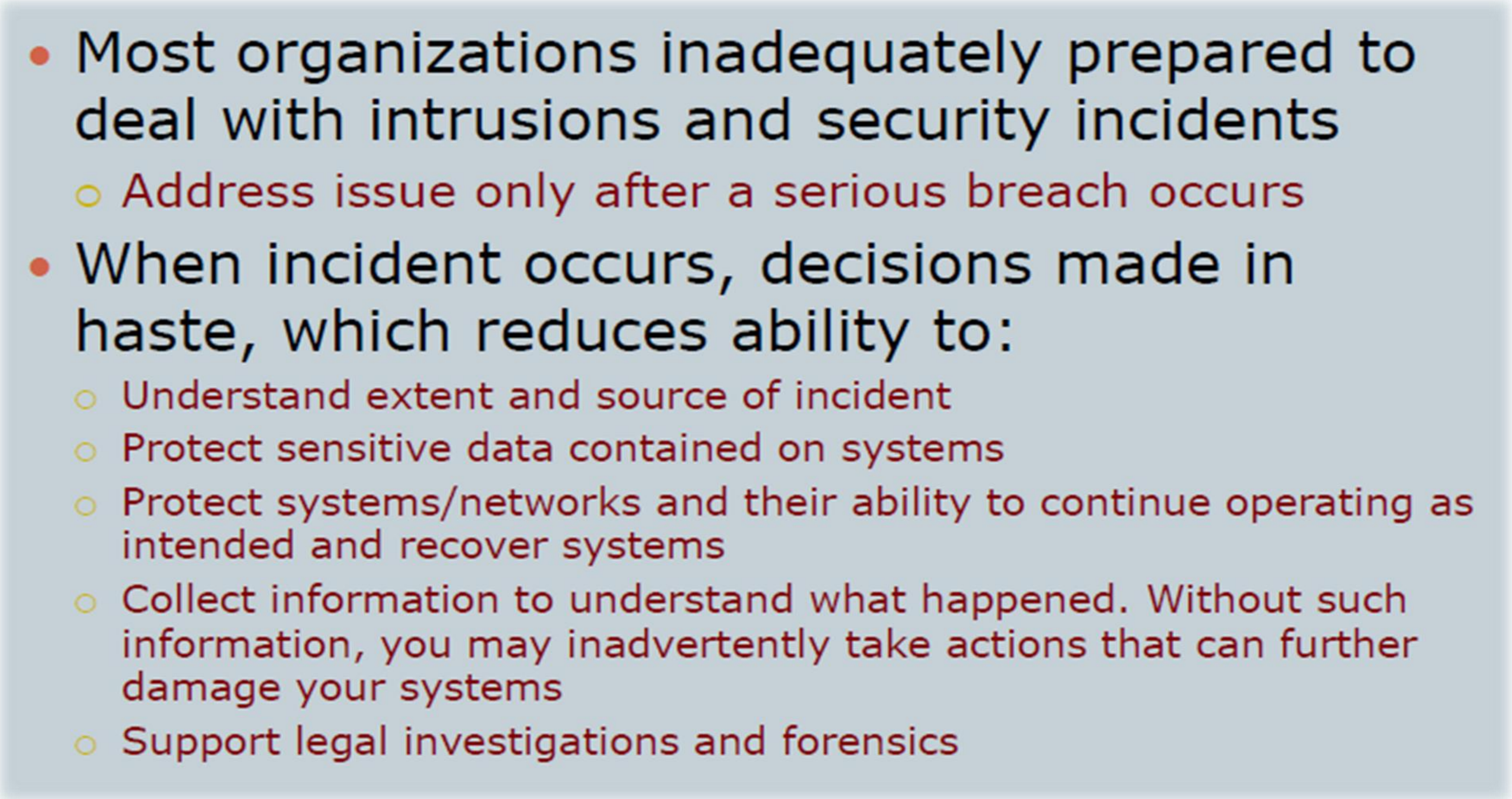
RPC
Ethernet
SMB TCP/IP
Windows ASCII
Solaris RS-232
Linux Telnet SQL
TFTP NFS NetBIOS
802.11b WEP SSID HTTP

This helps, and it’s all on the Internet

# Current Challenges

- Onslaught of security data from disparate systems, platforms and applications
- Numerous point solutions (antivirus, firewalls, IDS/IPS, ERP, access control, IdM, SSO, etc.)
- Millions of messages daily
- Attacks becoming more frequent and sophisticated
- Regulatory compliance issues place increasing burden on systems and network administrators

# Current Challenges



- Most organizations inadequately prepared to deal with intrusions and security incidents
  - Address issue only after a serious breach occurs
- When incident occurs, decisions made in haste, which reduces ability to:
  - Understand extent and source of incident
  - Protect sensitive data contained on systems
  - Protect systems/networks and their ability to continue operating as intended and recover systems
  - Collect information to understand what happened. Without such information, you may inadvertently take actions that can further damage your systems
  - Support legal investigations and forensics

# The current SOC landscape…

- In recent years, the complexity of managing a SOC has increased exponentially
- Security operations is not just about perimeter threats anymore
  - Array of hundreds of event sources - firewalls, IPS, IDS, proxy information, applications, identity management, database, router, switch, merchant/PCI, physical security devices and more
- SOC's are aggregation points of tens of millions of daily events that must be monitored, logged, analyzed and correlated

# Outsourced or In-house ?!?

## Outsourced SOC

### Advantages

- Avoid capital expenses – it's their hardware & software
- Often cheaper than in-house
- Less potential for collusion between monitoring team and attacker
- Good security people are difficult to find
- Unbiased
- SLA

### Disadvantages

- Contractors will never know your environment like internal employees
- Sending jobs outside organization can lower morale
- No long-term gain for the company
- Risk of external data mishandling

*... VS ...*

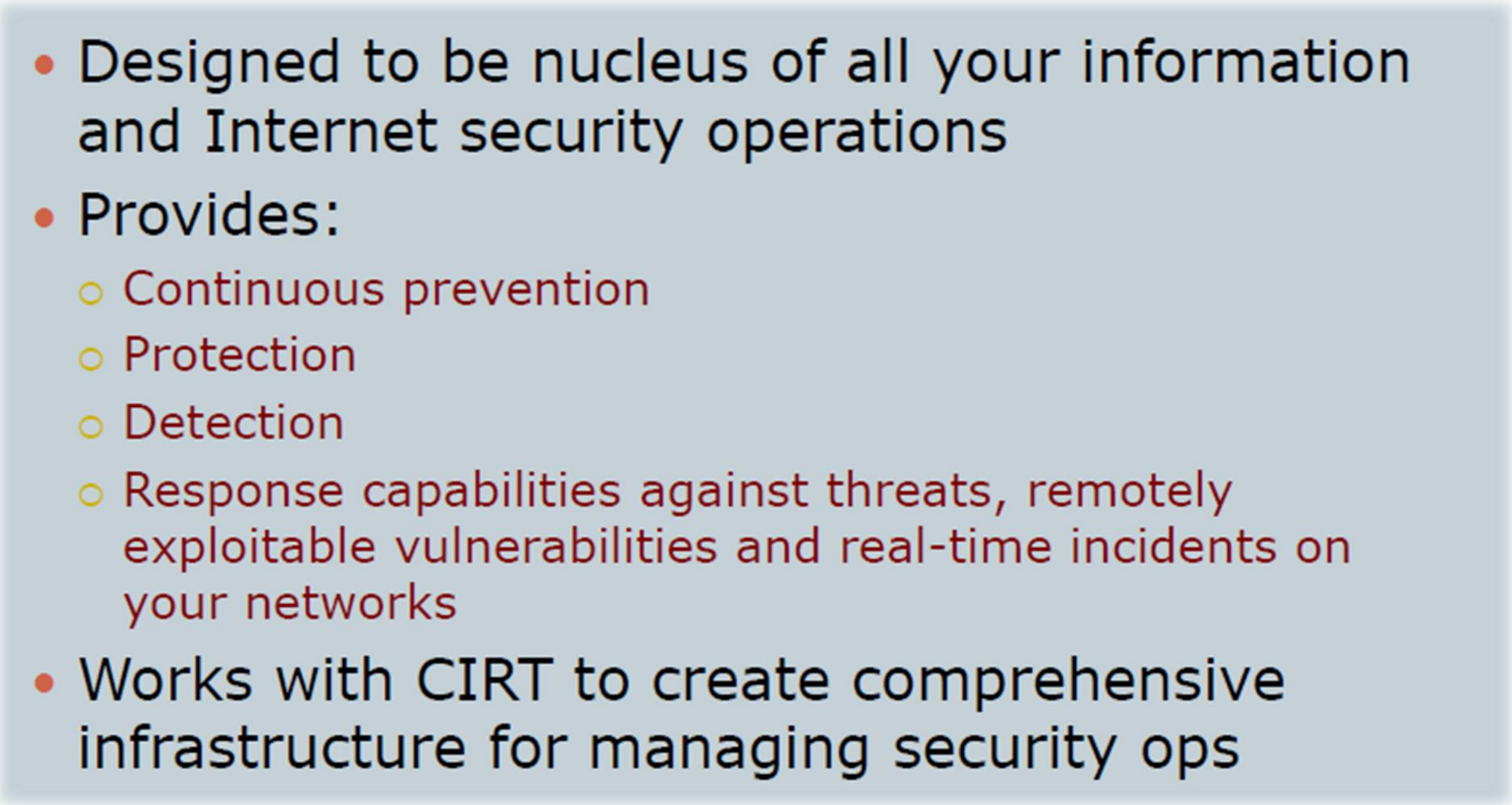
### Advantages

- Knows environment better than a third-party
- Solutions are generally easier to customize
- Potential to be most efficient
- Most likely to notice correlations between groups
- Better tool pricing – higher volume

### Disadvantages

- Larger up-front investment
- Higher pressure to show ROI quickly
- Higher potential for collusion between analyst and attacker
- Less likely to recognize large-scale, subtle patterns that include multiple groups

# Why build a SOC?



- Designed to be nucleus of all your information and Internet security operations
- Provides:
  - Continuous prevention
  - Protection
  - Detection
  - Response capabilities against threats, remotely exploitable vulnerabilities and real-time incidents on your networks
- Works with CIRT to create comprehensive infrastructure for managing security ops

# Key Objectives for SOC … (1)

- Manages and Coordinates the response to Cyber Threats and Incidents
- Monitors the Cyber Security posture and reports deficiencies
- Coordinates with regulatory bodies
- Performs Threat and Vulnerability Analysis
- Performs Analysis of Cyber Security Events
- Maintains an Internal Database of Cyber Security Incidents
- Provide Alerts and Notifications to General and Specific Threats
- Provide regular reporting to Management and Cyber Incident Responders

# Key Objectives for  SOC … (2)

- Reduce the response time of security incident from initial findings, to reporting to containment
- Recovery Time Objective (RTO) in case of security incident materializing
- Proactive Security Monitoring based on predefined security metrics / KPI
- Raise Awareness of Information Security across  community of leaders and sub-ordinates
- Ability to correlate system, application, network, server, security logs in a consistent way

# Key Objectives for  SOC … (3)

- Ability to automate the requirement to meet compliance – vulnerability assessment and risk management
- Ensure change control function is integrated into the SOC process
- Identification for all security attack vectors and classification of incidents
- Define disaster recovery plans for ICE (in-case of emergency).
- Build a comprehensive reporting dashboard that is aligned to security metrics
- Build a local in-house SIRT (security incident response team) that collaborates with national CERT

# Key Objectives for  SOC … (4)

- To build SOC processes that are aligned to existing  ISO27001 security policies
- Build a physical and virtual team of SOC personnel for 24 x 7 monitoring
- Build forensics capabilities to be able to reconstruct series of events during an incident
- Proactive monitoring of network and security infrastructure devices

# Components of a SOC

- To build the SOC with simple acceptance and execution model
- Maximize the use of technology.
- To build security intelligence and visibility that was previously unknown; build effective coordination and response unit and to introduce automation of security process.
- Develop SOC processes that are inline to industry best practices and accepted standards – ISO27001:2013, PCI-DSS3.0

### REAL-TIME MONITORING

- DATA AGGREGATION
- DATA CORRELATION
- AGGREGATE LOGS
- CORDINATE RESPONSE
- AUTOMATED REMEDIATION

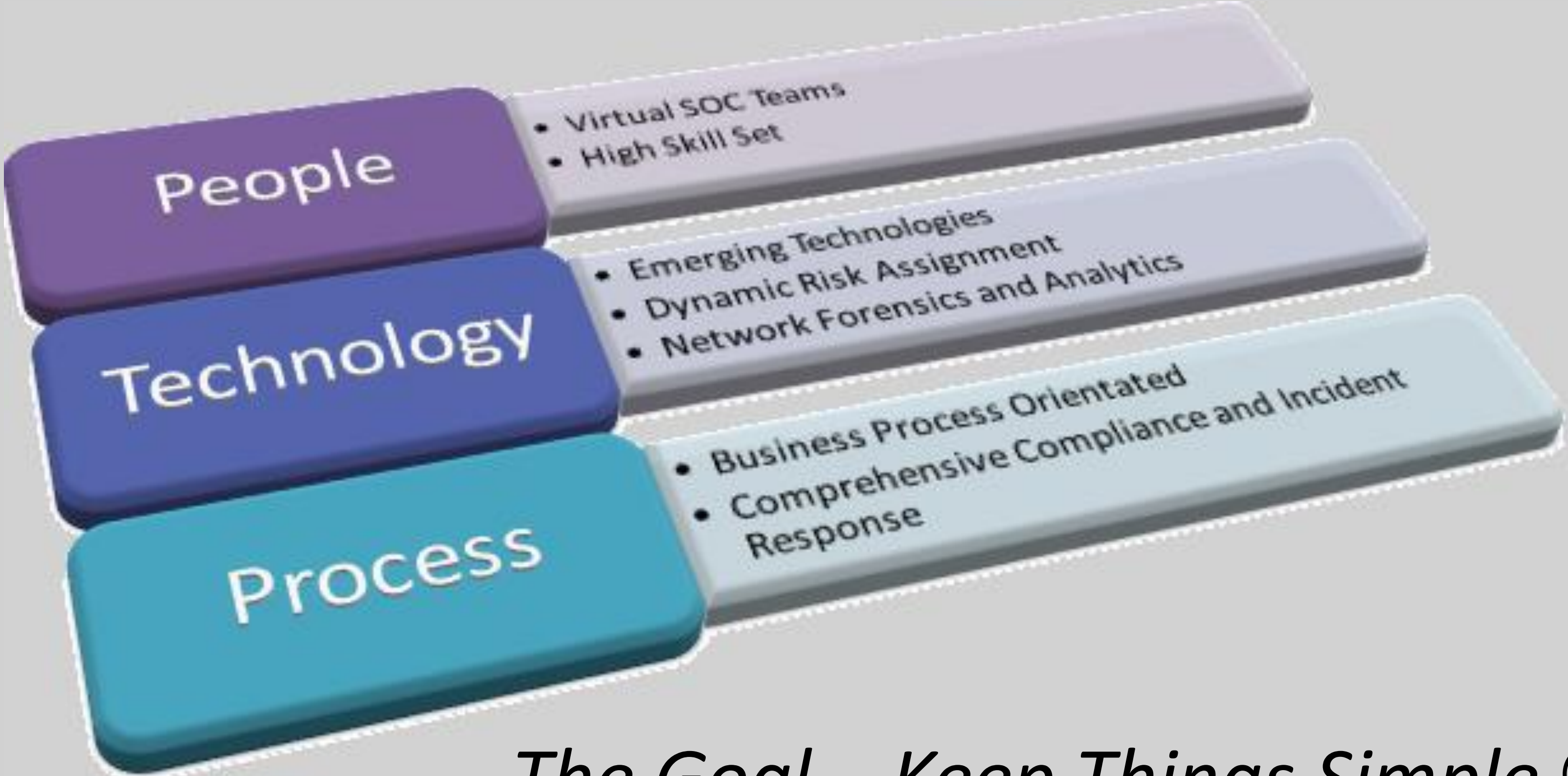
### REPORTING

- EXECUTIVE SUMMARY
- AUDIT AND ASSESSMENT
- SECURITY METRIC REPORTING
- KPI COMPLIANCE
- SLA REPORTING

### SECURITY INCIDENT MANAGEMENT

- PRE AND POST INCIDENT ANALYSIS
- FORENSICS ANALYSIS
- ROOT CAUSE ANALYSIS
- INCIDENT HANDLING
- aeCERT INTEGRATION

# Key Success Factors in a SOC



People
- Virtual SOC Teams
- High Skill Set

Technology
- Emerging Technologies
- Dynamic Risk Assignment
- Network Forensics and Analytics

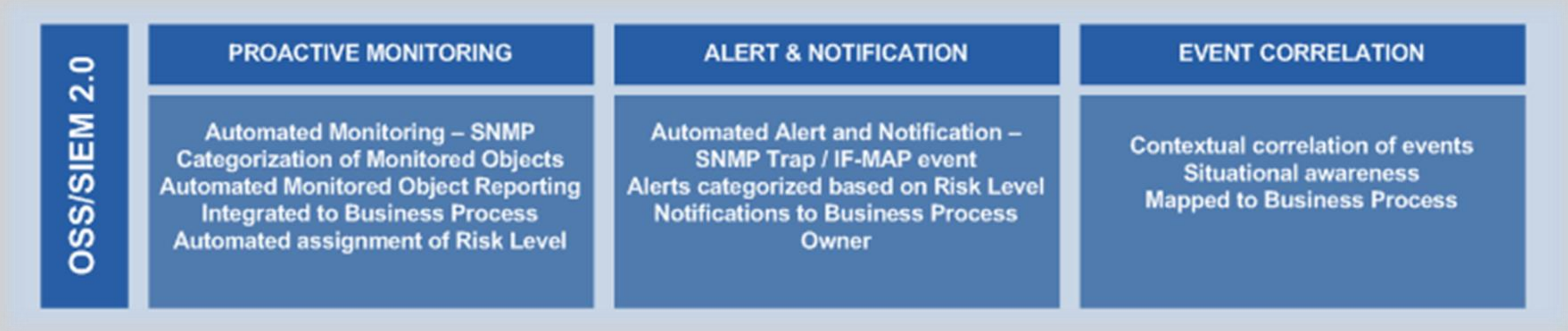
Process
- Business Process Orientated
- Comprehensive Compliance and Incident Response

*The Goal – Keep Things Simple ☺*

# SOC – Core Components

## *Core Components for a SOC 2.0*

- OSS – Operational Support System
- SIEM – Security Information and Event Management
- Proactive Monitoring  - Network and Security and Server Infrastructure
- Alert and Notification – Security Incident Reporting
- Events Correlation and Heuristics / Behavioural / Anomaly

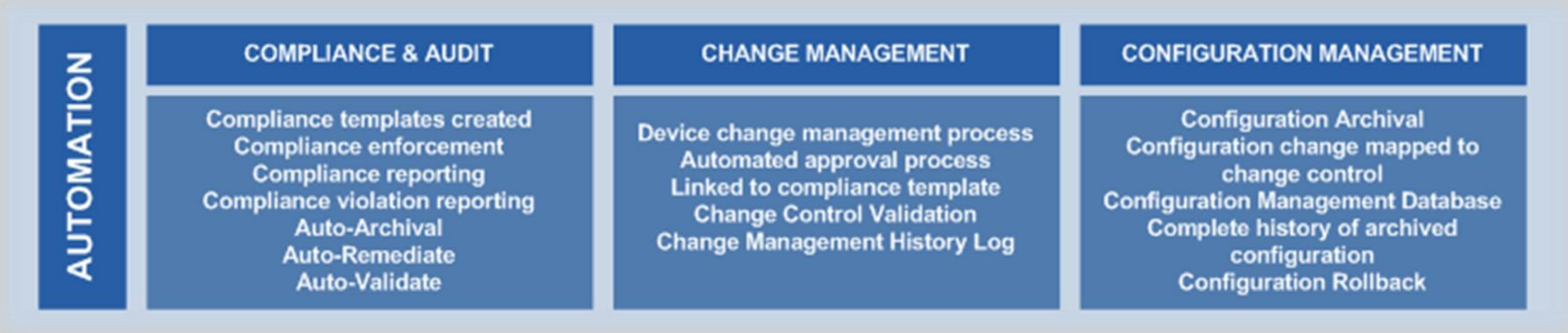


| OSS/SIEM 2.0 | PROACTIVE MONITORING | ALERT & NOTIFICATION | EVENT CORRELATION |
|---|---|---|---|
| | Automated Monitoring – SNMP<br>Categorization of Monitored Objects<br>Automated Monitored Object Reporting<br>Integrated to Business Process<br>Automated assignment of Risk Level | Automated Alert and Notification – SNMP Trap / IF-MAP event<br>Alerts categorized based on Risk Level<br>Notifications to Business Process Owner | Contextual correlation of events<br>Situational awareness<br>Mapped to Business Process |

# SOC – Core Components

## ***Core Components for a SOC 2.0***

- Information and Network Security *$$ Automation $$*
- To natively build-in compliance and audit functions
- To manage change control process through integrated ITILv3 CM and SD
- Configuration Management of Infrastructure Components

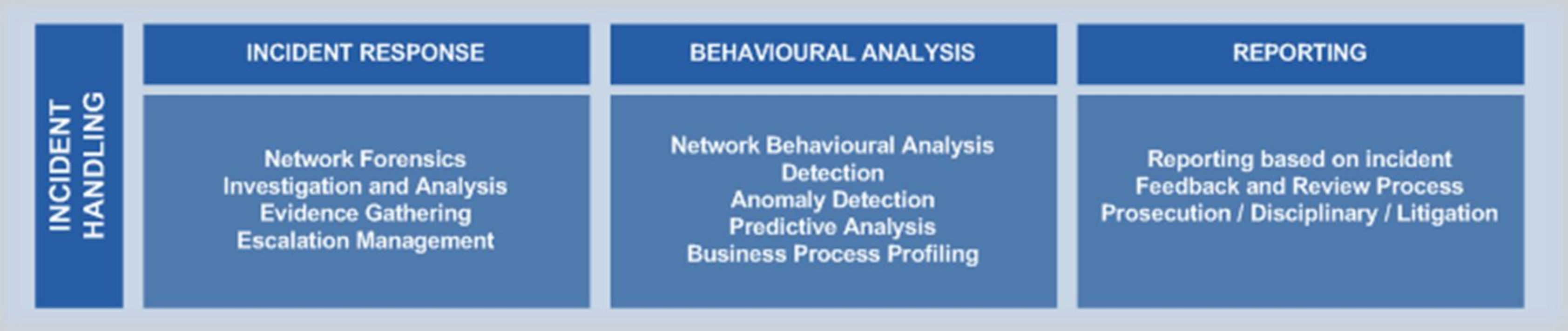


|  | COMPLIANCE & AUDIT | CHANGE MANAGEMENT | CONFIGURATION MANAGEMENT |
|---|---|---|---|
| AUTOMATION | Compliance templates created<br>Compliance enforcement<br>Compliance reporting<br>Compliance violation reporting<br>Auto-Archival<br>Auto-Remediate<br>Auto-Validate | Device change management process<br>Automated approval process<br>Linked to compliance template<br>Change Control Validation<br>Change Management History Log | Configuration Archival<br>Configuration change mapped to change control<br>Configuration Management Database<br>Complete history of archived configuration<br>Configuration Rollback |

# SOC – Core Components

## *Core Components for a SOC 2.0*

- Alignment of Risk Management with  Business Needs
- Qualified Risk Ranking
- Risks are ranked based on business impact (BIA)
- Risk framework is built into the SIEM solution;
  - **incident = risk severity = appropriate remediation and isolation action**
- SOC is integrated with Vulnerability and Patch Management

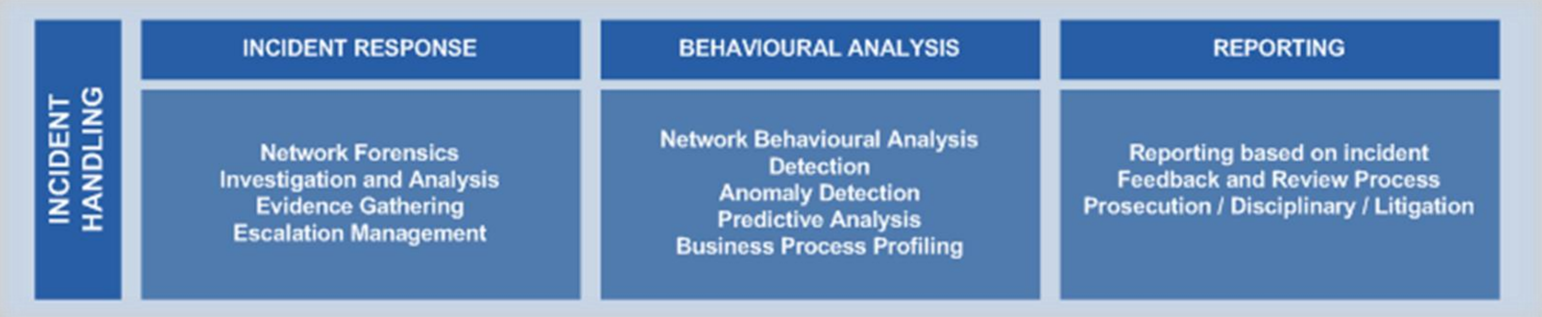


| INCIDENT HANDLING | INCIDENT RESPONSE | BEHAVIOURAL ANALYSIS | REPORTING |
|---|---|---|---|
| | Network Forensics<br>Investigation and Analysis<br>Evidence Gathering<br>Escalation Management | Network Behavioural Analysis<br>Detection<br>Anomaly Detection<br>Predictive Analysis<br>Business Process Profiling | Reporting based on incident<br>Feedback and Review Process<br>Prosecution / Disciplinary / Litigation |

# SOC – Core Components

## ***Core Components for a SOC 2.0***

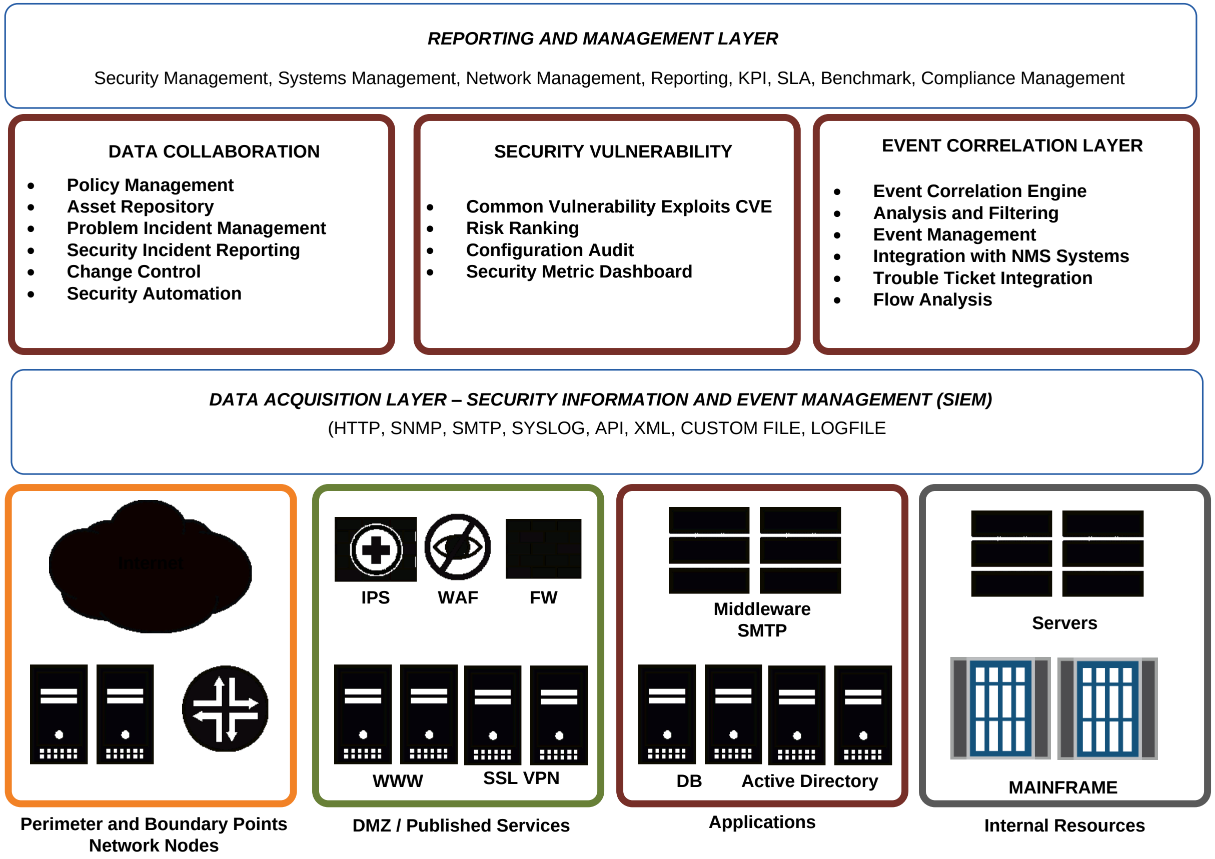
- IRH – Incident Response Handling
  - How effective the SOC is measured by how incidents are managed, handled, administered, remediated and isolated.
  - Continuous cyclic feedback mechanism drives IRH
- Critical functions include Network Forensics and Surveillance Tech..
- Reconstruct the incident …. Evidence gathering … Effective Investigation
- Escalation Management – know who to communicate during an incident



| INCIDENT HANDLING | INCIDENT RESPONSE | BEHAVIOURAL ANALYSIS | REPORTING |
|---|---|---|---|
| | Network Forensics<br>Investigation and Analysis<br>Evidence Gathering<br>Escalation Management | Network Behavioural Analysis<br>Detection<br>Anomaly Detection<br>Predictive Analysis<br>Business Process Profiling | Reporting based on incident<br>Feedback and Review Process<br>Prosecution / Disciplinary / Litigation |

# SOC – Core Components

## *Proposed Architecture for the SOC*



***REPORTING AND MANAGEMENT LAYER***

Security Management, Systems Management, Network Management, Reporting, KPI, SLA, Benchmark, Compliance Management

**DATA COLLABORATION**

- **Policy Management**
- **Asset Repository**
- **Problem Incident Management**
- **Security Incident Reporting**
- **Change Control**
- **Security Automation**

**SECURITY VULNERABILITY**

- **Common Vulnerability Exploits CVE**
- **Risk Ranking**
- **Configuration Audit**
- **Security Metric Dashboard**

**EVENT CORRELATION LAYER**

- **Event Correlation Engine**
- **Analysis and Filtering**
- **Event Management**
- **Integration with NMS Systems**
- **Trouble Ticket Integration**
- **Flow Analysis**

***DATA ACQUISITION LAYER – SECURITY INFORMATION AND EVENT MANAGEMENT (SIEM)***

(HTTP, SNMP, SMTP, SYSLOG, API, XML, CUSTOM FILE, LOGFILE

**Perimeter and Boundary Points Network Nodes**

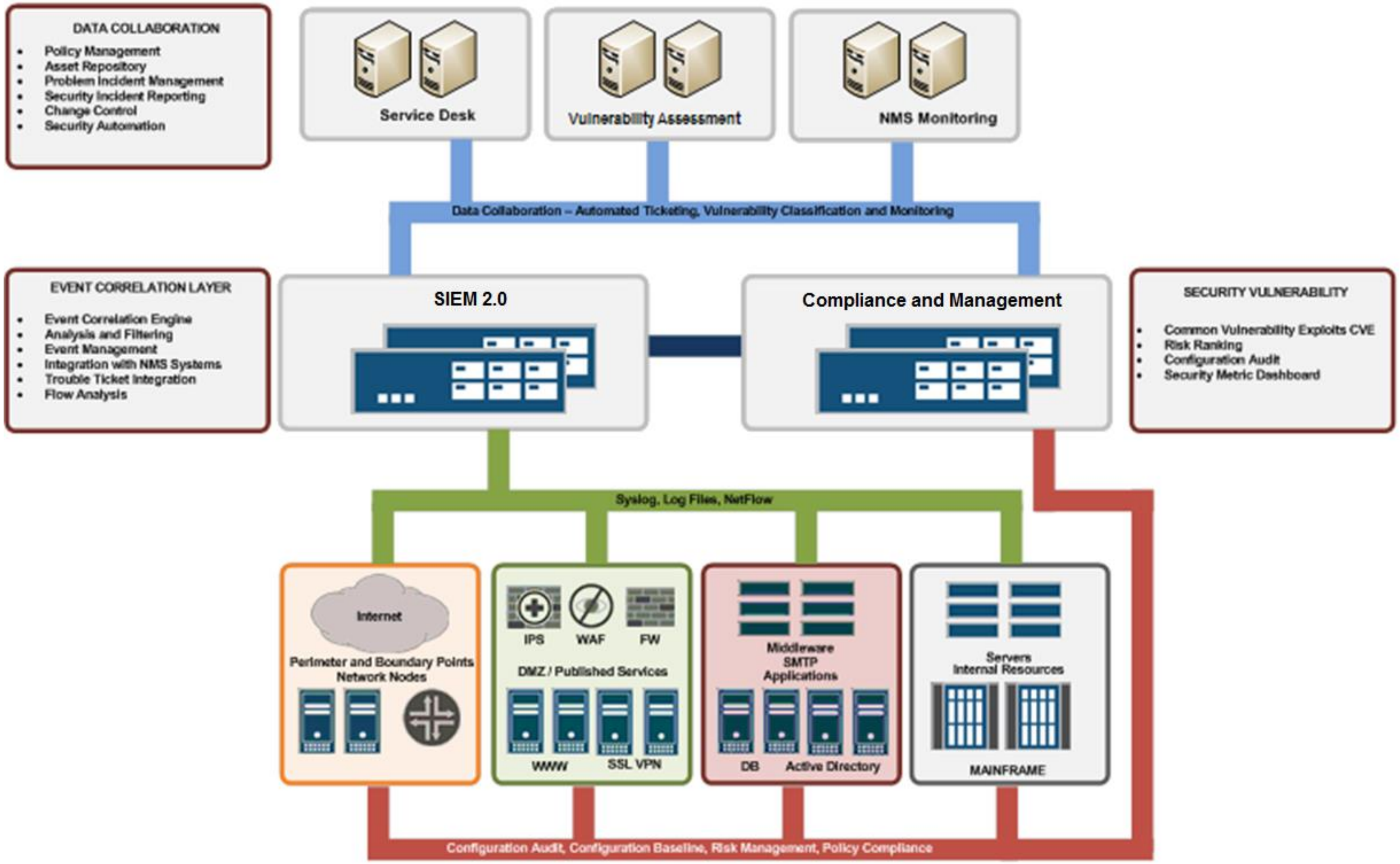
**DMZ / Published Services**

**Applications**

**Internal Resources**

# SOC – Core Components

***Integration of Core SOC Components***



DATA COLLABORATION

- Policy Management
- Asset Repository
- Problem Incident Management
- Security Incident Reporting
- Change Control
- Security Automation

EVENT CORRELATION LAYER

- Event Correlation Engine
- Analysis and Filtering
- Event Management
- Integration with NMS Systems
- Trouble Ticket Integration
- Flow Analysis

SECURITY VULNERABILITY

- Common Vulnerability Exploits CVE
- Risk Ranking
- Configuration Audit
- Security Metric Dashboard

Service Desk
Vulnerability Assessment
NMS Monitoring
Data Collaboration – Automated Ticketing, Vulnerability Classification and Monitoring
SIEM 2.0
Compliance and Management
Syslog, Log Files, NetFlow
Internet
Perimeter and Boundary Points
Network Nodes
IPS
WAF
FW
DMZ / Published Services
WWW
SSL VPN
Middleware
SMTP
Applications
DB
Active Directory
Servers
Internal Resources
MAINFRAME
Configuration Audit, Configuration Baseline, Risk Management, Policy Compliance

# SOC Technologies …

## *So now the technologies …*

**SIEM Solutions**

- Event Collector – Syslog, Log Files, Application Log Export
- Flow Collection – NetFlow, J-Flow, S-Flow, IPIX
- Asset Database
- Event and Flow Correlation
- Centralized Management Console for Security Dashboard and Reporting
- Integration with service desk for automated ticket creation

**Compliance Management and Policy Conformance**

- Configuration Audit
- ISO27001 / PCI-DSS3.0 Policy Compliance
- Risk Management
- Baseline Configuration Violation Monitoring
- Network Topology Mapping and Visualization
- Vulnerability Assessment

# SOC Technologies …

## *So now the technology …*

**Network and Security Monitoring**

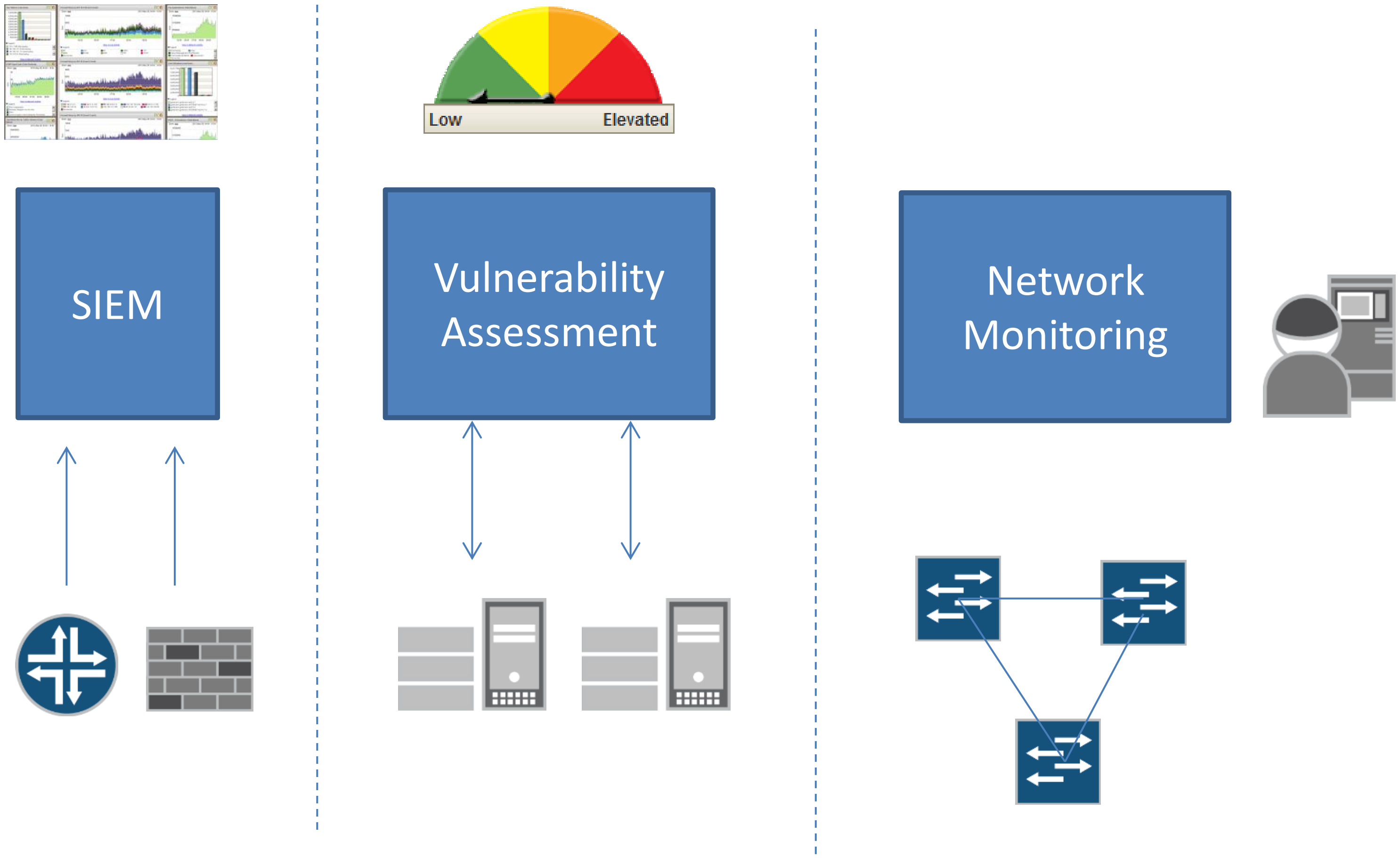
- Network Performance Monitor - SNMP
- Network Monitoring
- Link Utilization
- Availability Monitoring
- SLA reporting
- Integration with service desk for automated ticket creation

**Security Intelligence**

- Network Forensics
- Situation Awareness
- Artifacts and Packet Reconstruction
- Monitor all Internet Activity
- Record metadata for recursive analysis during incident response
- Integration with Incident Response Handling (IRH)

# SOC (before) ….. < The Silos >…

***Technology Integration … the old practice***



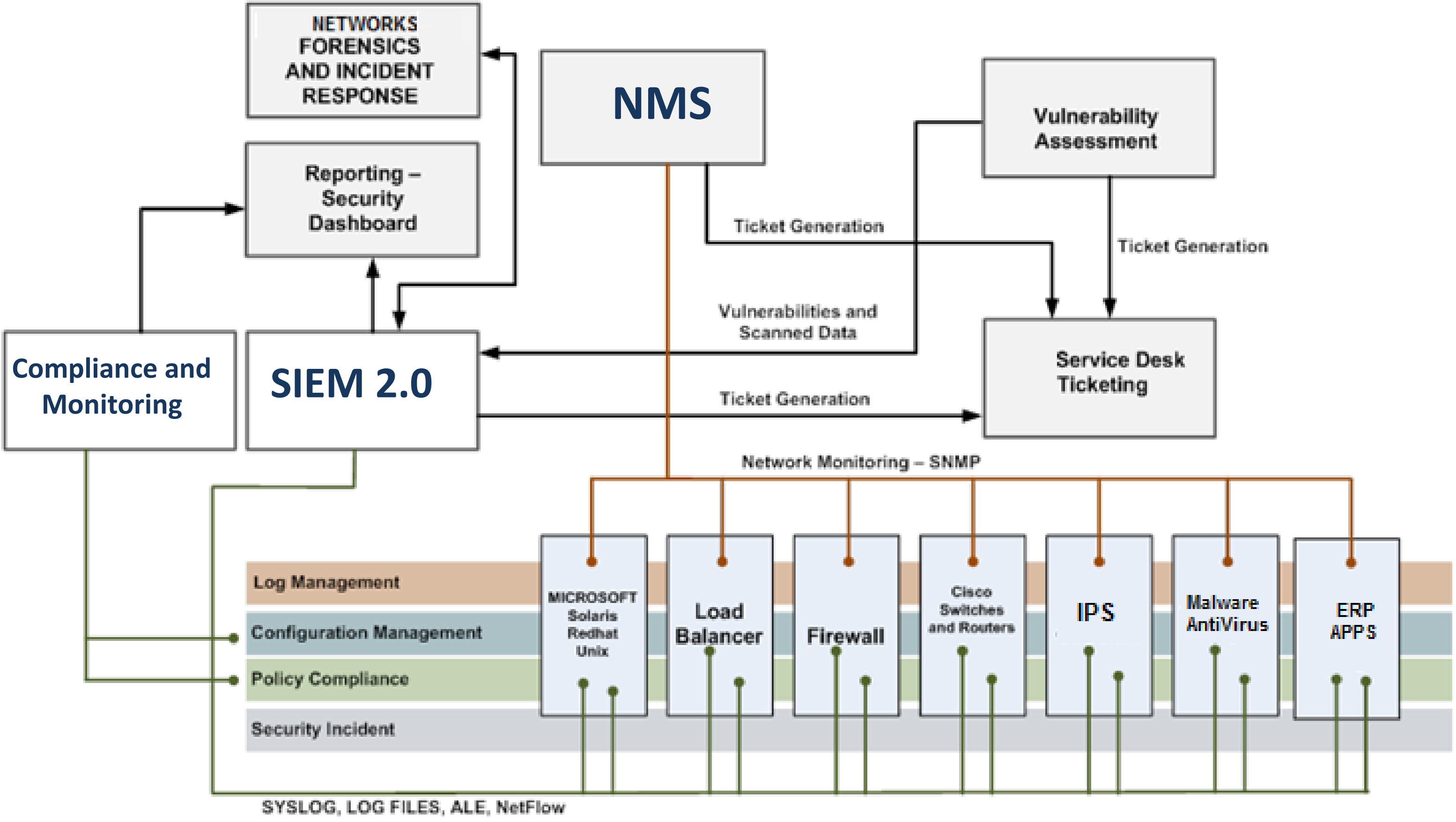
SIEM

Vulnerability Assessment

Network Monitoring

# SOC (after) …. Automation

***Technology Integration … the new … WORKFLOW***


NETWORKS FORENSICS AND INCIDENT RESPONSE
NMS
Vulnerability Assessment
Reporting – Security Dashboard
Ticket Generation
Ticket Generation
Vulnerabilities and Scanned Data
Compliance and Monitoring
SIEM 2.0
Service Desk Ticketing
Ticket Generation
Network Monitoring – SNMP
Log Management
Configuration Management
Policy Compliance
Security Incident
MICROSOFT Solaris Redhat Unix
Load Balancer
Firewall
Cisco Switches and Routers
IPS
Malware AntiVirus
ERP APPS
SYSLOG, LOG FILES, ALE, NetFlow

# SOC – Processes …. Look familiar…

***Creating the SOC Processes***

*… now that we have discussed technology, lets discuss processes …*

**DATA SECURITY AND MONITORING**

- ***Data Asset Classification***
- ***Data Collection***
- ***Data Normalization***
- ***Data at Rest and In Motion***
- ***Data Protection***
- ***Data Distribution***

# SOC – Processes

## ***Creating the SOC Processes***

*… now that we have discussed technology, lets discuss processes …*

**EVENT MANAGEMENT**

- ***Event Correlation***
- ***Identification***
- ***Triage***
- ***Roles***
- ***Containment***
- ***Notification***
- ***Ticketing***
- ***Recovery***
- ***Forensics and Situational Awareness***

# SOC – Processes

***Creating the SOC Processes***

*… now that we have discussed technology, lets discuss processes …*

**INCIDENT RESPONSE PRACTICE**

- ***Security Incident Reporting Structure***
- ***Security Incident Monitoring***
- ***Security Incident Escalation Procedure***
- ***Forensics and Root Cause Analysis***
- ***Return to Normal Operations***
- ***Post-Incident Planning and Monitoring***
- ***Communication Guidelines***
- ***SIRT Integration***

# SOC – Processes

## *Creating the SOC Processes*

*… now that we have discussed technology, lets discuss processes …*

**SOC OPERATING GUIDELINES**

- ***SOC Workflow***
- ***Personnel Shift Description***
- ***Shift Reporting***
- ***Shift Change***
- ***Information Acquisition***
- ***SOC Monitoring Suite***
- ***SOC Reporting Structure***
- ***Organizational Chart***

# SOC – Processes

***Creating the SOC Processes***

*… now that we have discussed technology, lets discuss processes …*

**ESCALATION MANAGEMENT**

- ***Escalation Procedure***
- ***Pre-Escalation Tasks***
- ***IT Security***
- ***Network Operation Center***
- ***Security Engineering***
- ***SIRT Integration***
- ***Law Enforcement***
- ***3rd Party Service Providers and Vendors***

# SOC – Processes

## ***Creating the SOC Processes***

*… now that we have discussed technology, lets discuss processes …*

**DATA RECOVERY PROCEDURES**

- ***Disaster Recovery and BCP Procedure***
- ***Recovery Time Objective***
- ***Recovery Point Objective***
- ***Resiliency and High Availability***
- ***Facilities Outage Procedure***

# SOC – Processes

## SECURITY INCIDENT PROCEDURES

- *Email Phishing - Email Security Incident*
- *Virus and Worm Infection*
- *Anti-Virus Management Incident*
- *NetFlow Abnormal Behavior Incident*
- *Network Behaviour Analysis Incident*
- *Distributed Denial of Service Incident*
- *Host Compromise - Web Application Security Incident*
- *Network Compromise*
- *Internet Misuse*
- *Human Resource - Hiring and Termination*
- *Domain Hijack or DNS Cache Poisoning*
- *Suspicious User Activity*
- *Unauthorized User Access (Employee)*

# SOC – Processes

***Creating the SOC Processes***

*… now that we have discussed technology, lets discuss processes …*

**VULNERABILITY AND PATCH MANAGEMENT**

- *Vulnerability Research*
- *Patch Management - Microsoft SCOM*
- *Identification*
- *Dissemination*
- *Compliance Monitoring*
- *Network Configuration Baseline*
- *Anti-Virus Signature Management*
- *Microsoft Updates*

# SOC – Processes

***Creating the SOC Processes***

*… now that we have discussed technology, lets discuss processes …*

## TOOLS OPERATING MANUAL FOR SOC PERSONNEL

- ***Operating Procedure for SIEM Solutions – Event Management and Flow Collector/Processor***
- ***Firewall Security Logs***
- ***IDS/IPS Security Logs***
- ***DMZ Jump Server / SSL VPN logs***
- ***Endpoint Security logs (AV, DLP, HIPS)***
- ***User Activity / Login Logs***
- ***Operating Procedure for Policy  and Configuration Compliance***
- ***Operating Procedure for Network Monitoring Systems***
- ***Operating Procedure for Vulnerability Assessment***

# SOC – Processes

***Creating the SOC Processes***

*… now that we have discussed technology, lets discuss processes …*

**SECURITY ALARMS AND ALERT CLASSIFICATION**

- ***Critical Alarms and Alerts with Action Definition***
  ***Non-Critical and Information Alarms***
  ***Alarm reporting and SLA to resolve the alarms***

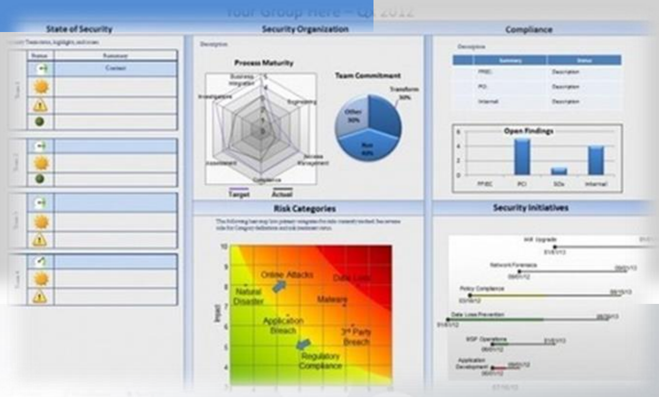
# SOC – Processes

***Creating the SOC Processes***

*… now that we have discussed technology, lets discuss processes …*

**SECURITY METRIC AND DASHBOARD – EXECUTIVE SUMMARY**

- ***Definition of Security Metrics based on Center of Internet Security standards***
- ***Security KPI reporting definition***
- ***Security Balanced Scorecard and Executive Reporting***



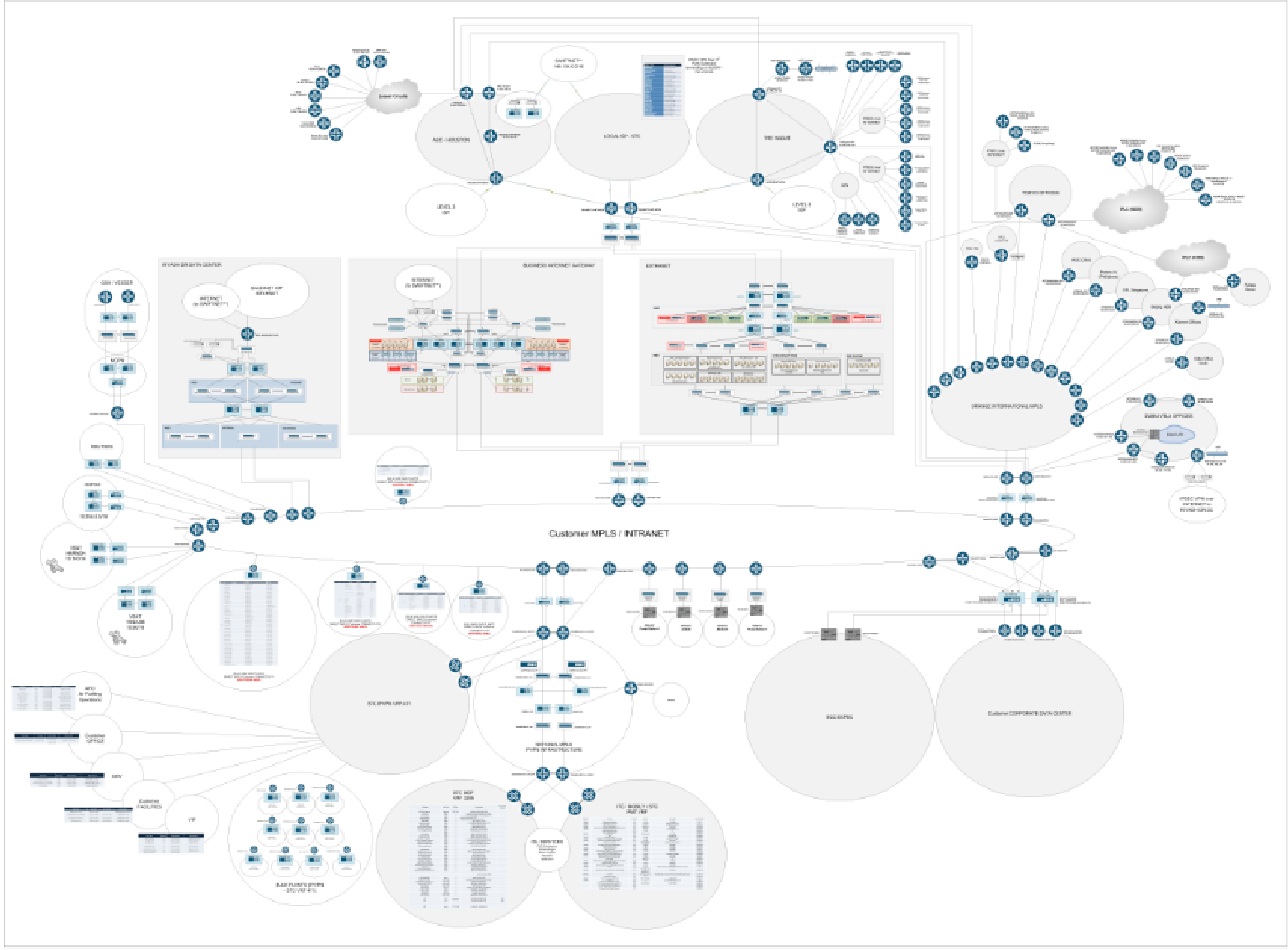
DTS SOLUTION
smart solution for the smart business

# ….Know your infrastructure….

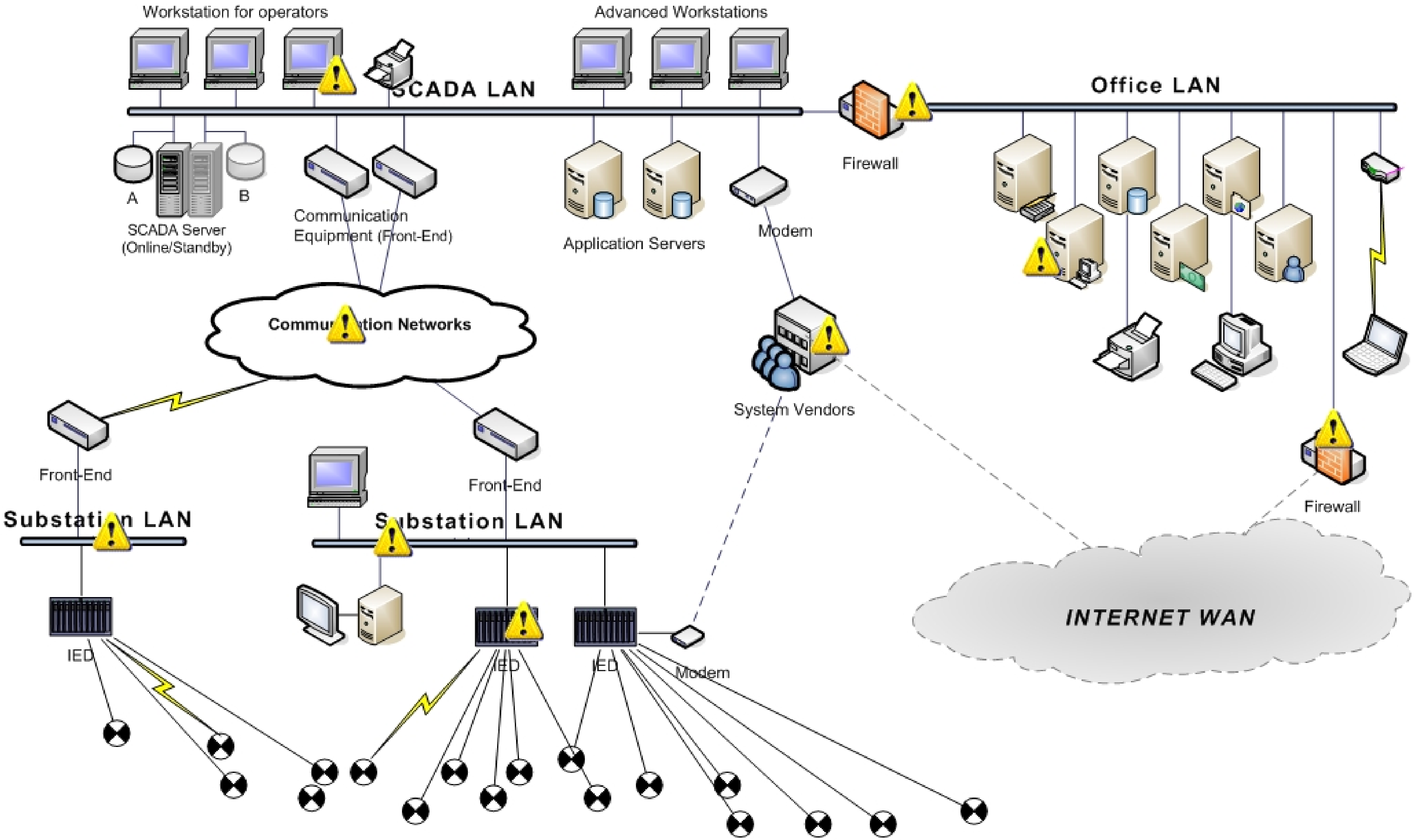
You can only monitor what you know ☺

- Environments
- Location
- Device Types
- System Types
- Security Zones
- Demarcation Points
- Ingress Perimeters
- Data Center
- Extranet
- WAN

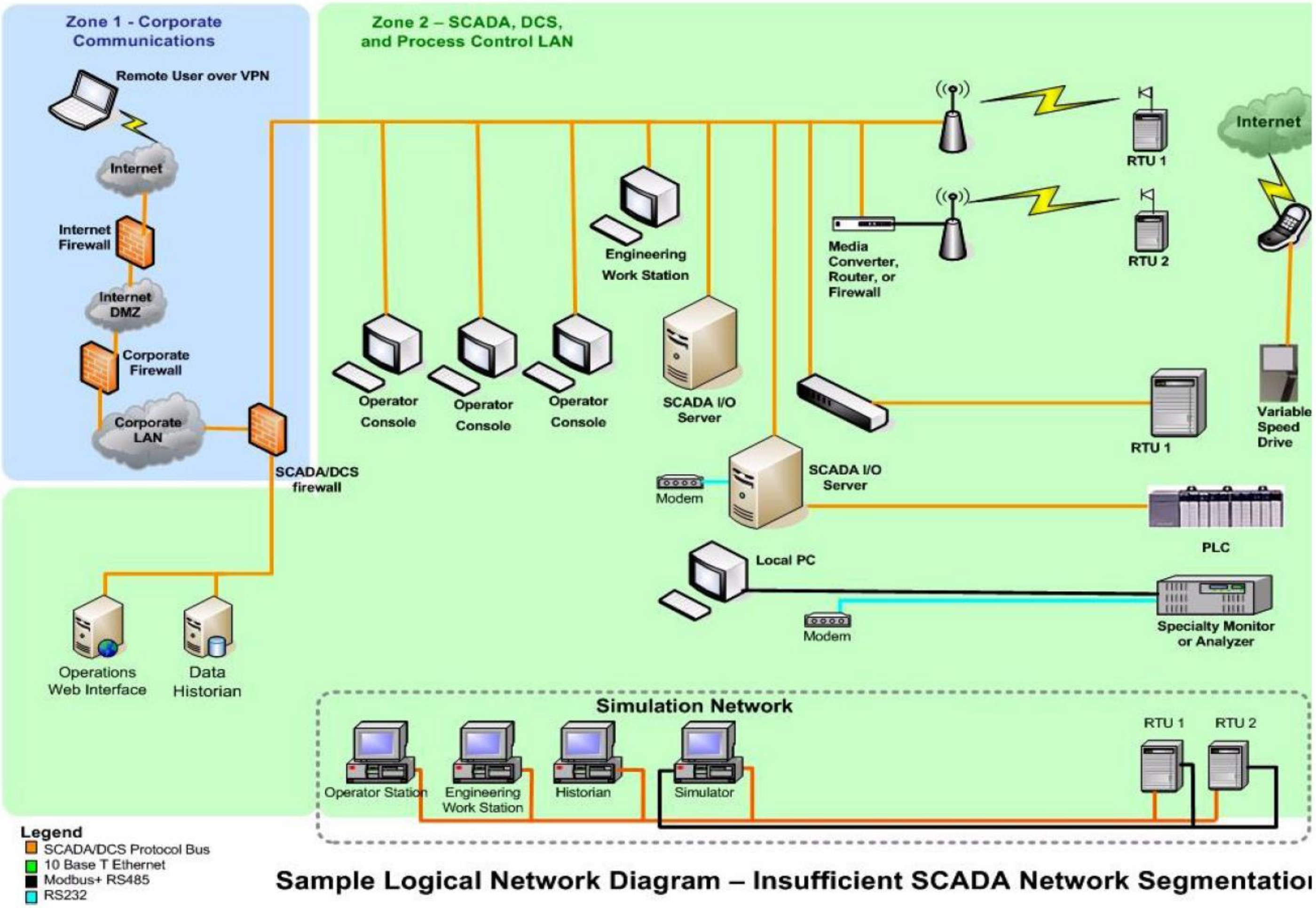
# ….Know your infrastructure….



# Industrial Control Systems Security

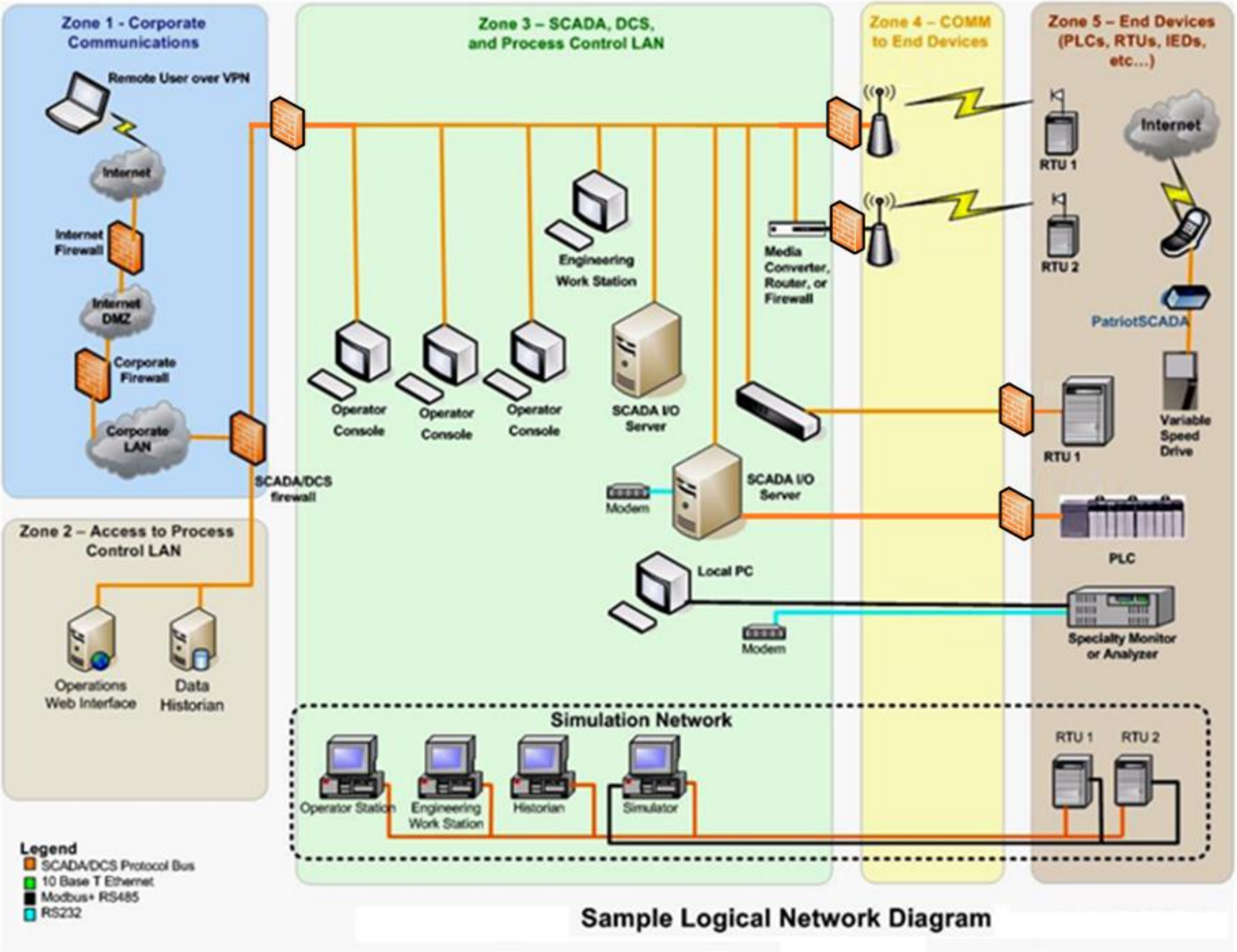


# SCADA Network… What is the problem?



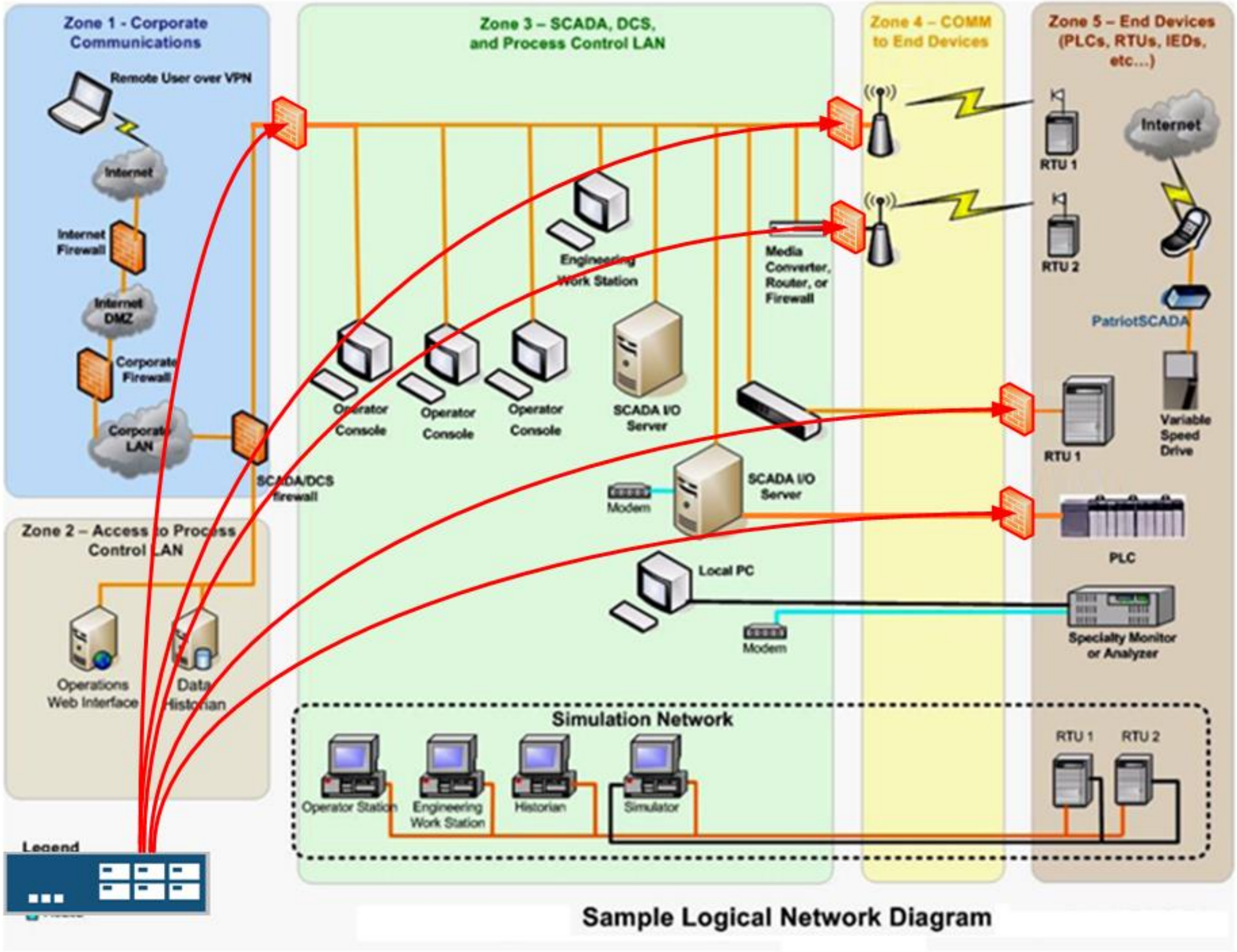
**Sample Logical Network Diagram – Insufficient SCADA Network Segmentatio**

# SCADA Network… Isolation and Zoning



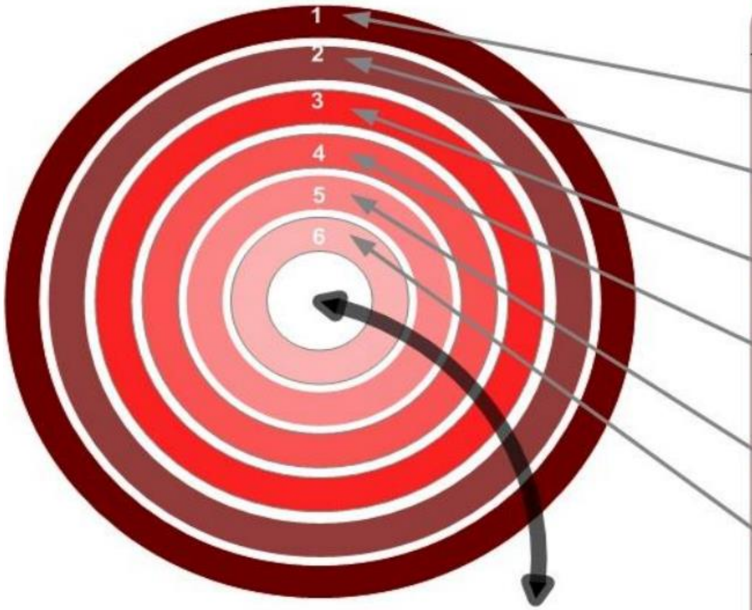
Sample Logical Network Diagram

# SCADA Network… Secured Zones



Sample Logical Network Diagram

# Defense in Depth Strategy



### Technical Controls

1. **Physical Security**
   (Fencing, Surveillance, Guards, Gates, Locks)
2. **Network Infrastructure**
   (Switches, Routers, Firewalls, 3rd Party Connections, and Modems)
3. **Manufacturing IT DMZ**
   (Data Historians, Data Logging, Web Servers)
4. **Mission Critical DCS Servers, Workstations, and Operator Consoles**
   (Operating System Security, Application Security)
5. **Communications to Field Devices**
   (Profibus, Modbus, OPC, and other protocols...)
6. **Field Devices**
   (PLCs, RTUs, IEDs, Plant Equip.)

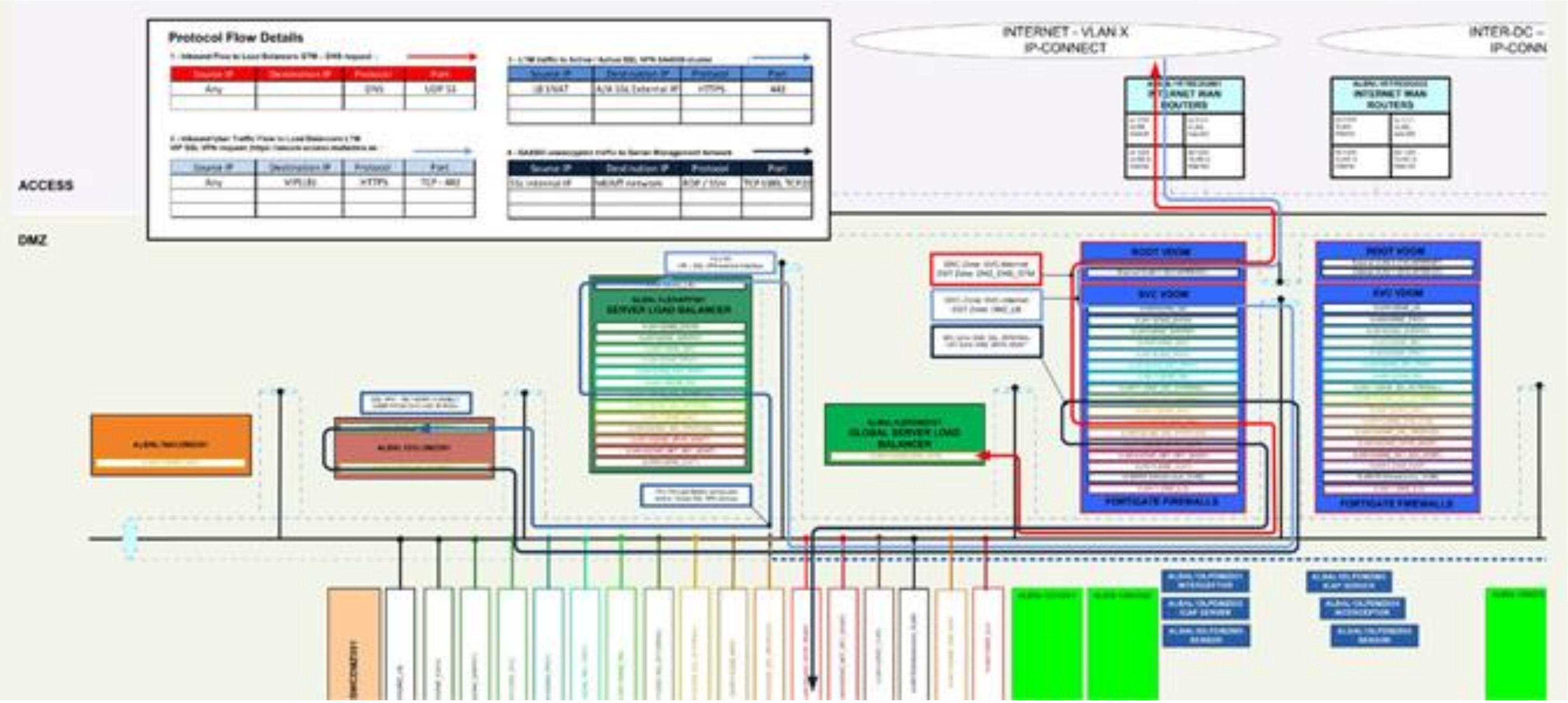
### Procedural Controls

Across all **Six Layers** spans the need for procedural controls that include:

- Governance, Security Policies, Plans, Procedures, and System Ownership
- Asset Inventory, System Documentation, Management of Change, and Test / Development Systems
- Risk Management, Patch Management, Lifecycle Planning, and Routine Assessments
- Crisis Management, Emergency Planning, Safety, and Safe Shutdown Procedures, Backup and Recovery

# …. Service Flows ……

- Knowledge on how service flow across your infrastructure….



| Source IP | Destination IP | Protocol | Port |
|---|---|---|---|
| Any | | DNS | UDP 53 |

| Source IP | Destination IP | Protocol | Port |
|---|---|---|---|
| [illegible] | A/A SSL External IP | HTTPS | 443 |

| Source IP | Destination IP | Protocol | Port |
|---|---|---|---|
| Any | VIP(LB) | HTTPS | TCP - 443 |

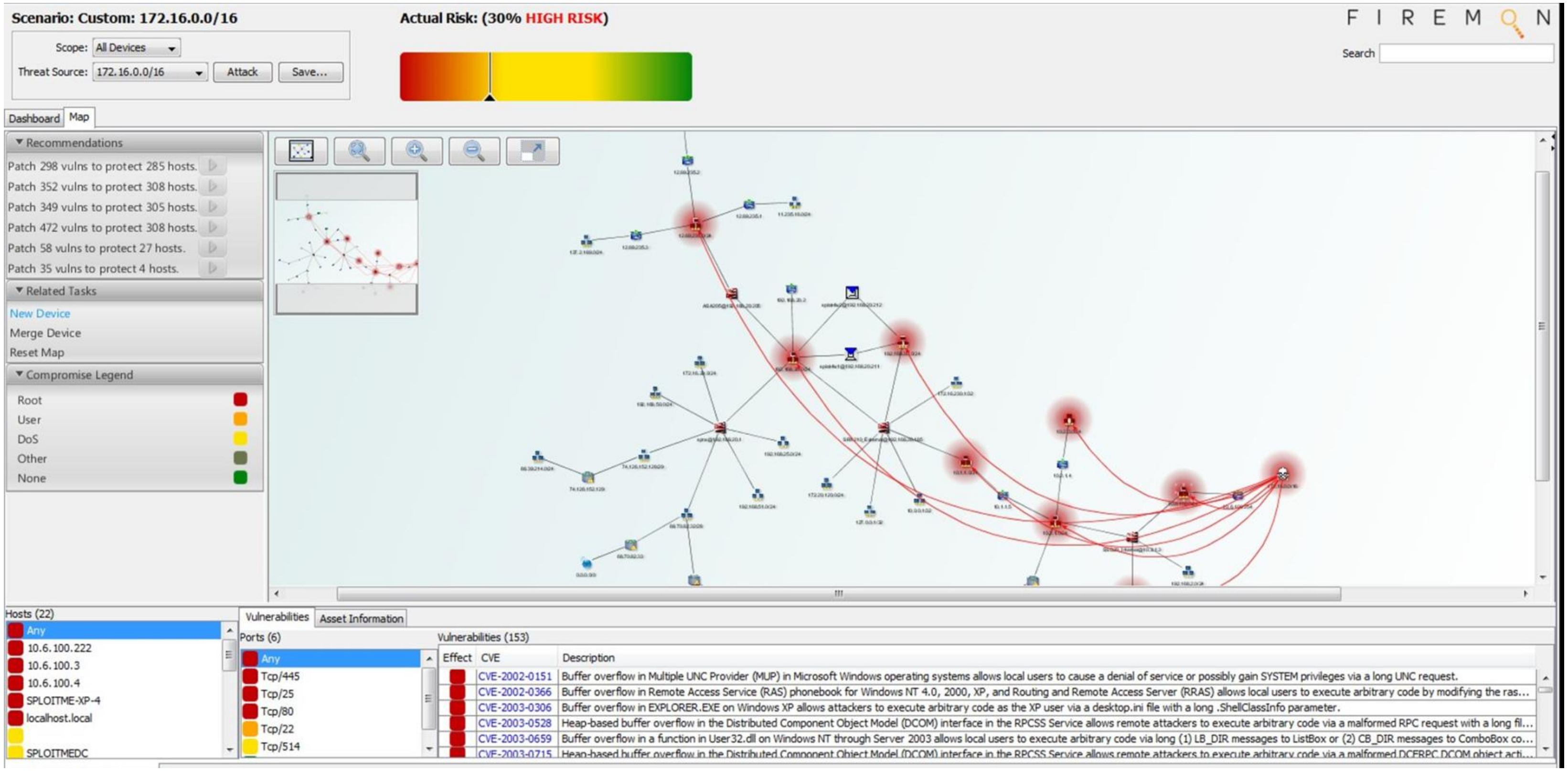
| Source IP | Destination IP | Protocol | Port |
|---|---|---|---|
| SSL internal IP | MGMT network | RDP / SSH | [illegible] |

**BUILD A SECURITY SERVICES CATALOG**

# …. Service Flows ……

- Understanding the service flows will allow you to VISUALIZE…

….. HEAT MAP …..



**Scenario: Custom: 172.16.0.0/16**

Scope: All Devices

Threat Source: 172.16.0.0/16

**Actual Risk: (30% HIGH RISK)**

▼ Recommendations

- Patch 298 vulns to protect 285 hosts.
- Patch 352 vulns to protect 308 hosts.
- Patch 349 vulns to protect 305 hosts.
- Patch 472 vulns to protect 308 hosts.
- Patch 58 vulns to protect 27 hosts.
- Patch 35 vulns to protect 4 hosts.

▼ Related Tasks

- New Device
- Merge Device
- Reset Map

▼ Compromise Legend

| | |
|---|---|
| Root | 🟥 |
| User | 🟧 |
| DoS | 🟨 |
| Other | ▨ |
| None | 🟩 |

Hosts (22)

- 🟥 Any
- 🟥 10.6.100.222
- 🟥 10.6.100.3
- 🟥 10.6.100.4
- 🟥 SPLOITME-XP-4
- 🟥 localhost.local
- 🟨
- 🟨 SPLOITMEDC

Ports (6)

- 🟥 Any
- 🟥 Tcp/445
- 🟥 Tcp/25
- 🟥 Tcp/80
- 🟧 Tcp/22
- 🟨 Tcp/514

Vulnerabilities (153)

| Effect | CVE | Description |
|---|---|---|
| 🟥 | CVE-2002-0151 | Buffer overflow in Multiple UNC Provider (MUP) in Microsoft Windows operating systems allows local users to cause a denial of service or possibly gain SYSTEM privileges via a long UNC request. |
| 🟥 | CVE-2002-0366 | Buffer overflow in Remote Access Service (RAS) phonebook for Windows NT 4.0, 2000, XP, and Routing and Remote Access Server (RRAS) allows local users to execute arbitrary code by modifying the ras... |
| 🟥 | CVE-2003-0306 | Buffer overflow in EXPLORER.EXE on Windows XP allows attackers to execute arbitrary code as the XP user via a desktop.ini file with a long .ShellClassInfo parameter. |
| 🟥 | CVE-2003-0528 | Heap-based buffer overflow in the Distributed Component Object Model (DCOM) interface in the RPCSS Service allows remote attackers to execute arbitrary code via a malformed RPC request with a long fil... |
| 🟥 | CVE-2003-0659 | Buffer overflow in a function in User32.dll on Windows NT through Server 2003 allows local users to execute arbitrary code via long (1) LB_DIR messages to ListBox or (2) CB_DIR messages to ComboBox co... |
| 🟥 | CVE-2003-0715 | Heap-based buffer overflow in the Distributed Component Object Model (DCOM) interface in the RPCSS Service allows remote attackers to execute arbitrary code via a malformed DCERPC DCOM object acti... |

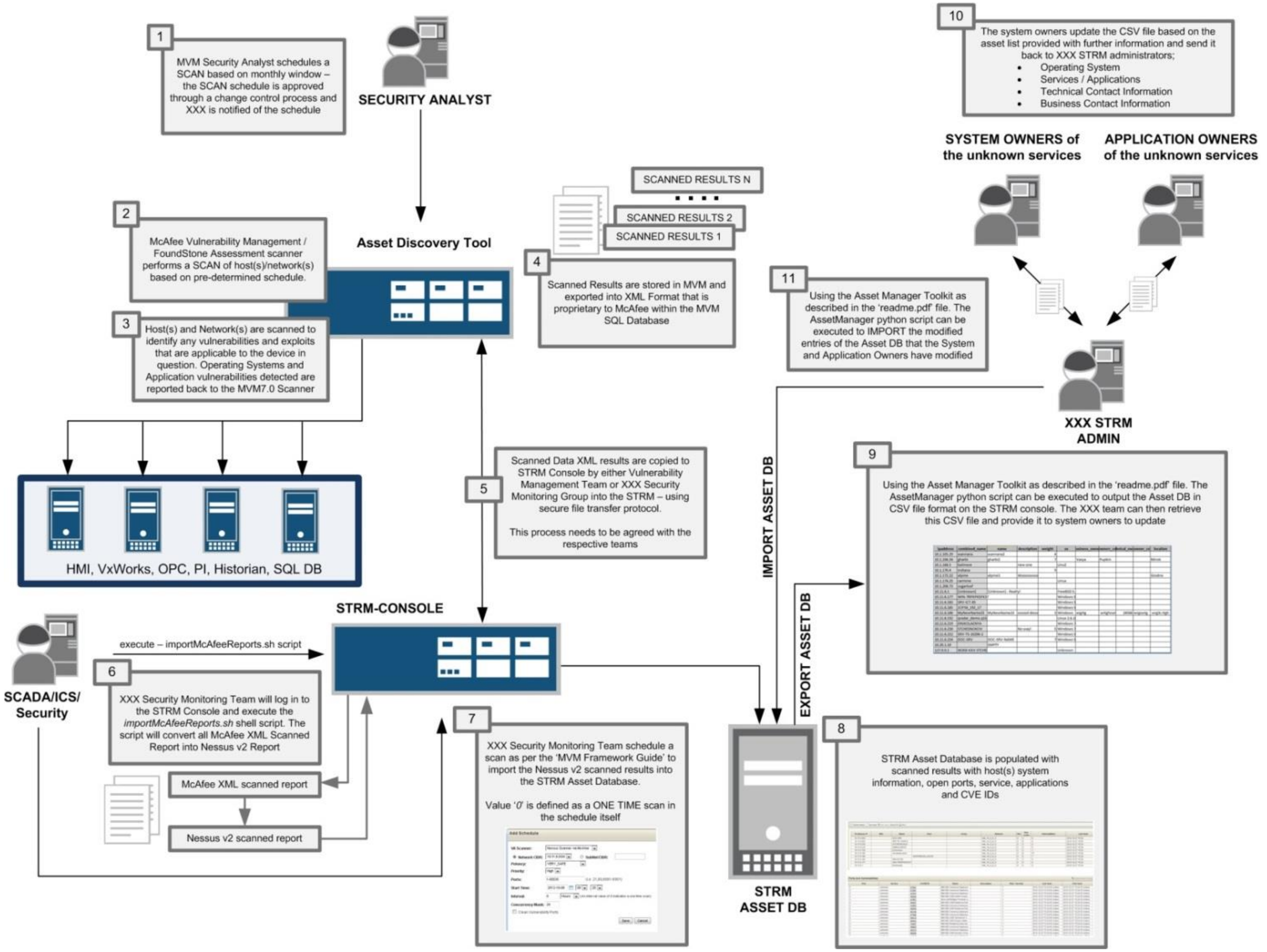
# Build an Asset Repository

Build an Asset Database and Integrated into SIEM;

Following asset details can be adjusted with Asset Manager:

- Name
- Description
- Weight
- Operating System
- Business Owner
- Business Owner Contact Information
- Technical Owner
- Technical Owner Contact Information
- Location

# SCADA / ICS – ASSET REPOSITORY



1 MVM Security Analyst schedules a SCAN based on monthly window – the SCAN schedule is approved through a change control process and XXX is notified of the schedule

2 McAfee Vulnerability Management / FoundStone Assessment scanner performs a SCAN of host(s)/network(s) based on pre-determined schedule.

3 Host(s) and Network(s) are scanned to identify any vulnerabilities and exploits that are applicable to the device in question. Operating Systems and Application vulnerabilities detected are reported back to the MVM7.0 Scanner

4 Scanned Results are stored in MVM and exported into XML Format that is proprietary to McAfee within the MVM SQL Database

5 Scanned Data XML results are copied to STRM Console by either Vulnerability Management Team or XXX Security Monitoring Group into the STRM – using secure file transfer protocol.

This process needs to be agreed with the respective teams

6 XXX Security Monitoring Team will log in to the STRM Console and execute the *importMcAfeeReports.sh* shell script. The script will convert all McAfee XML Scanned Report into Nessus v2 Report

7 XXX Security Monitoring Team schedule a scan as per the 'MVM Framework Guide' to import the Nessus v2 scanned results into the STRM Asset Database.

Value '*0*' is defined as a ONE TIME scan in the schedule itself

8 STRM Asset Database is populated with scanned results with host(s) system information, open ports, service, applications and CVE IDs

9 Using the Asset Manager Toolkit as described in the 'readme.pdf' file. The AssetManager python script can be executed to output the Asset DB in CSV file format on the STRM console. The XXX team can then retrieve this CSV file and provide it to system owners to update

10 The system owners update the CSV file based on the asset list provided with further information and send it back to XXX STRM administrators;

- Operating System
- Services / Applications
- Technical Contact Information
- Business Contact Information

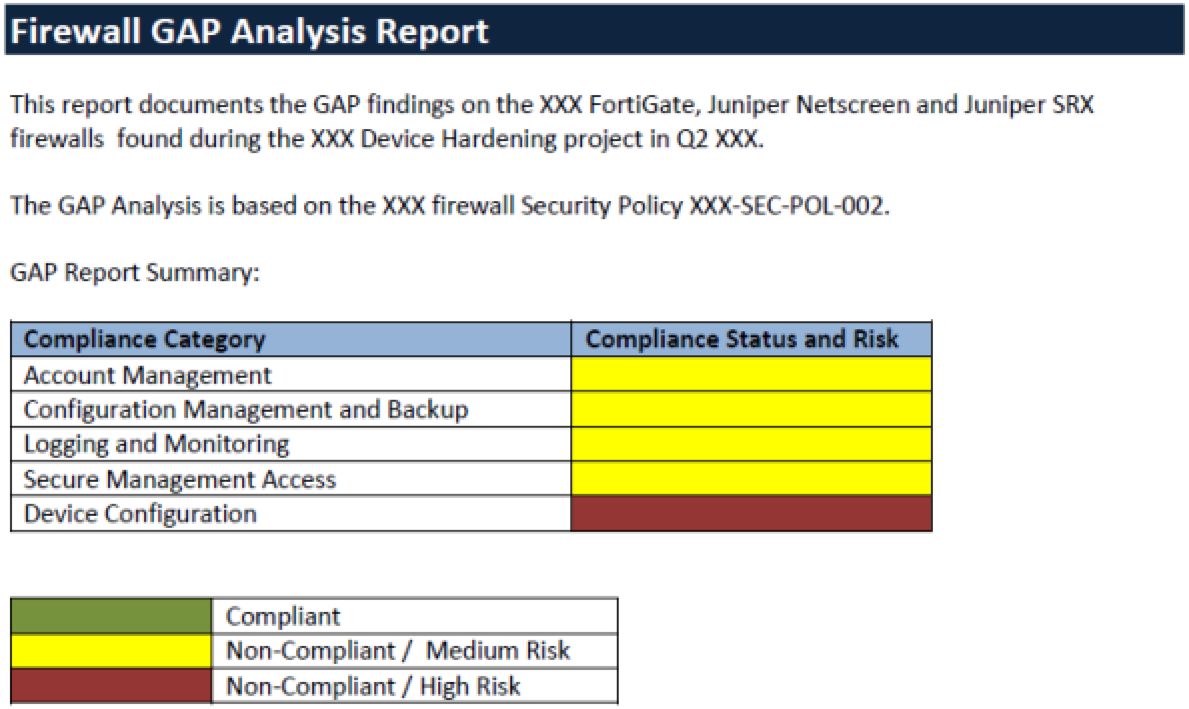
11 Using the Asset Manager Toolkit as described in the 'readme.pdf' file. The AssetManager python script can be executed to IMPORT the modified entries of the Asset DB that the System and Application Owners have modified

# Develop Threat Cases

Now that we have the processes, technology and people what next…..

- Build contextual threat cases per environment;
  - Extranet
  - Internet
  - Intranet
  - Data Center
  - Active Directory
  - Malware / Virus Infection and Propagation
  - NetFlow Analysis
  - Remote Sites / WAN
  - Remote Access – IPSEC VPN / SSL VPN
  - Wireless
  - etc…..

# Sample: Firewall GAP Analysis Report



## Firewall GAP Analysis Report

This report documents the GAP findings on the XXX FortiGate, Juniper Netscreen and Juniper SRX firewalls  found during the XXX Device Hardening project in Q2 XXX.

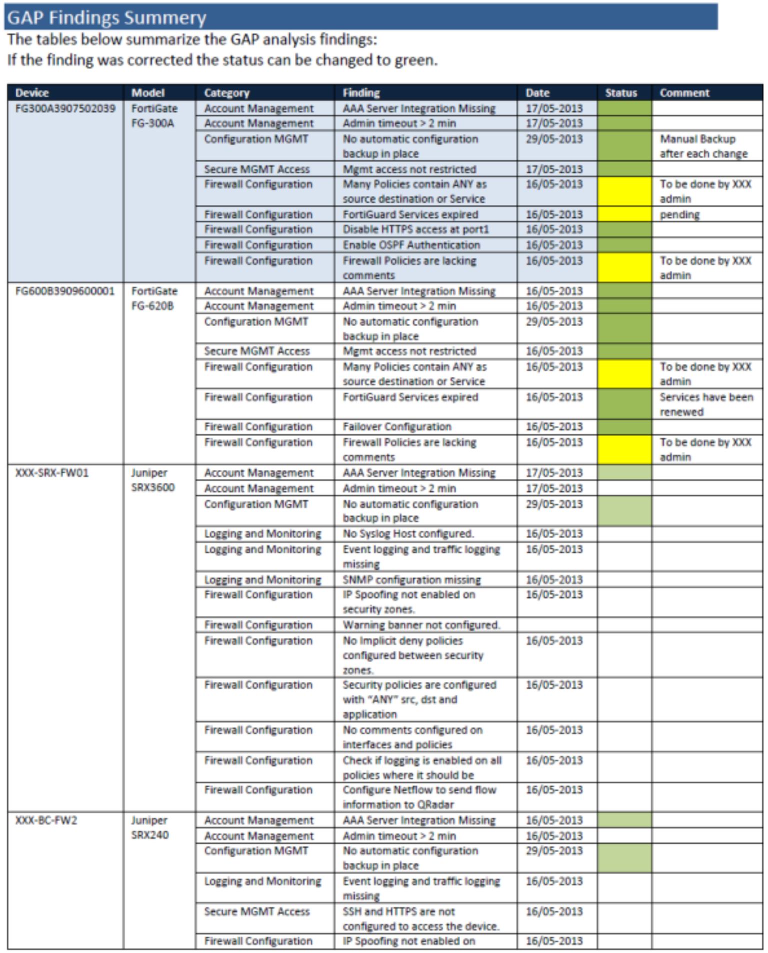
The GAP Analysis is based on the XXX firewall Security Policy XXX-SEC-POL-002.

GAP Report Summary:

| Compliance Category | Compliance Status and Risk |
|---|---|
| Account Management | 🟨 |
| Configuration Management and Backup | 🟨 |
| Logging and Monitoring | 🟨 |
| Secure Management Access | 🟨 |
| Device Configuration | 🟥 |

| | |
|---|---|
| 🟩 | Compliant |
| 🟨 | Non-Compliant /  Medium Risk |
| 🟥 | Non-Compliant / High Risk |

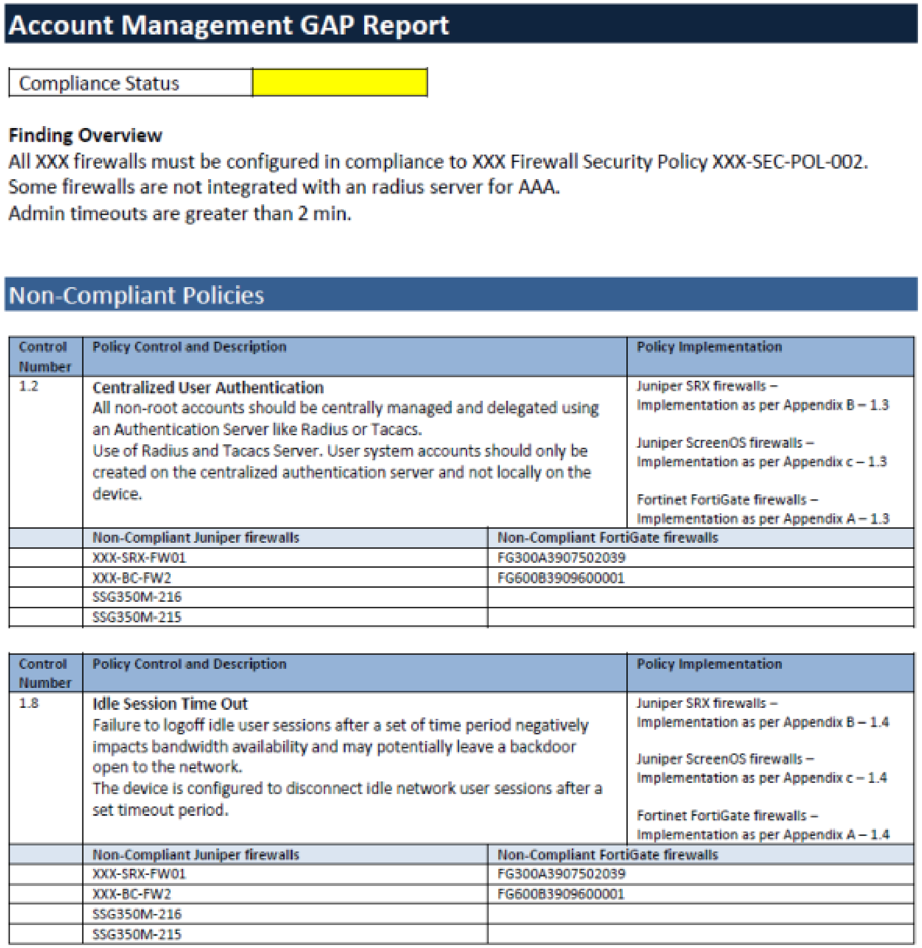
# Sample: Firewall GAP Analysis Report



## GAP Findings Summery

The tables below summarize the GAP analysis findings:
If the finding was corrected the status can be changed to green.

| Device | Model | Category | Finding | Date | Status | Comment |
|---|---|---|---|---|---|---|
| FG300A3907502039 | FortiGate FG-300A | Account Management | AAA Server Integration Missing | 17/05-2013 | 🟩 | |
| | | Account Management | Admin timeout > 2 min | 17/05-2013 | 🟩 | |
| | | Configuration MGMT | No automatic configuration backup in place | 29/05-2013 | 🟩 | Manual Backup after each change |
| | | Secure MGMT Access | Mgmt access not restricted | 17/05-2013 | 🟩 | |
| | | Firewall Configuration | Many Policies contain ANY as source destination or Service | 16/05-2013 | 🟨 | To be done by XXX admin |
| | | Firewall Configuration | FortiGuard Services expired | 16/05-2013 | 🟨 | pending |
| | | Firewall Configuration | Disable HTTPS access at port1 | 16/05-2013 | 🟩 | |
| | | Firewall Configuration | Enable OSPF Authentication | 16/05-2013 | 🟩 | |
| | | Firewall Configuration | Firewall Policies are lacking comments | 16/05-2013 | 🟨 | To be done by XXX admin |
| FG600B3909600001 | FortiGate FG-620B | Account Management | AAA Server Integration Missing | 16/05-2013 | 🟩 | |
| | | Account Management | Admin timeout > 2 min | 16/05-2013 | 🟩 | |
| | | Configuration MGMT | No automatic configuration backup in place | 29/05-2013 | 🟩 | |
| | | Secure MGMT Access | Mgmt access not restricted | 16/05-2013 | 🟩 | |
| | | Firewall Configuration | Many Policies contain ANY as source destination or Service | 16/05-2013 | 🟨 | To be done by XXX admin |
| | | Firewall Configuration | FortiGuard Services expired | 16/05-2013 | 🟩 | Services have been renewed |
| | | Firewall Configuration | Failover Configuration | 16/05-2013 | 🟩 | |
| | | Firewall Configuration | Firewall Policies are lacking comments | 16/05-2013 | 🟨 | To be done by XXX admin |
| XXX-SRX-FW01 | Juniper SRX3600 | Account Management | AAA Server Integration Missing | 17/05-2013 | 🟩 | |
| | | Account Management | Admin timeout > 2 min | 17/05-2013 | | |
| | | Configuration MGMT | No automatic configuration backup in place | 29/05-2013 | 🟩 | |
| | | Logging and Monitoring | No Syslog Host configured. | 16/05-2013 | | |
| | | Logging and Monitoring | Event logging and traffic logging missing | 16/05-2013 | | |
| | | Logging and Monitoring | SNMP configuration missing | 16/05-2013 | | |
| | | Firewall Configuration | IP Spoofing not enabled on security zones. | 16/05-2013 | | |
| | | Firewall Configuration | Warning banner not configured. | | | |
| | | Firewall Configuration | No Implicit deny policies configured between security zones. | 16/05-2013 | | |
| | | Firewall Configuration | Security policies are configured with "ANY" src, dst and application | 16/05-2013 | | |
| | | Firewall Configuration | No comments configured on interfaces and policies | 16/05-2013 | | |
| | | Firewall Configuration | Check if logging is enabled on all policies where it should be | 16/05-2013 | | |
| | | Firewall Configuration | Configure Netflow to send flow information to QRadar | 16/05-2013 | | |
| XXX-BC-FW2 | Juniper SRX240 | Account Management | AAA Server Integration Missing | 16/05-2013 | 🟩 | |
| | | Account Management | Admin timeout > 2 min | 16/05-2013 | | |
| | | Configuration MGMT | No automatic configuration backup in place | 29/05-2013 | 🟩 | |
| | | Logging and Monitoring | Event logging and traffic logging missing | 16/05-2013 | | |
| | | Secure MGMT Access | SSH and HTTPS are not configured to access the device. | 16/05-2013 | | |
| | | Firewall Configuration | IP Spoofing not enabled on | 16/05-2013 | | |



## Account Management GAP Report

| | |
|---|---|
| Compliance Status | 🟨 |

**Finding Overview**

All XXX firewalls must be configured in compliance to XXX Firewall Security Policy XXX-SEC-POL-002.
Some firewalls are not integrated with an radius server for AAA.
Admin timeouts are greater than 2 min.

## Non-Compliant Policies

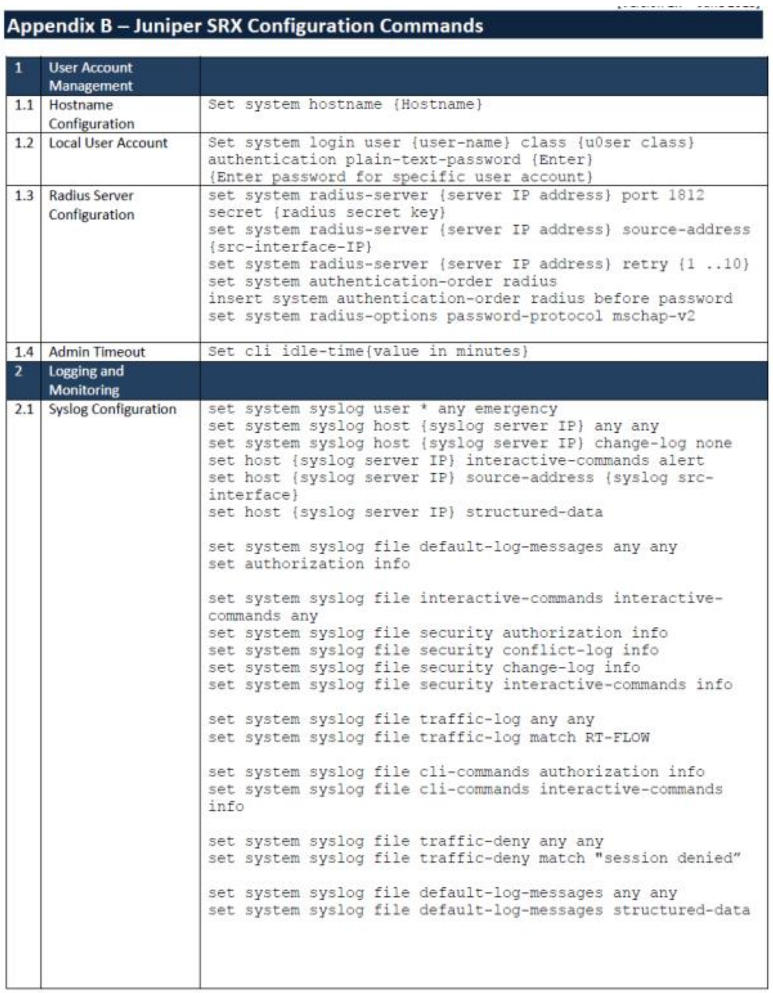
| Control Number | Policy Control and Description | Policy Implementation |
|---|---|---|
| 1.2 | **Centralized User Authentication**<br>All non-root accounts should be centrally managed and delegated using an Authentication Server like Radius or Tacacs.<br>Use of Radius and Tacacs Server. User system accounts should only be created on the centralized authentication server and not locally on the device. | Juniper SRX firewalls – Implementation as per Appendix B – 1.3<br>Juniper ScreenOS firewalls – Implementation as per Appendix c – 1.3<br>Fortinet FortiGate firewalls – Implementation as per Appendix A – 1.3 |

| | Non-Compliant Juniper firewalls | Non-Compliant FortiGate firewalls |
|---|---|---|
| | XXX-SRX-FW01 | FG300A3907502039 |
| | XXX-BC-FW2 | FG600B3909600001 |
| | SSG350M-216 | |
| | SSG350M-215 | |

| Control Number | Policy Control and Description | Policy Implementation |
|---|---|---|
| 1.8 | **Idle Session Time Out**<br>Failure to logoff idle user sessions after a set of time period negatively impacts bandwidth availability and may potentially leave a backdoor open to the network.<br>The device is configured to disconnect idle network user sessions after a set timeout period. | Juniper SRX firewalls – Implementation as per Appendix B – 1.4<br>Juniper ScreenOS firewalls – Implementation as per Appendix c – 1.4<br>Fortinet FortiGate firewalls – Implementation as per Appendix A – 1.4 |

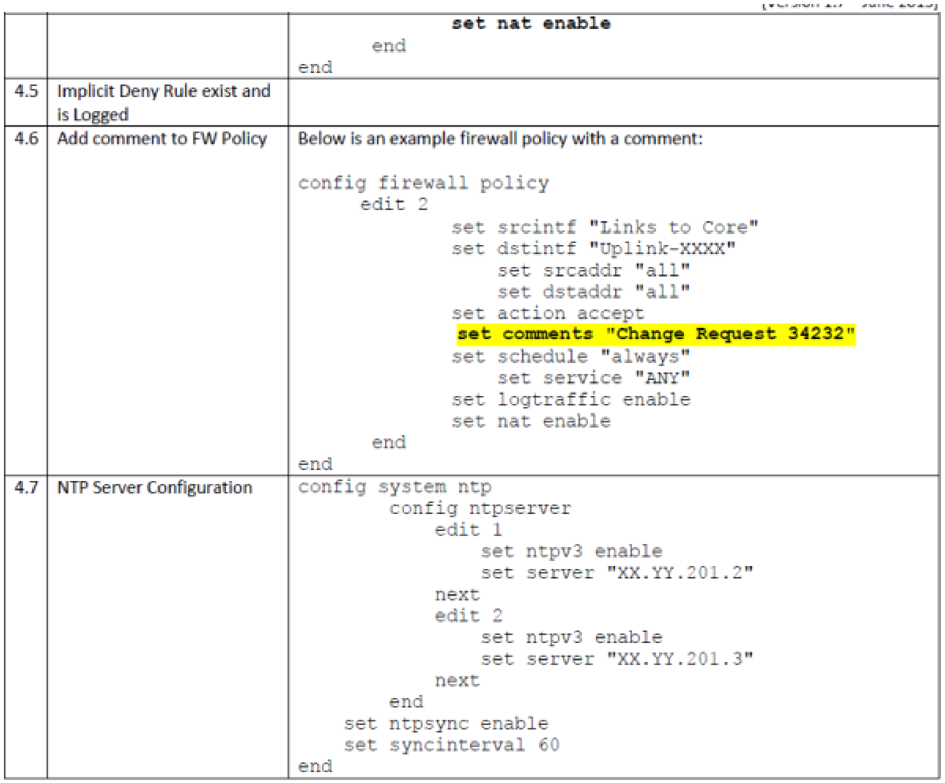
| | Non-Compliant Juniper firewalls | Non-Compliant FortiGate firewalls |
|---|---|---|
| | XXX-SRX-FW01 | FG300A3907502039 |
| | XXX-BC-FW2 | FG600B3909600001 |
| | SSG350M-216 | |
| | SSG350M-215 | |

# Sample: Firewall GAP Analysis Report



## Appendix B – Juniper SRX Configuration Commands

| | | |
|---|---|---|
| 1 | User Account Management | |
| 1.1 | Hostname Configuration | `Set system hostname {Hostname}` |
| 1.2 | Local User Account | `Set system login user {user-name} class {u0ser class} authentication plain-text-password {Enter}`<br>`{Enter password for specific user account}` |
| 1.3 | Radius Server Configuration | `set system radius-server {server IP address} port 1812 secret {radius secret key}`<br>`set system radius-server {server IP address} source-address {src-interface-IP}`<br>`set system radius-server {server IP address} retry {1 ..10}`<br>`set system authentication-order radius`<br>`insert system authentication-order radius before password`<br>`set system radius-options password-protocol mschap-v2` |
| 1.4 | Admin Timeout | `Set cli idle-time{value in minutes}` |
| 2 | Logging and Monitoring | |
| 2.1 | Syslog Configuration | `set system syslog user * any emergency`<br>`set system syslog host {syslog server IP} any any`<br>`set system syslog host {syslog server IP} change-log none`<br>`set host {syslog server IP} interactive-commands alert`<br>`set host {syslog server IP} source-address {syslog src-interface}`<br>`set host {syslog server IP} structured-data`<br><br>`set system syslog file default-log-messages any any`<br>`set authorization info`<br><br>`set system syslog file interactive-commands interactive-commands any`<br>`set system syslog file security authorization info`<br>`set system syslog file security conflict-log info`<br>`set system syslog file security change-log info`<br>`set system syslog file security interactive-commands info`<br><br>`set system syslog file traffic-log any any`<br>`set system syslog file traffic-log match RT-FLOW`<br><br>`set system syslog file cli-commands authorization info`<br>`set system syslog file cli-commands interactive-commands info`<br><br>`set system syslog file traffic-deny any any`<br>`set system syslog file traffic-deny match "session denied"`<br><br>`set system syslog file default-log-messages any any`<br>`set system syslog file default-log-messages structured-data` |



| | | |
|---|---|---|
| | | `set nat enable`<br>`end`<br>`end` |
| 4.5 | Implicit Deny Rule exist and is Logged | |
| 4.6 | Add comment to FW Policy | Below is an example firewall policy with a comment:<br><br>`config firewall policy`<br>`edit 2`<br>`set srcintf "Links to Core"`<br>`set dstintf "Uplink-XXXX"`<br>`set srcaddr "all"`<br>`set dstaddr "all"`<br>`set action accept`<br>**`set comments "Change Request 34232"`**<br>`set schedule "always"`<br>`set service "ANY"`<br>`set logtraffic enable`<br>`set nat enable`<br>`end`<br>`end` |
| 4.7 | NTP Server Configuration | `config system ntp`<br>`config ntpserver`<br>`edit 1`<br>`set ntpv3 enable`<br>`set server "XX.YY.201.2"`<br>`next`<br>`edit 2`<br>`set ntpv3 enable`<br>`set server "XX.YY.201.3"`<br>`next`<br>`end`<br>`set ntpsync enable`<br>`set syncinterval 60`<br>`end` |

# ADVANCED THREAT CASES - ENVIRONMENT

- To define threat cases per environment … not by system…. (silo)
  - CONTEXTUAL
  - SERVICE ORIENTATED
  - USER CENTRIC

| ID | Threat Case Development |
|---|---|
| **OS.WIN** | Microsoft Windows Servers - Threat Case Development Documentation<br>Microsoft Active Directory - Threat Case Development Documentation |
| **MSIIS**<br>**MSSQL**<br>**MSEXC** | Microsoft Application - Threat Case Development Documentation<br>• IIS<br>• MSSQL<br>• Exchange |
| **IBMAIX**<br>**LINUX**<br>**SOLARIS** | UNIX/LINUX/SOLARIS/AIX – Threat Case Development Documentation |
| **PRIVACC** | Advanced Threat Cases for Privileged User and Special Account Activity and Monitoring |
| **N/A** | Baseline Security Settings on UNIX/LINUX/SOLARIS/AIX server |
| **BUSINT** | Business Internet |
| **EXTRNT** | Extranet |
| **S2SVPN** | Site to Site VPN |

# ADVANCED THREAT CASES - ENVIRONMENT

- To define threat cases per environment …
  …. Eventually …. Should …. Include …. All …. Environment …..

| ID | Threat Case Development |
|---|---|
| INTOFF | International Offices – Global MPLS |
| SSLVPN | Juniper SSL VPN |
| NATIONAL | IPVPN –National MPLS IPVPN |
| WIRLESS | Wireless Infrastructure |
| VOIPUC | Voice over IP |
| VSAT | VSAT – Satellite |
| DIGPKI | PKI and X.509 Digital Certificates (systems threat case) |
| AAA | AAA (systems threat case) |
| HIPS | HIPS (system threat case and ePO integration) |
| EXECACC | Executive Account Monitoring |
| SAP | SAP Router and SAP Privilege Activity Monitoring |
| COMPLIANCE | Compliance and Best Practices Configuration |
| NAC | Network Admission Control – |

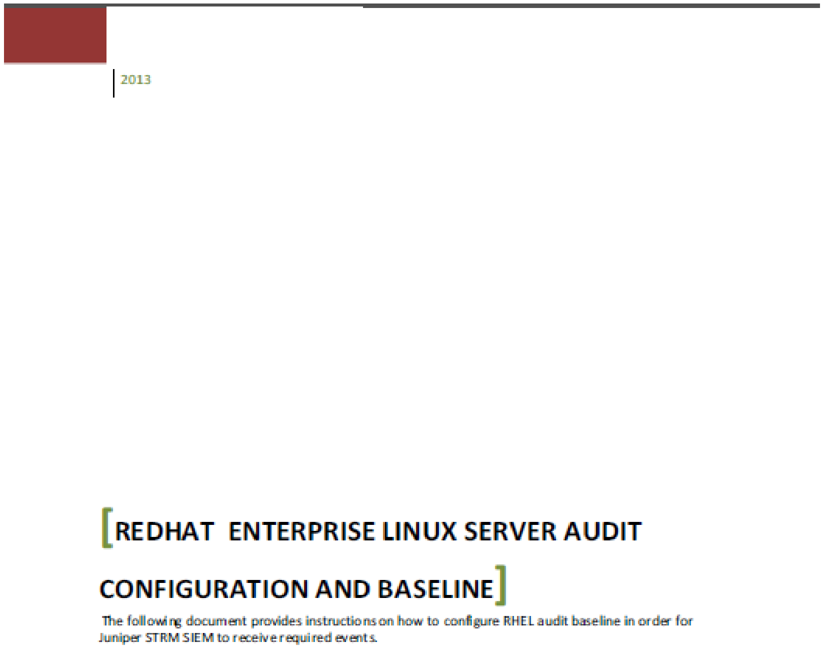
# ADVANCED THREAT CASES - ENVIRONMENT

- To define threat cases per environment …
  …. Eventually …. Should …. Include …. All …. Environment …..

| ID | Threat Case Development |
|---|---|
| **IPS-AV** | IPS and AV Management Console |
| **EMAIL** | Email Security – Business Internet Gateway |
| **DAM** | Database Activity Monitoring (DAM) |
| **SFT** | Secure File Transfer |

- *IMPORTANT – understand the environment and understand the threats related to those environment…..*

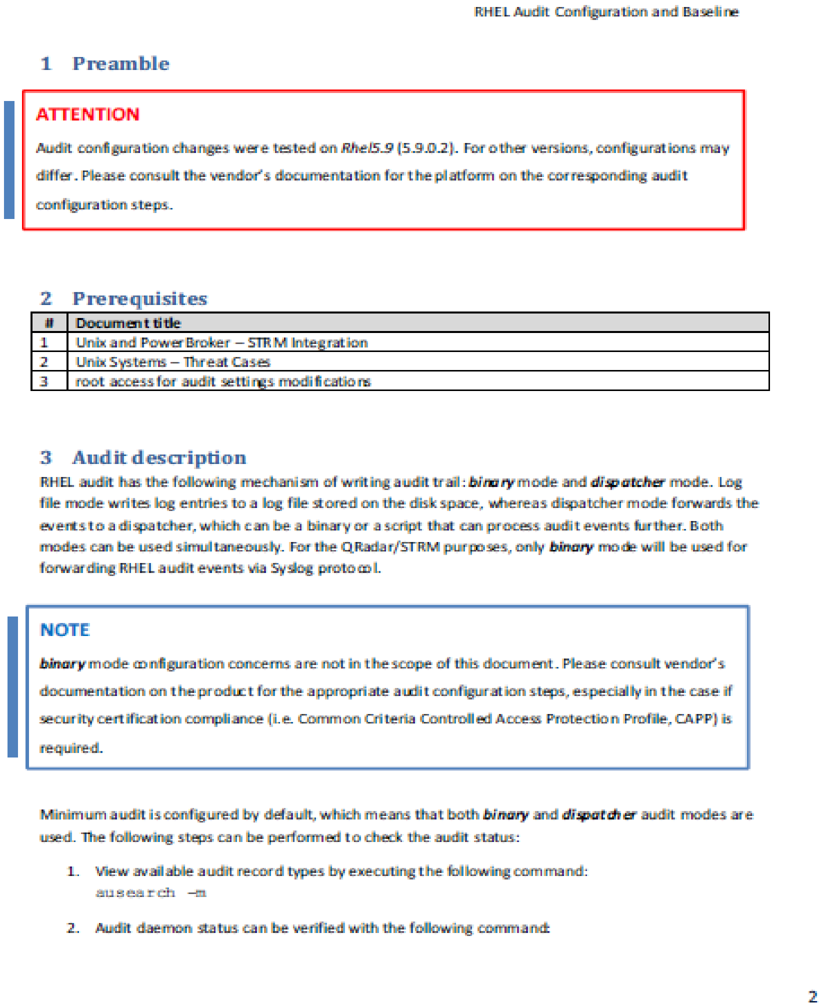
# Develop Threat Cases – RHEL



2013

[REDHAT ENTERPRISE LINUX SERVER AUDIT CONFIGURATION AND BASELINE]

The following document provides instructions on how to configure RHEL audit baseline in order for Juniper STRM SIEM to receive required events.



RHEL Audit Configuration and Baseline

## 1 Preamble

**ATTENTION**

Audit configuration changes were tested on *Rhel5.9* (5.9.0.2). For other versions, configurations may differ. Please consult the vendor's documentation for the platform on the corresponding audit configuration steps.

## 2 Prerequisites

| # | Document title |
|---|---|
| 1 | Unix and Power Broker – STRM Integration |
| 2 | Unix Systems – Threat Cases |
| 3 | root access for audit settings modifications |

## 3 Audit description

RHEL audit has the following mechanism of writing audit trail: ***binary*** mode and ***dispatcher*** mode. Log file mode writes log entries to a log file stored on the disk space, whereas dispatcher mode forwards the events to a dispatcher, which can be a binary or a script that can process audit events further. Both modes can be used simultaneously. For the QRadar/STRM purposes, only ***binary*** mode will be used for forwarding RHEL audit events via Syslog protocol.

**NOTE**

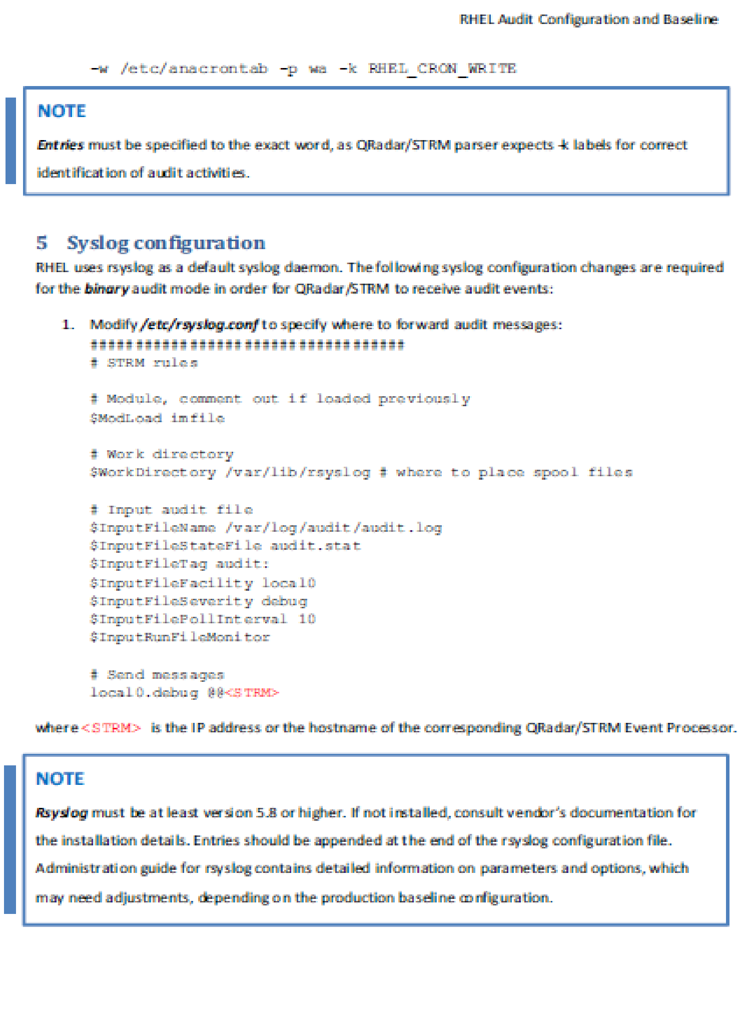
***binary*** mode configuration concerns are not in the scope of this document. Please consult vendor's documentation on the product for the appropriate audit configuration steps, especially in the case if security certification compliance (i.e. Common Criteria Controlled Access Protection Profile, CAPP) is required.

Minimum audit is configured by default, which means that both ***binary*** and ***dispatcher*** audit modes are used. The following steps can be performed to check the audit status:

1. View available audit record types by executing the following command:
   ```
   ausearch –m
   ```
2. Audit daemon status can be verified with the following command:

2

# Develop Threat Cases – RHEL



```
-w /etc/anacrontab -p wa -k RHEL_CRON_WRITE
```

**NOTE**

***Entries*** must be specified to the exact word, as QRadar/STRM parser expects -k labels for correct identification of audit activities.

## 5 Syslog configuration

RHEL uses rsyslog as a default syslog daemon. The following syslog configuration changes are required for the ***binary*** audit mode in order for QRadar/STRM to receive audit events:

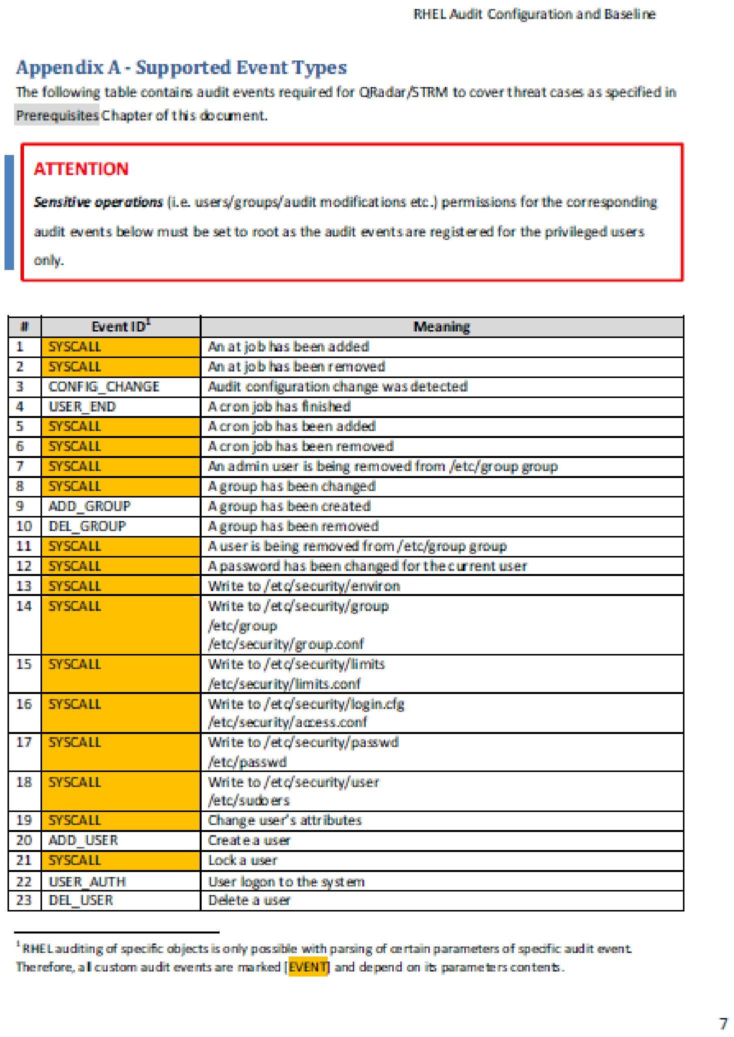
1. Modify ***/etc/rsyslog.conf*** to specify where to forward audit messages:

```
##################################
# STRM rules

# Module, comment out if loaded previously
$ModLoad imfile

# Work directory
$WorkDirectory /var/lib/rsyslog # where to place spool files

# Input audit file
$InputFileName /var/log/audit/audit.log
$InputFileStateFile audit.stat
$InputFileTag audit:
$InputFileFacility local0
$InputFileSeverity debug
$InputFilePollInterval 10
$InputRunFileMonitor

# Send messages
local0.debug @@<STRM>
```

where <STRM> is the IP address or the hostname of the corresponding QRadar/STRM Event Processor.

**NOTE**

***Rsyslog*** must be at least version 5.8 or higher. If not installed, consult vendor's documentation for the installation details. Entries should be appended at the end of the rsyslog configuration file. Administration guide for rsyslog contains detailed information on parameters and options, which may need adjustments, depending on the production baseline configuration.



## Appendix A - Supported Event Types

The following table contains audit events required for QRadar/STRM to cover threat cases as specified in Prerequisites Chapter of this document.

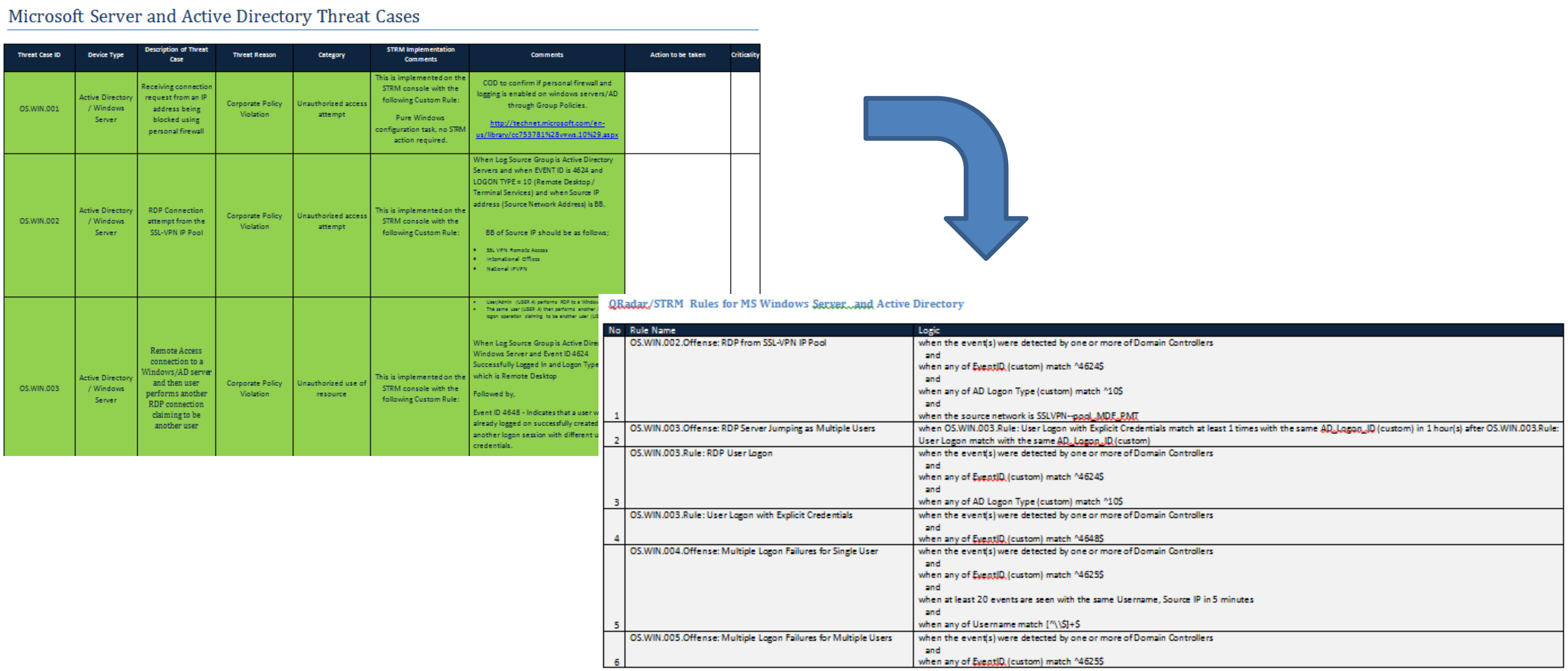
**ATTENTION**

***Sensitive operations*** (i.e. users/groups/audit modifications etc.) permissions for the corresponding audit events below must be set to root as the audit events are registered for the privileged users only.

| # | Event ID[1] | Meaning |
|---|---|---|
| 1 | SYSCALL | An at job has been added |
| 2 | SYSCALL | An at job has been removed |
| 3 | CONFIG_CHANGE | Audit configuration change was detected |
| 4 | USER_END | A cron job has finished |
| 5 | SYSCALL | A cron job has been added |
| 6 | SYSCALL | A cron job has been removed |
| 7 | SYSCALL | An admin user is being removed from /etc/group group |
| 8 | SYSCALL | A group has been changed |
| 9 | ADD_GROUP | A group has been created |
| 10 | DEL_GROUP | A group has been removed |
| 11 | SYSCALL | A user is being removed from /etc/group group |
| 12 | SYSCALL | A password has been changed for the current user |
| 13 | SYSCALL | Write to /etc/security/environ |
| 14 | SYSCALL | Write to /etc/security/group<br>/etc/group<br>/etc/security/group.conf |
| 15 | SYSCALL | Write to /etc/security/limits<br>/etc/security/limits.conf |
| 16 | SYSCALL | Write to /etc/security/login.cfg<br>/etc/security/access.conf |
| 17 | SYSCALL | Write to /etc/security/passwd<br>/etc/passwd |
| 18 | SYSCALL | Write to /etc/security/user<br>/etc/sudoers |
| 19 | SYSCALL | Change user's attributes |
| 20 | ADD_USER | Create a user |
| 21 | SYSCALL | Lock a user |
| 22 | USER_AUTH | User logon to the system |
| 23 | DEL_USER | Delete a user |

[1] RHEL auditing of specific objects is only possible with parsing of certain parameters of specific audit event. Therefore, all custom audit events are marked [EVENT] and depend on its parameters contents.

# Develop Threat Cases – Windows Servers



Microsoft Server and Active Directory Threat Cases

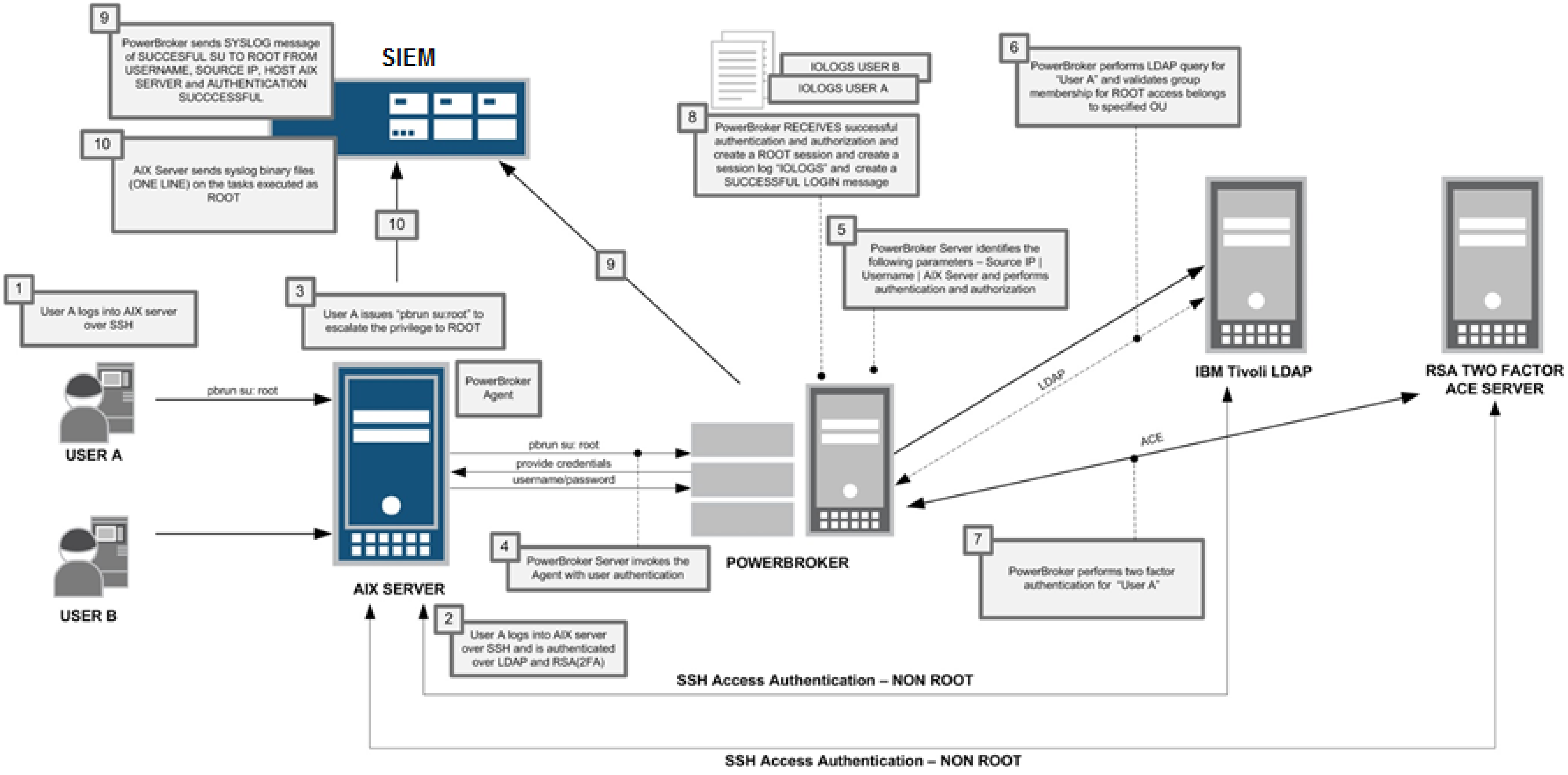
| Threat Case ID | Device Type | Description of Threat Case | Threat Reason | Category | STRM Implementation Comments | Comments | Action to be taken | Criticality |
|---|---|---|---|---|---|---|---|---|
| OS.WIN.001 | Active Directory / Windows Server | Receiving connection request from an IP address being blocked using personal firewall | Corporate Policy Violation | Unauthorized access attempt | This is implemented on the STRM console with the following Custom Rule:<br>Pure Windows configuration task, no STRM action required. | COD to confirm if personal firewall and logging is enabled on windows servers/AD through Group Policies.<br>http://technet.microsoft.com/en-us/library/cc753781%28v=ws.10%29.aspx | | |
| OS.WIN.002 | Active Directory / Windows Server | RDP Connection attempt from the SSL-VPN IP Pool | Corporate Policy Violation | Unauthorized access attempt | This is implemented on the STRM console with the following Custom Rule: | When Log Source Group is Active Directory Servers and when EVENT ID is 4624 and LOGON TYPE = 10 (Remote Desktop / Terminal Services) and when Source IP address (Source Network Address) is BB.<br>BB of Source IP should be as follows;<br>• SSL VPN Remote Access<br>• International Offices<br>• National IPVPN | | |
| OS.WIN.003 | Active Directory / Windows Server | Remote Access connection to a Windows/AD server and then user performs another RDP connection claiming to be another user | Corporate Policy Violation | Unauthorized use of resource | This is implemented on the STRM console with the following Custom Rule: | • User/Admin (USER A) performs RDP to a Window<br>• The same user (USER A) then performs another logon operation claiming to be another user (US<br>When Log Source Group is Active Direc Windows Server and Event ID 4624 Successfully Logged In and Logon Type which is Remote Desktop<br>Followed by,<br>Event ID 4648 - Indicates that a user w already logged on successfully created another logon session with different u credentials. | | |

QRadar/STRM Rules for MS Windows Server and Active Directory

| No | Rule Name | Logic |
|---|---|---|
| 1 | OS.WIN.002.Offense: RDP from SSL-VPN IP Pool | when the event(s) were detected by one or more of Domain Controllers<br>and<br>when any of EventID (custom) match ^4624$<br>and<br>when any of AD Logon Type (custom) match ^10$<br>and<br>when the source network is SSLVPN--pool_MDF_PMT |
| 2 | OS.WIN.003.Offense: RDP Server Jumping as Multiple Users | when OS.WIN.003.Rule: User Logon with Explicit Credentials match at least 1 times with the same AD_Logon_ID (custom) in 1 hour(s) after OS.WIN.003.Rule: User Logon match with the same AD_Logon_ID (custom) |
| 3 | OS.WIN.003.Rule: RDP User Logon | when the event(s) were detected by one or more of Domain Controllers<br>and<br>when any of EventID (custom) match ^4624$<br>and<br>when any of AD Logon Type (custom) match ^10$ |
| 4 | OS.WIN.003.Rule: User Logon with Explicit Credentials | when the event(s) were detected by one or more of Domain Controllers<br>and<br>when any of EventID (custom) match ^4648$ |
| 5 | OS.WIN.004.Offense: Multiple Logon Failures for Single User | when the event(s) were detected by one or more of Domain Controllers<br>and<br>when any of EventID (custom) match ^4625$<br>and<br>when at least 20 events are seen with the same Username, Source IP in 5 minutes<br>and<br>when any of Username match [^\\$]+$ |
| 6 | OS.WIN.005.Offense: Multiple Logon Failures for Multiple Users | when the event(s) were detected by one or more of Domain Controllers<br>and<br>when any of EventID (custom) match ^4625$ |

**Important Note**:
"**OS.WIN.010.Offense: Multiple Logon for Single User from Different Locations**" offense is disabled pending application/system accounts names clarifications to be excluded from the rule's logic.

# *NIX AUTHENTICATION … FOLLOW THE PROCESS



9
PowerBroker sends SYSLOG message of SUCCESFUL SU TO ROOT FROM USERNAME, SOURCE IP, HOST AIX SERVER and AUTHENTICATION SUCCCESSFUL

SIEM

10
AIX Server sends syslog binary files (ONE LINE) on the tasks executed as ROOT

IOLOGS USER B

IOLOGS USER A

8
PowerBroker RECEIVES successful authentication and authorization and create a ROOT session and create a session log "IOLOGS" and create a SUCCESSFUL LOGIN message

6
PowerBroker performs LDAP query for "User A" and validates group membership for ROOT access belongs to specified OU

5
PowerBroker Server identifies the following parameters – Source IP | Username | AIX Server and performs authentication and authorization

10

9

1
User A logs into AIX server over SSH

3
User A issues "pbrun su:root" to escalate the privilege to ROOT

IBM Tivoli LDAP

RSA TWO FACTOR ACE SERVER

LDAP

pbrun su: root

PowerBroker Agent

USER A

pbrun su: root

provide credentials

username/password

ACE

USER B

4
PowerBroker Server invokes the Agent with user authentication

POWERBROKER

7
PowerBroker performs two factor authentication for "User A"

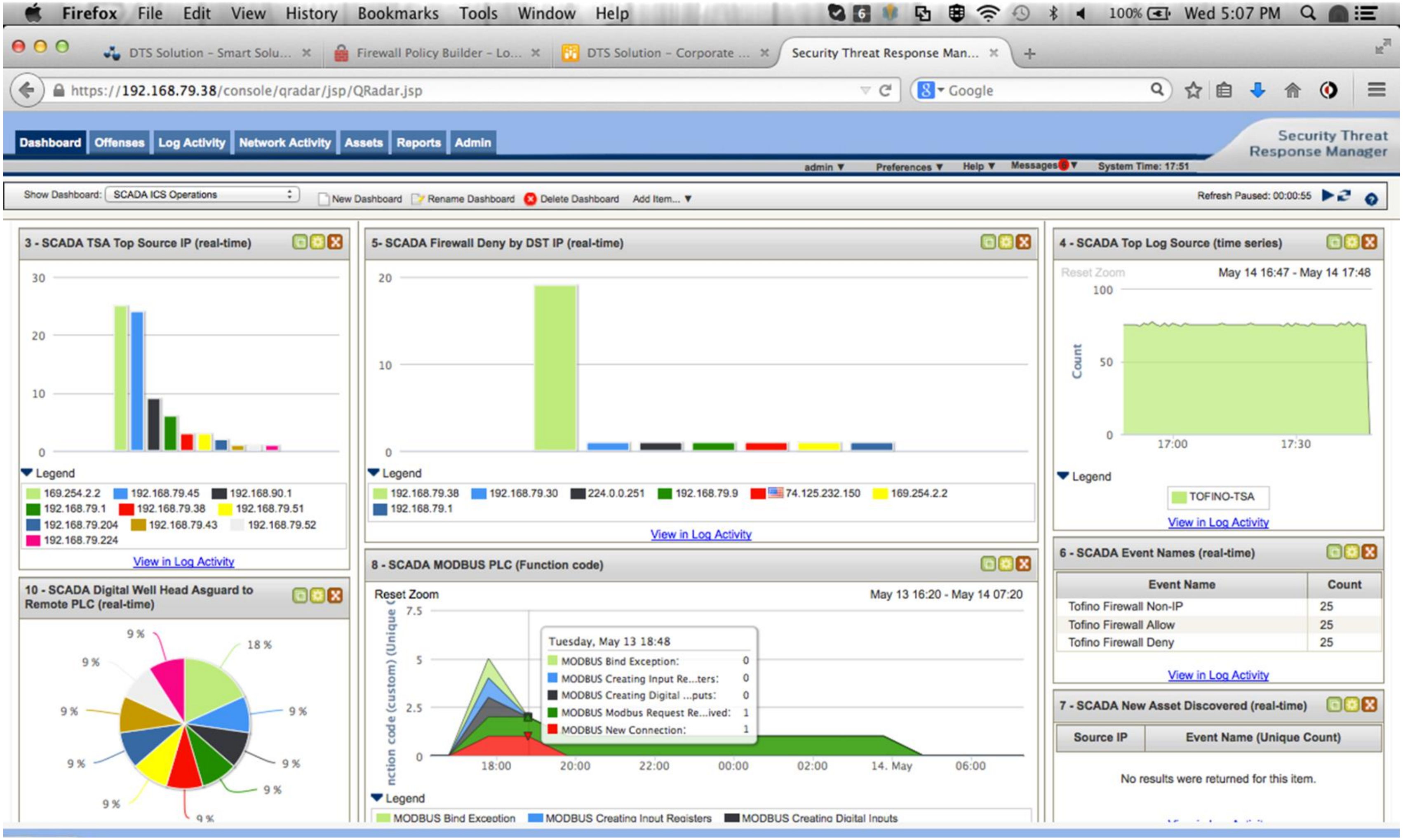
AIX SERVER

2
User A logs into AIX server over SSH and is authenticated over LDAP and RSA(2FA)

SSH Access Authentication – NON ROOT

SSH Access Authentication – NON ROOT

# Sample SCADA/ICS Dashboard

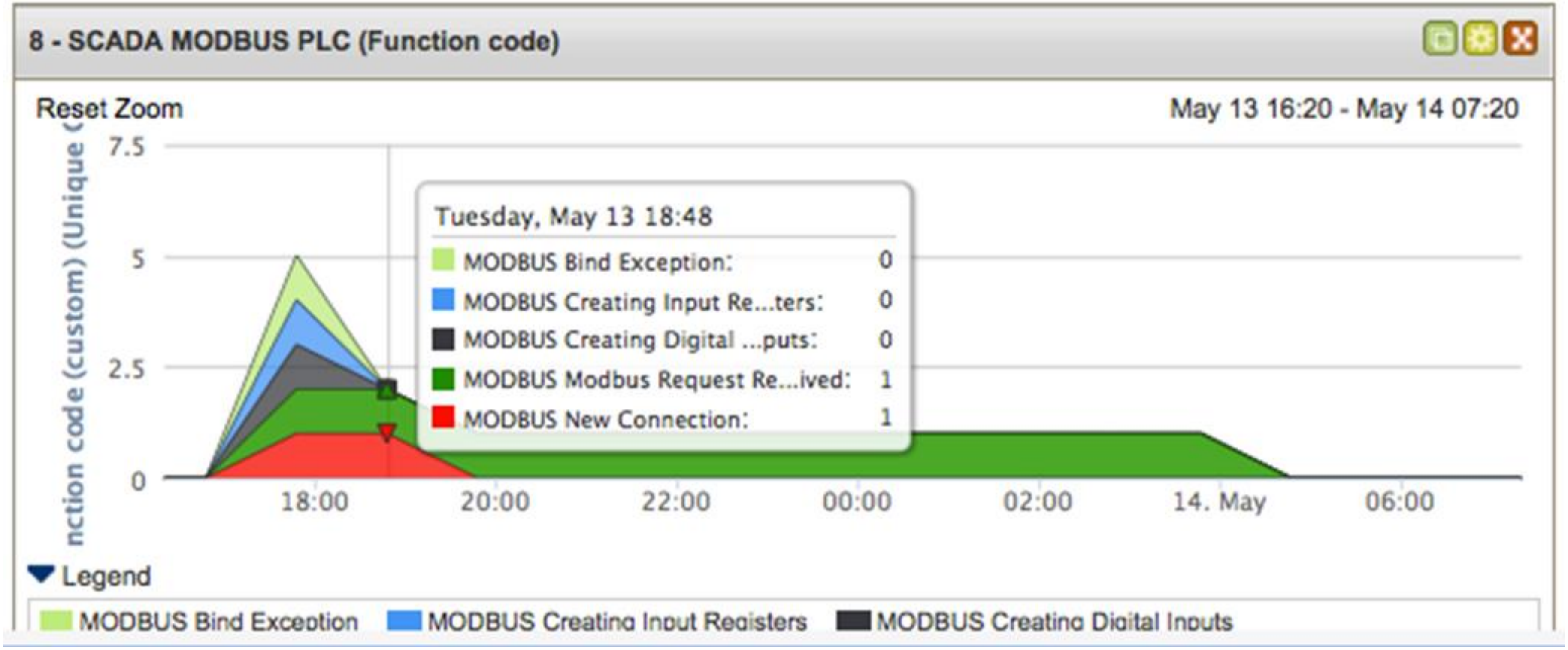

Firefox File Edit View History Bookmarks Tools Window Help
100% Wed 5:07 PM
DTS Solution - Smart Solu...
Firewall Policy Builder - Lo...
DTS Solution - Corporate ...
Security Threat Response Man...
https://192.168.79.38/console/qradar/jsp/QRadar.jsp
Google
Dashboard
Offenses
Log Activity
Network Activity
Assets
Reports
Admin
Security Threat Response Manager
admin ▼
Preferences ▼
Help ▼
Messages ▼
System Time: 17:51
Show Dashboard: SCADA ICS Operations
New Dashboard
Rename Dashboard
Delete Dashboard
Add Item... ▼
Refresh Paused: 00:00:55
3 - SCADA TSA Top Source IP (real-time)
30
20
10
0
Legend
192.168.79.38
192.168.79.51
169.254.2.2
192.168.79.45
192.168.90.1
192.168.79.1
192.168.79.204
192.168.79.43
192.168.79.52
192.168.79.224
View in Log Activity
5- SCADA Firewall Deny by DST IP (real-time)
20
10
0
Legend
192.168.79.38
192.168.79.30
224.0.0.251
192.168.79.9
74.125.232.150
169.254.2.2
192.168.79.1
View in Log Activity
4 - SCADA Top Log Source (time series)
Reset Zoom
May 14 16:47 - May 14 17:48
100
50
0
Count
17:00
17:30
Legend
TOFINO-TSA
View in Log Activity
10 - SCADA Digital Well Head Asguard to Remote PLC (real-time)
9 %
18 %
9 %
9 %
9 %
9 %
9 %
9 %
9 %
9 %
8 - SCADA MODBUS PLC (Function code)
Reset Zoom
May 13 16:20 - May 14 07:20
7.5
5
2.5
0
nction code (custom) (Unique (
18:00
20:00
22:00
00:00
02:00
14. May
06:00
Tuesday, May 13 18:48
MODBUS Bind Exception: 0
MODBUS Creating Input Re...ters: 0
MODBUS Creating Digital ...puts: 0
MODBUS Modbus Request Re...ived: 1
MODBUS New Connection: 1
Legend
MODBUS Bind Exception
MODBUS Creating Input Registers
MODBUS Creating Digital Inputs
6 - SCADA Event Names (real-time)
View in Log Activity
7 - SCADA New Asset Discovered (real-time)

| Event Name | Count |
|---|---|
| Tofino Firewall Non-IP | 25 |
| Tofino Firewall Allow | 25 |
| Tofino Firewall Deny | 25 |

| Source IP | Event Name (Unique Count) |
|---|---|

No results were returned for this item.

# Sample SCADA/ICS Dashboard



8 - SCADA MODBUS PLC (Function code)

Reset Zoom

May 13 16:20 - May 14 07:20

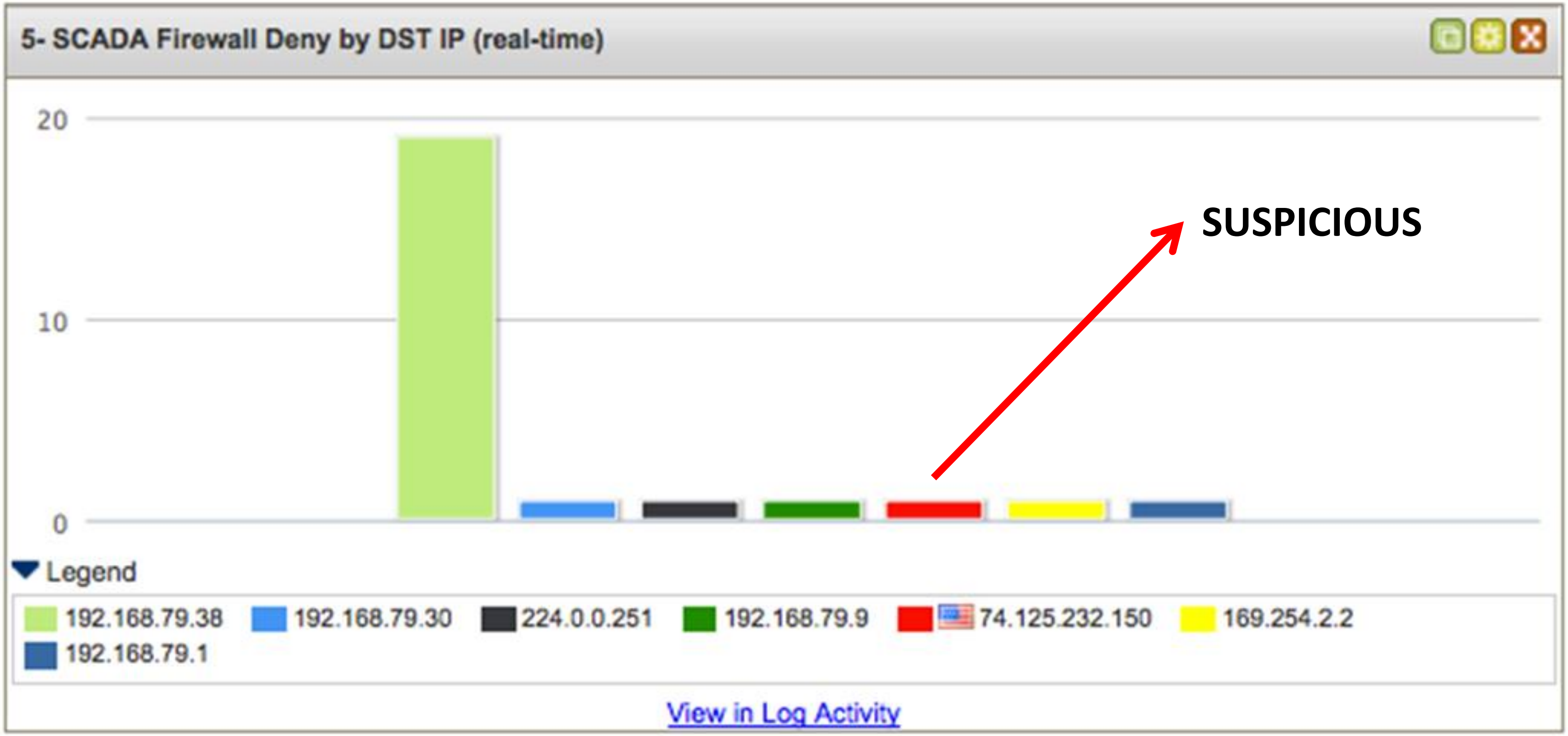
Tuesday, May 13 18:48

| | |
|---|---|
| 🟩 MODBUS Bind Exception: | 0 |
| 🟦 MODBUS Creating Input Re...ters: | 0 |
| ⬛ MODBUS Creating Digital ...puts: | 0 |
| 🟩 MODBUS Modbus Request Re...ived: | 1 |
| 🟥 MODBUS New Connection: | 1 |

▼ Legend

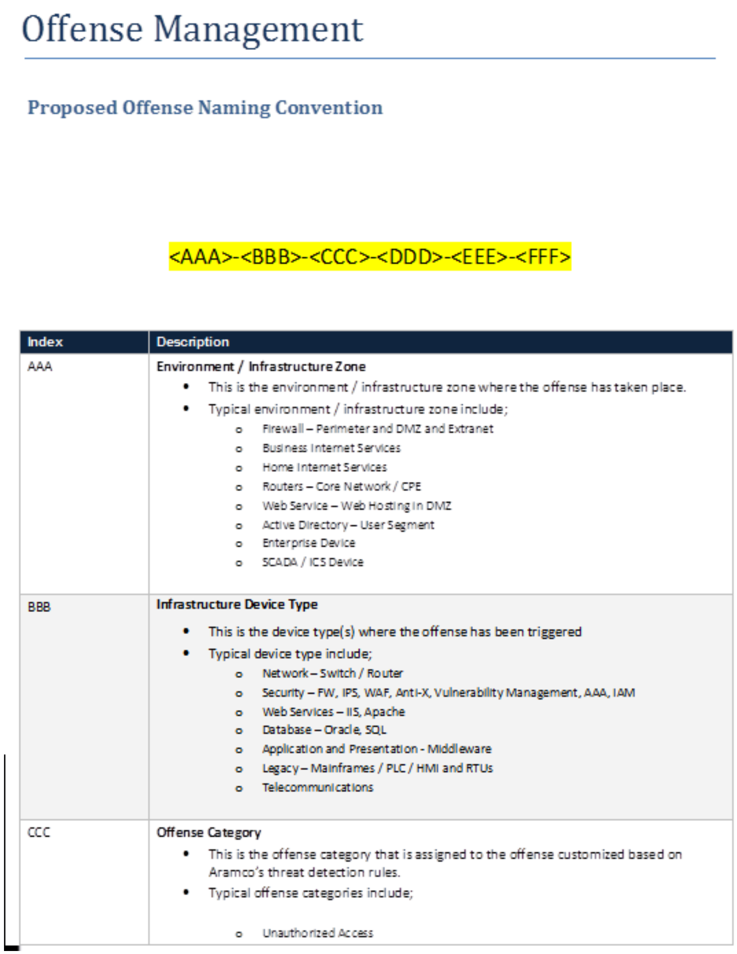
🟩 MODBUS Bind Exception 🟦 MODBUS Creating Input Registers ⬛ MODBUS Creating Digital Inputs

# Sample SCADA/ICS Dashboard



**SUSPICIOUS**

# Offense Management Naming Convention



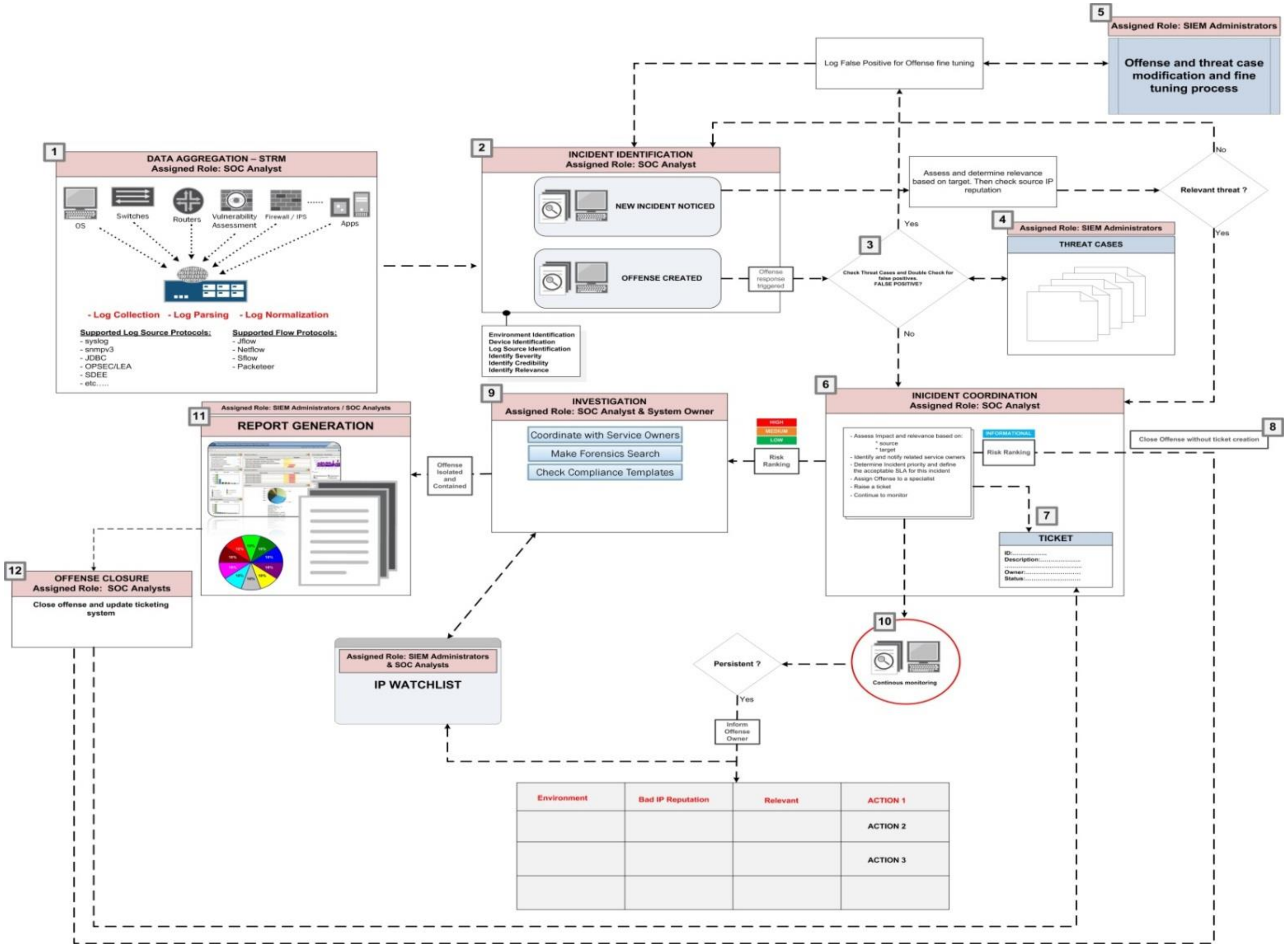
## Offense Management

### Proposed Offense Naming Convention

<AAA>-<BBB>-<CCC>-<DDD>-<EEE>-<FFF>

| Index | Description |
|---|---|
| AAA | **Environment / Infrastructure Zone**<br>• This is the environment / infrastructure zone where the offense has taken place.<br>• Typical environment / infrastructure zone include;<br>o Firewall – Perimeter and DMZ and Extranet<br>o Business Internet Services<br>o Home Internet Services<br>o Routers – Core Network / CPE<br>o Web Service – Web Hosting in DMZ<br>o Active Directory – User Segment<br>o Enterprise Device<br>o SCADA / ICS Device |
| BBB | **Infrastructure Device Type**<br>• This is the device type(s) where the offense has been triggered<br>• Typical device type include;<br>o Network – Switch / Router<br>o Security – FW, IPS, WAF, Anti-X, Vulnerability Management, AAA, IAM<br>o Web Services – IIS, Apache<br>o Database – Oracle, SQL<br>o Application and Presentation - Middleware<br>o Legacy – Mainframes / PLC / HMI and RTUs<br>o Telecommunications |
| CCC | **Offense Category**<br>• This is the offense category that is assigned to the offense customized based on Aramco's threat detection rules.<br>• Typical offense categories include;<br>o Unauthorized Access |

# Offense Management Workflow



1 DATA AGGREGATION – STRM
Assigned Role: SOC Analyst

- Log Collection - Log Parsing - Log Normalization

**Supported Log Source Protocols:**
- syslog
- snmpv3
- JDBC
- OPSEC/LEA
- SDEE
- etc.....

**Supported Flow Protocols:**
- Jflow
- Netflow
- Sflow
- Packeteer

2 INCIDENT IDENTIFICATION
Assigned Role: SOC Analyst

NEW INCIDENT NOTICED

OFFENSE CREATED

Environment Identification
Device Identification
Log Source Identification
Identify Severity
Identify Credibility
Identify Relevance

Offense response triggered

3 Check Threat Cases and Double Check for false positives.
FALSE POSITIVE?

Log False Positive for Offense fine tuning

Assess and determine relevance based on target. Then check source IP reputation

Relevant threat ?

4 Assigned Role: SIEM Administrators
THREAT CASES

5 Assigned Role: SIEM Administrators
Offense and threat case modification and fine tuning process

6 INICIDENT COORDINATION
Assigned Role: SOC Analyst

- Assess Impact and relevance based on:
  * source
  * target
- Identify and notify related service owners
- Determine incident priority and define the acceptable SLA for this incident
- Assign Offense to a specialist
- Raise a ticket
- Continue to monitor

Risk Ranking

7 TICKET
ID:.................
Description:......................
.........................................
Owner:.............................
Status:.............................

8 Close Offense without ticket creation

9 INVESTIGATION
Assigned Role: SOC Analyst & System Owner

Coordinate with Service Owners

Make Forensics Search

Check Compliance Templates

Risk Ranking

Offense Isolated and Contained

11 Assigned Role: SIEM Administrators / SOC Analysts
REPORT GENERATION

12 OFFENSE CLOSURE
Assigned Role: SOC Analysts
Close offense and update ticketing system

Assigned Role: SIEM Administrators & SOC Analysts
IP WATCHLIST

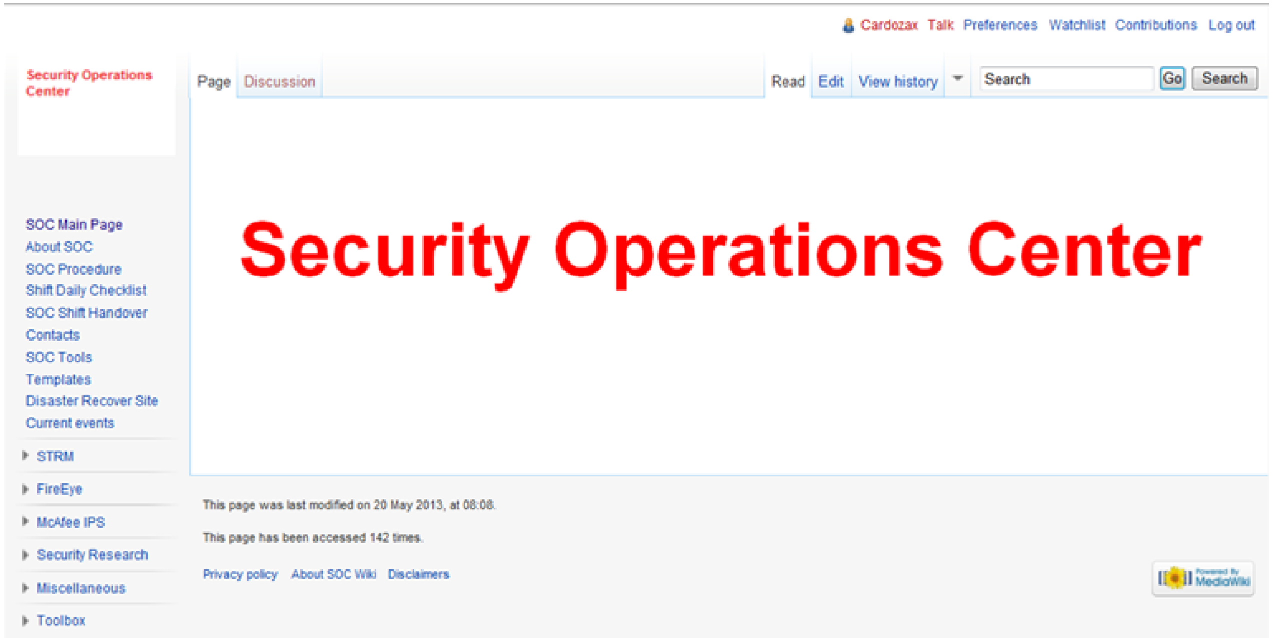
10 Continous monitoring

Persistent ?

Inform Offense Owner

| Environment | Bad IP Reputation | Relevant | ACTION 1 |
|---|---|---|---|
| | | | ACTION 2 |
| | | | ACTION 3 |
| | | | |

# SOC Wiki



Security Operations Center

This page was last modified on 20 May 2013, at 08:08.

This page has been accessed 142 times.

SOC-Wiki

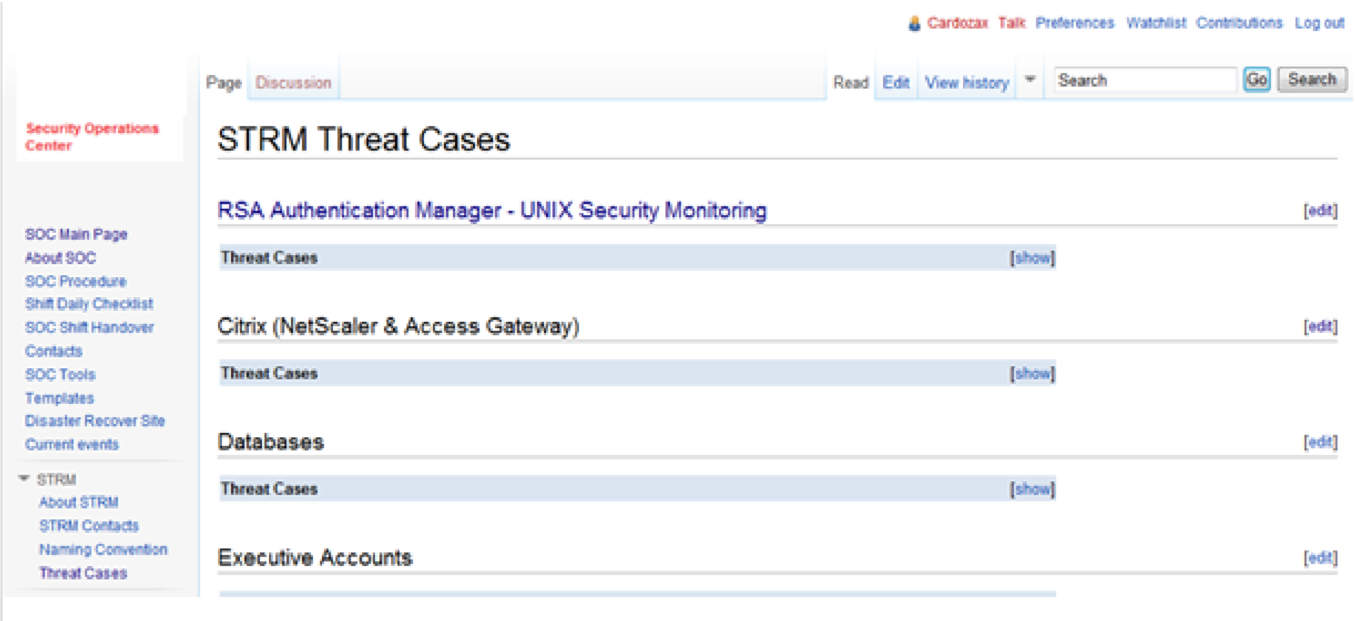
https://SOC-wiki.intranet.com

# SOC-Wiki - Goals

- Centralized Knowledge Repository for SOC
- Collaborate and Share Information with other Team Members
- Easy of use and Searchable
- Integrations with other Toolsets

# SOC Wiki – SIEM Integration

- Current Issues with SIEM Processes, Documentations, Offence Handling, Knowledge Sharing
- SIEM Integrations into SOC-Wiki
- SIEM Threat Cases



## STRM Threat Cases

### RSA Authentication Manager - UNIX Security Monitoring [edit]

Threat Cases [show]

### Citrix (NetScaler & Access Gateway) [edit]

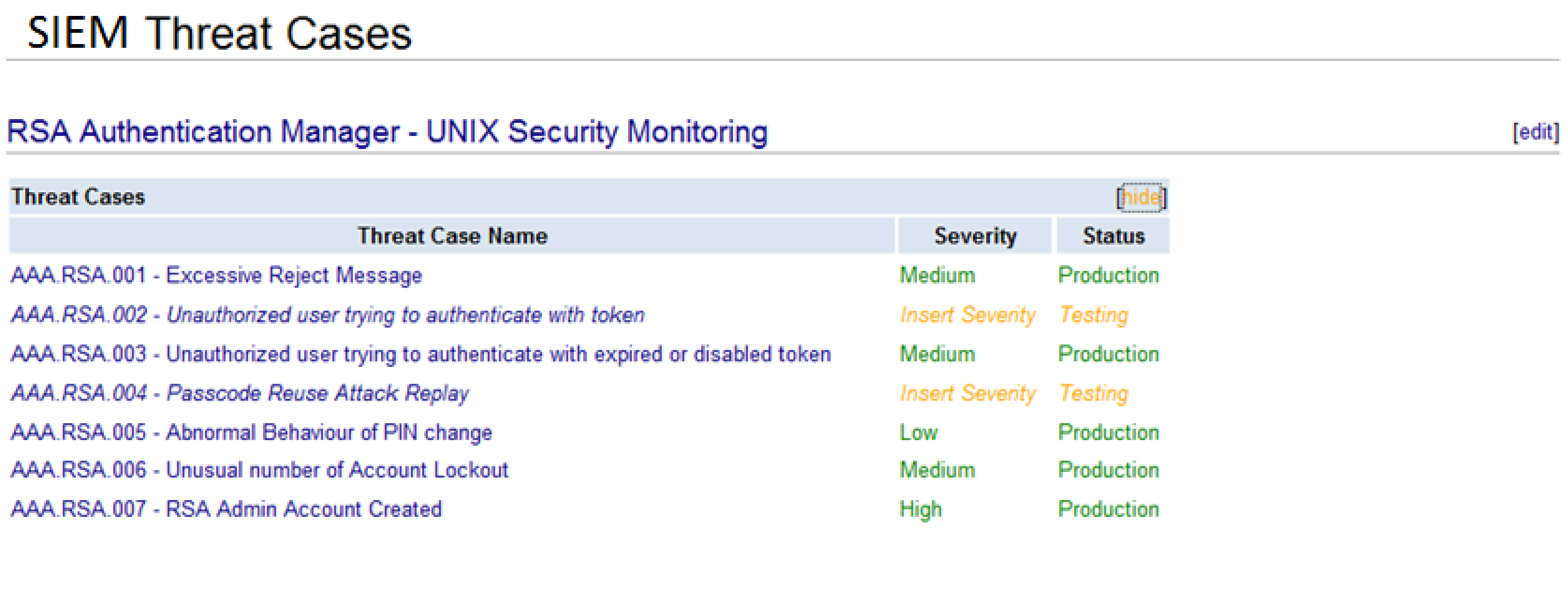
Threat Cases [show]

### Databases [edit]

Threat Cases [show]

### Executive Accounts [edit]

# SOC Wiki – SIEM Threat Cases



## SIEM Threat Cases

### RSA Authentication Manager - UNIX Security Monitoring

[edit]

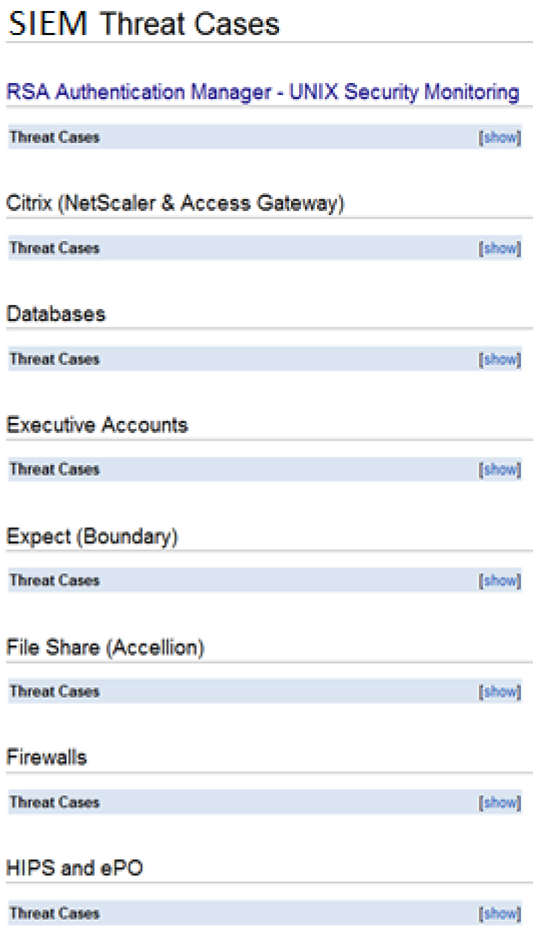
Threat Cases [hide]

| Threat Case Name | Severity | Status |
|---|---|---|
| AAA.RSA.001 - Excessive Reject Message | Medium | Production |
| *AAA.RSA.002 - Unauthorized user trying to authenticate with token* | *Insert Severity* | *Testing* |
| AAA.RSA.003 - Unauthorized user trying to authenticate with expired or disabled token | Medium | Production |
| *AAA.RSA.004 - Passcode Reuse Attack Replay* | *Insert Severity* | *Testing* |
| AAA.RSA.005 - Abnormal Behaviour of PIN change | Low | Production |
| AAA.RSA.006 - Unusual number of Account Lockout | Medium | Production |
| AAA.RSA.007 - RSA Admin Account Created | High | Production |

- Listed above is how Threat Cases are displayed in SOC-Wiki
- Threat Case Name, Severity, Status
- Information - Centralized, Detailed and Searchable
- Information updated by SIEM and SOC Teams

# SOC Wiki – SIEM Threat Cases

- Example:



## SIEM Threat Cases

RSA Authentication Manager - UNIX Security Monitoring

Threat Cases [show]

Citrix (NetScaler & Access Gateway)

Threat Cases [show]

Databases

Threat Cases [show]

Executive Accounts

Threat Cases [show]

Expect (Boundary)

Threat Cases [show]

File Share (Accellion)

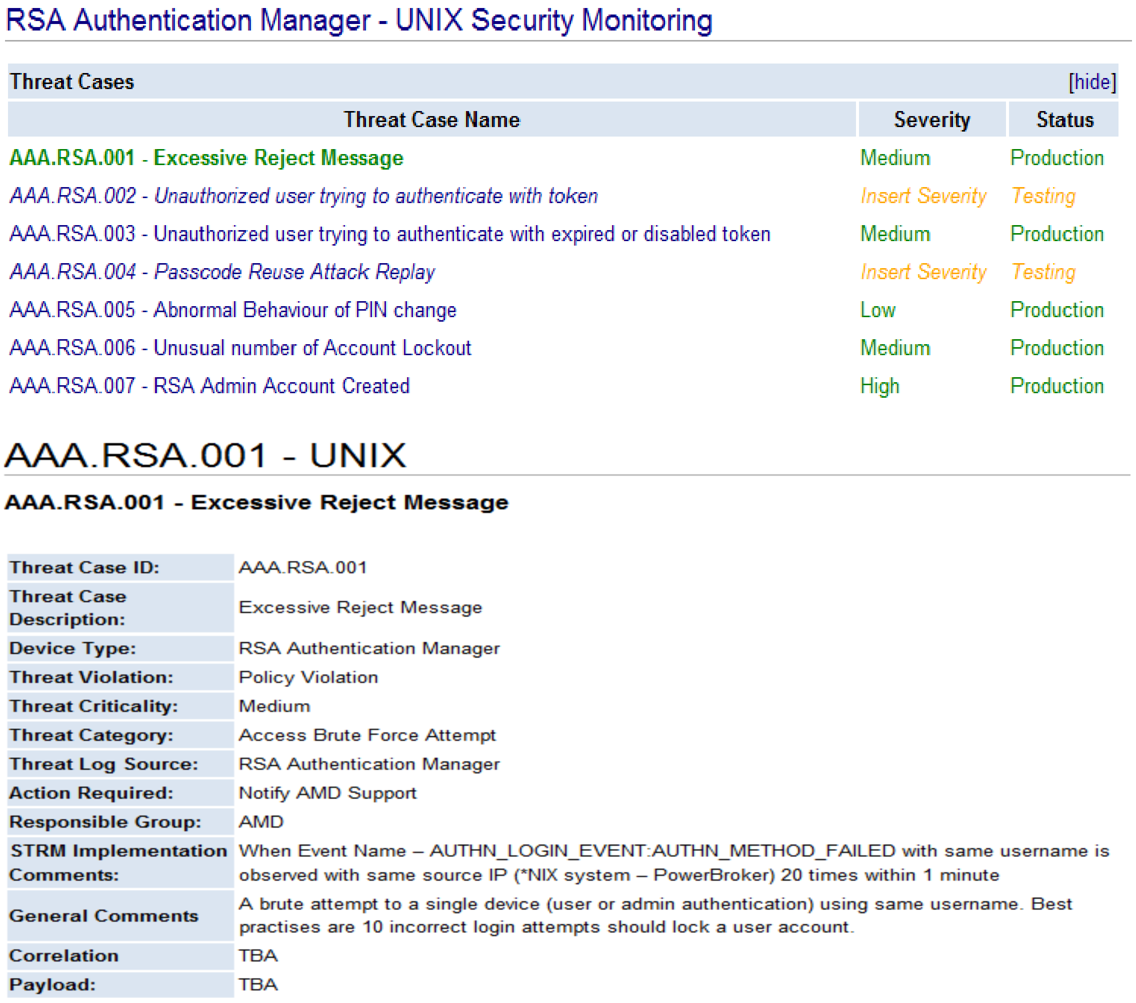
Threat Cases [show]

Firewalls

Threat Cases [show]

HIPS and ePO

Threat Cases [show]



## RSA Authentication Manager - UNIX Security Monitoring

Threat Cases [hide]

| Threat Case Name | Severity | Status |
|---|---|---|
| AAA.RSA.001 - Excessive Reject Message | Medium | Production |
| *AAA.RSA.002 - Unauthorized user trying to authenticate with token* | *Insert Severity* | *Testing* |
| AAA.RSA.003 - Unauthorized user trying to authenticate with expired or disabled token | Medium | Production |
| *AAA.RSA.004 - Passcode Reuse Attack Replay* | *Insert Severity* | *Testing* |
| AAA.RSA.005 - Abnormal Behaviour of PIN change | Low | Production |
| AAA.RSA.006 - Unusual number of Account Lockout | Medium | Production |
| AAA.RSA.007 - RSA Admin Account Created | High | Production |

## AAA.RSA.001 - UNIX

**AAA.RSA.001 - Excessive Reject Message**

| | |
|---|---|
| **Threat Case ID:** | AAA.RSA.001 |
| **Threat Case Description:** | Excessive Reject Message |
| **Device Type:** | RSA Authentication Manager |
| **Threat Violation:** | Policy Violation |
| **Threat Criticality:** | Medium |
| **Threat Category:** | Access Brute Force Attempt |
| **Threat Log Source:** | RSA Authentication Manager |
| **Action Required:** | Notify AMD Support |
| **Responsible Group:** | AMD |
| **STRM Implementation Comments:** | When Event Name – AUTHN_LOGIN_EVENT:AUTHN_METHOD_FAILED with same username is observed with same source IP (*NIX system – PowerBroker) 20 times within 1 minute |
| **General Comments** | A brute attempt to a single device (user or admin authentication) using same username. Best practises are 10 incorrect login attempts should lock a user account. |
| **Correlation** | TBA |
| **Payload:** | TBA |

DTS SOLUTION
smart solution for the smart business

# Security Assurance Level

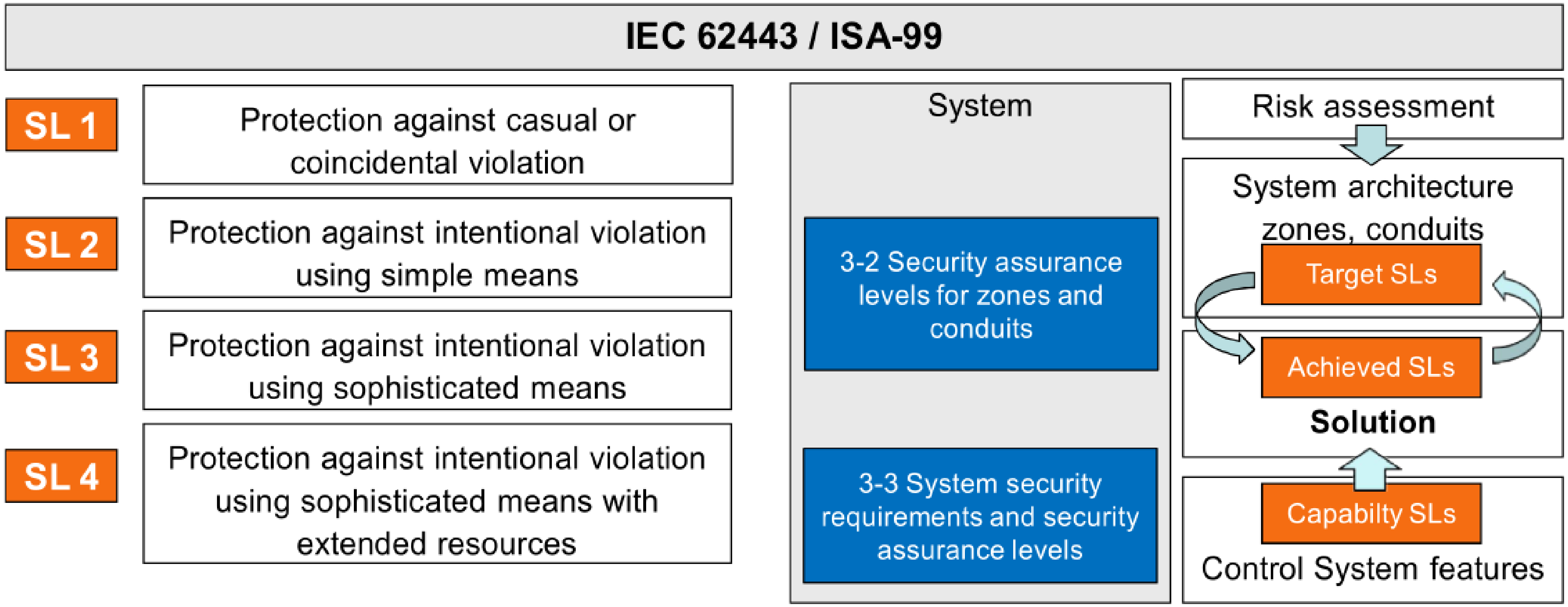
- **Security Assurance Levels (SALs) in Critical Infrastructure**
  - **Functional Requirements**
  - **Security Levels**

  - Based on 7 x Functional Requirements

    - **a) Access control (AC)**
    - **b) Use control (UC)**
    - **c) Data integrity (DI)**
    - **d) Data confidentiality (DC)**
    - **e) Restrict data flow (RDF)**
    - **f) Timely response to an event (TRE)**
    - **g) Resource availability (RA)**

# Security Assurance Level

- **Security Assurance Levels (SALs) in Critical Infrastructure**
  - **Functional Requirements**
  - **Security Levels**
    - Based on 4 x Security Levels



**IEC 62443 / ISA-99**

| | |
|---|---|
| SL 1 | Protection against casual or coincidental violation |
| SL 2 | Protection against intentional violation using simple means |
| SL 3 | Protection against intentional violation using sophisticated means |
| SL 4 | Protection against intentional violation using sophisticated means with extended resources |

System

3-2 Security assurance levels for zones and conduits

3-3 System security requirements and security assurance levels

Risk assessment

System architecture zones, conduits

Target SLs

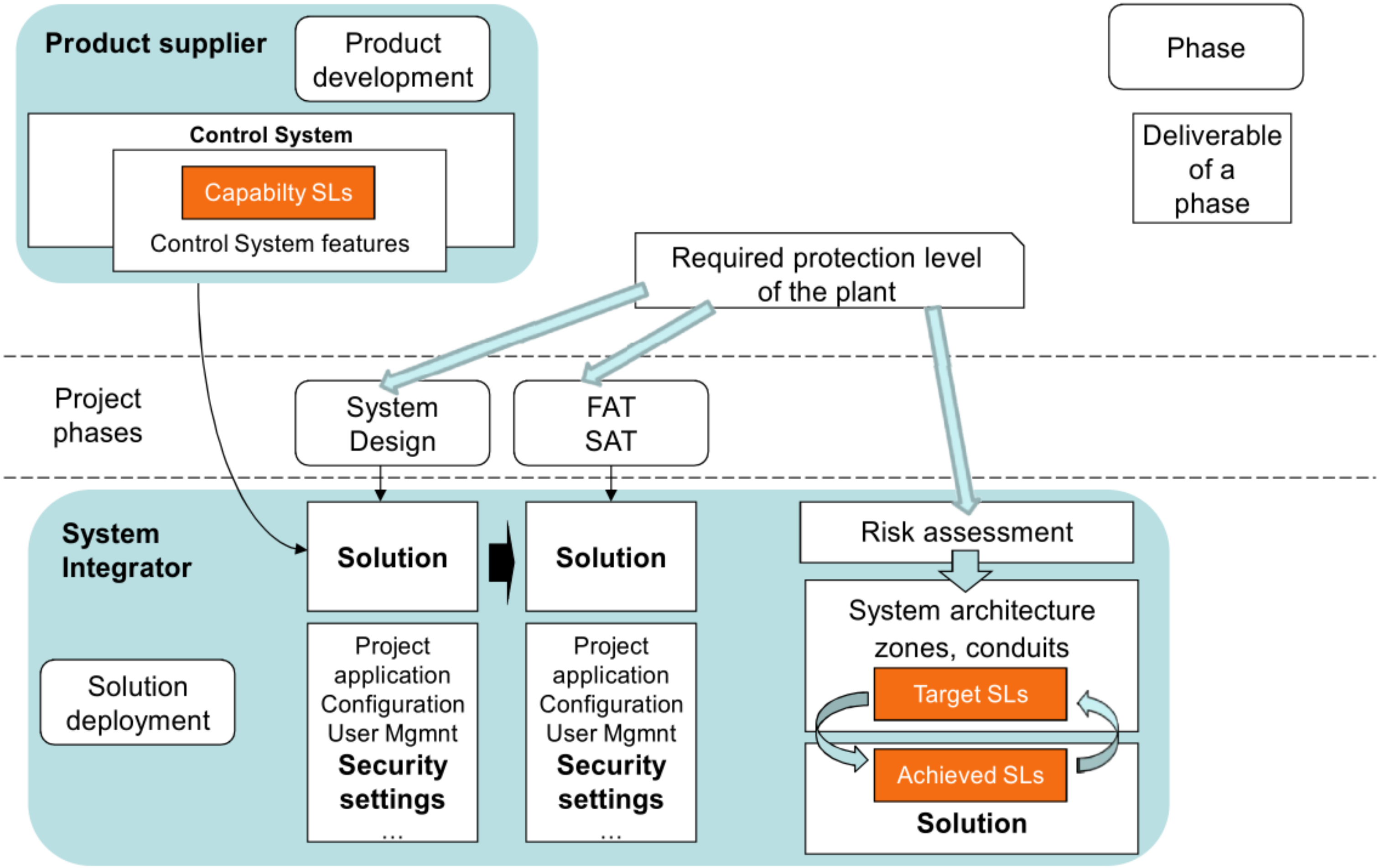
Achieved SLs

**Solution**

Capabilty SLs

Control System features

# Security Assurance Level



Product supplier

Product development

Control System

Capabilty SLs

Control System features

Phase

Deliverable of a phase

Required protection level of the plant

Project phases

System Design

FAT SAT

System Integrator

Solution deployment

Solution

Project application Configuration User Mgmnt **Security settings** …

Solution

Project application Configuration User Mgmnt **Security settings** …

Risk assessment

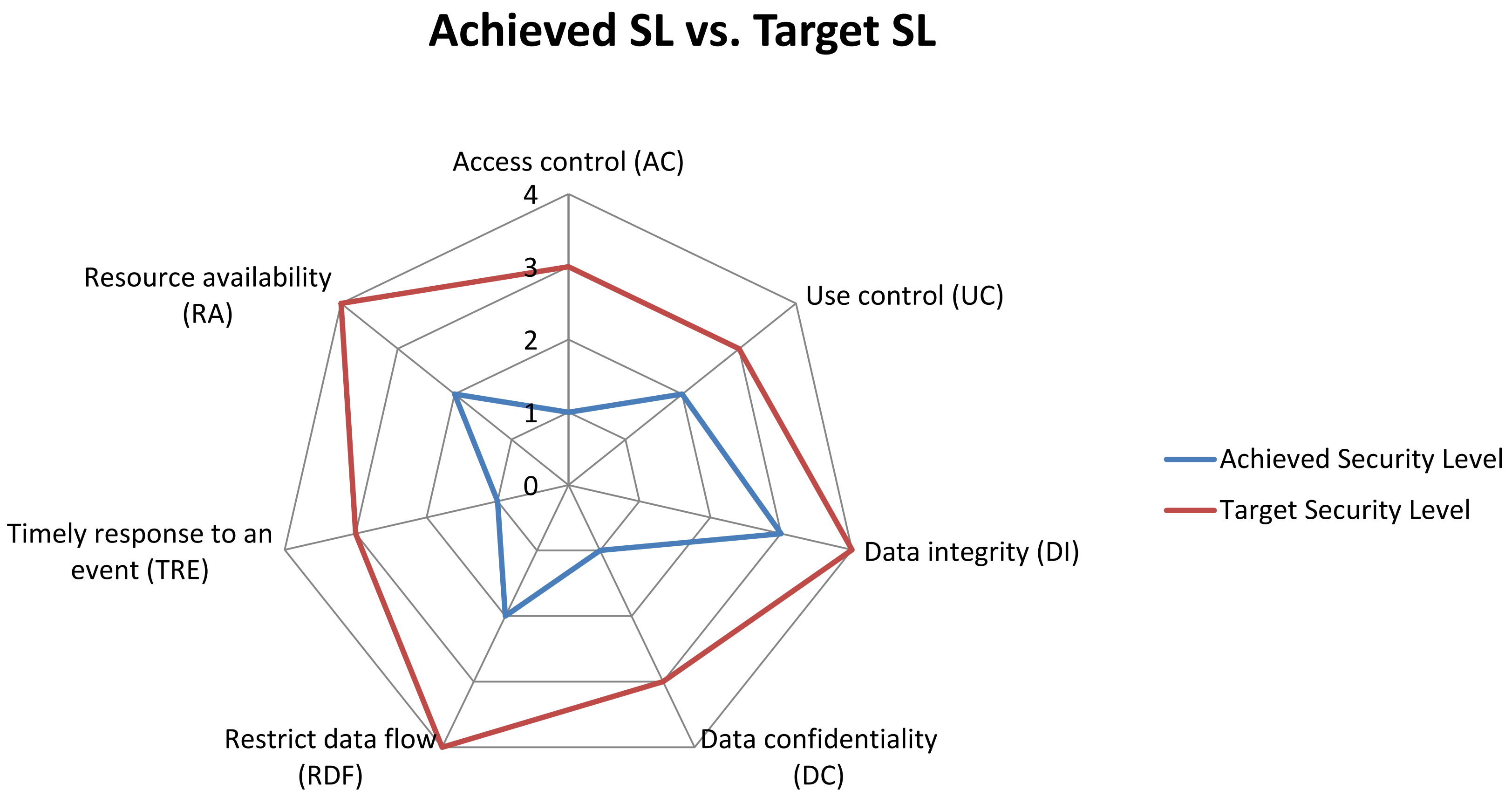
System architecture zones, conduits

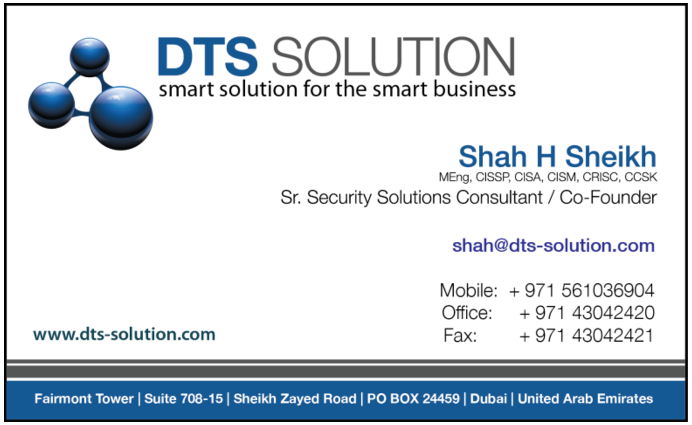
Target SLs

Achieved SLs

**Solution**

# Security Assurance Level





DTS SOLUTION
smart solution for the smart business

Shah H Sheikh
MEng, CISSP, CISA, CISM, CRISC, CCSK
Sr. Security Solutions Consultant / Co-Founder

shah@dts-solution.com

| | |
|---|---|
| Mobile: | + 971 561036904 |
| Office: | + 971 43042420 |
| Fax: | + 971 43042421 |

www.dts-solution.com

Fairmont Tower | Suite 708-15 | Sheikh Zayed Road | PO BOX 24459 | Dubai | United Arab Emirates

*Shah H Sheikh – Sr. Security Solutions Consultant*
MEng CISSP CISA CISM CRISC CCSK
shah@dts-solution.com