Building a SCADA Cyber Security Operations Center - PCN

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

www.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
ICS Security - Defense-in-Depth
Pathways into the Plant Floor

Office LAN

Plant Network

Control LAN

Internet

Infected Remote Support

Unauthorized Connections

SIEM

NMS

Backup / Recovery

3rd Party Issues

External Network

Mis-Configured Firewalls

Infected Laptops

Modems

USB Drives

3rd Party Issues

Backup / Recovery

External Network

SIEM

NMS

Unauthorized Connections

Infected Remote Support

Internet

Office LAN

Plant Network

Control LAN

Infected Laptops
## Automation Systems Security Really Unique?

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

In-house SOC

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 ...

• 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 subordinates
• 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

DTS SOLUTION
smart solution for the smart business
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 😊
### 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**

### Details:

<table>
<thead>
<tr>
<th>OSS/SIEM 2.0</th>
<th>Proactive Monitoring</th>
<th>Alert &amp; Notification</th>
<th>Event Correlation</th>
</tr>
</thead>
<tbody>
<tr>
<td>Automated Monitoring – SNMP</td>
<td>Automated Alert and Notification – SNMP Trap / IF-MAP event</td>
<td>Contextual correlation of events</td>
<td></td>
</tr>
<tr>
<td>Categorization of Monitored Objects</td>
<td>Alerts categorized based on Risk Level</td>
<td>Situational awareness</td>
<td></td>
</tr>
<tr>
<td>Automated Monitored Object Reporting</td>
<td>Notifications to Business Process Owner</td>
<td>Mapped to Business Process</td>
<td></td>
</tr>
<tr>
<td>Integrated to Business Process</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Automated assignment of Risk Level</td>
<td></td>
<td></td>
<td></td>
</tr>
</tbody>
</table>
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
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
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**
# 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

---

**Perimeter and Boundary Points**
- Internet
- IPS
- WAF
- FW

**DMZ / Published Services**
- WWW
- SSL VPN

**Applications**
- Middleware
- SMTP

**Internal Resources**
- Servers
- MAINFRAME
- DB
- Active Directory

---

**DTS SOLUTION**
smart solution for the smart business
SOC – Core Components

Integration of Core SOC Components

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

- **Vulnerability Assessment**
- **NMS Monitoring**

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

- **SIEM 2.0**
- **Compliance and Management**

- **SEVERITY VULNERABILITY**
  - Common Vulnerability Exploits (CVE)
  - Risk Ranking
  - Configuration Audit
  - Security Metric Dashboard

- **Syslog, Log Files, NetFlow**
- **Internet**
- **Perimeter and Boundary Points**
  - Network Nodes

- **DMZ/Published Services**
  - IPS
  - WAF
  - FW
  - SSL VPN

- **Middleware/SMTP Applications**
  - WWW
  - SSL VPN
  - DB
  - Active Directory
  - MAINFRAME

- **Configuration Audit, Configuration Baseline, Risk Management, Policy Compliance**

---

*DTS Solution*  
smart solution for the smart business
SOC Technologies ...

*So now the technologies ...*

**SIEM Solutions**
- Event Collector – Syslog, Log Files, Application Log Export
- 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
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
SOC – Processes …. Look familiar...

**Creating the SOC Processes**

... now that we have discussed technology, let's discuss processes ...

<table>
<thead>
<tr>
<th>DATA SECURITY AND MONITORING</th>
</tr>
</thead>
<tbody>
<tr>
<td>• Data Asset Classification</td>
</tr>
<tr>
<td>• Data Collection</td>
</tr>
<tr>
<td>• Data Normalization</td>
</tr>
<tr>
<td>• Data at Rest and In Motion</td>
</tr>
<tr>
<td>• Data Protection</td>
</tr>
<tr>
<td>• Data Distribution</td>
</tr>
</tbody>
</table>
Creating the SOC Processes

... now that we have discussed technology, let's discuss processes ...

<table>
<thead>
<tr>
<th>EVENT MANAGEMENT</th>
</tr>
</thead>
<tbody>
<tr>
<td>• Event Correlation</td>
</tr>
<tr>
<td>• Identification</td>
</tr>
<tr>
<td>• Triage</td>
</tr>
<tr>
<td>• Roles</td>
</tr>
<tr>
<td>• Containment</td>
</tr>
<tr>
<td>• Notification</td>
</tr>
<tr>
<td>• Ticketing</td>
</tr>
<tr>
<td>• Recovery</td>
</tr>
<tr>
<td>• Forensics and Situational Awareness</td>
</tr>
</tbody>
</table>
Creating the SOC Processes

... now that we have discussed technology, let's discuss processes ...

<table>
<thead>
<tr>
<th>INCIDENT RESPONSE PRACTICE</th>
</tr>
</thead>
<tbody>
<tr>
<td>• Security Incident Reporting Structure</td>
</tr>
<tr>
<td>• Security Incident Monitoring</td>
</tr>
<tr>
<td>• Security Incident Escalation Procedure</td>
</tr>
<tr>
<td>• Forensics and Root Cause Analysis</td>
</tr>
<tr>
<td>• Return to Normal Operations</td>
</tr>
<tr>
<td>• Post-Incident Planning and Monitoring</td>
</tr>
<tr>
<td>• Communication Guidelines</td>
</tr>
<tr>
<td>• SIRT Integration</td>
</tr>
</tbody>
</table>
Creating the SOC Processes

... now that we have discussed technology, let's discuss processes ...

SOC OPERATING GUIDELINES

• SOC Workflow
• Personnel Shift Description
• Shift Reporting
• Shift Change
• Information Acquisition
• SOC Monitoring Suite
• SOC Reporting Structure
• Organizational Chart
Creating the SOC Processes
... now that we have discussed technology, lets discuss processes ...

<table>
<thead>
<tr>
<th>ESCALATION MANAGEMENT</th>
</tr>
</thead>
<tbody>
<tr>
<td>• Escalation Procedure</td>
</tr>
<tr>
<td>• Pre-Escalation Tasks</td>
</tr>
<tr>
<td>• IT Security</td>
</tr>
<tr>
<td>• Network Operation Center</td>
</tr>
<tr>
<td>• Security Engineering</td>
</tr>
<tr>
<td>• SIRT Integration</td>
</tr>
<tr>
<td>• Law Enforcement</td>
</tr>
<tr>
<td>• 3rd Party Service Providers and Vendors</td>
</tr>
</tbody>
</table>
Creating the SOC Processes

... now that we have discussed technology, lets discuss processes ...

<table>
<thead>
<tr>
<th>DATA RECOVERY PROCEDURES</th>
</tr>
</thead>
<tbody>
<tr>
<td>• Disaster Recovery and BCP Procedure</td>
</tr>
<tr>
<td>• Recovery Time Objective</td>
</tr>
<tr>
<td>• Recovery Point Objective</td>
</tr>
<tr>
<td>• Resiliency and High Availability</td>
</tr>
<tr>
<td>• Facilities Outage Procedure</td>
</tr>
</tbody>
</table>
### 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, let's discuss processes ...

<table>
<thead>
<tr>
<th>TOOLS OPERATING MANUAL FOR SOC PERSONNEL</th>
</tr>
</thead>
<tbody>
<tr>
<td>• Operating Procedure for SIEM Solutions – Event Management and Flow Collector/Processor</td>
</tr>
<tr>
<td>• Firewall Security Logs</td>
</tr>
<tr>
<td>• IDS/IPS Security Logs</td>
</tr>
<tr>
<td>• DMZ Jump Server / SSL VPN logs</td>
</tr>
<tr>
<td>• Endpoint Security logs (AV, DLP, HIPS)</td>
</tr>
<tr>
<td>• User Activity / Login Logs</td>
</tr>
<tr>
<td>• Operating Procedure for Policy and Configuration Compliance</td>
</tr>
<tr>
<td>• Operating Procedure for Network Monitoring Systems</td>
</tr>
<tr>
<td>• Operating Procedure for Vulnerability Assessment</td>
</tr>
</tbody>
</table>

DTS SOLUTION
smart solution for the smart business
Creating the SOC Processes

... now that we have discussed technology, let's 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
Creating the SOC Processes

... now that we have discussed technology, let's discuss processes ...
….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?
SCADA Network... Isolation and Zoning
SCADA Network... Secured Zones
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)

   (Operating System Security, Application Security)

5. Communications to Field Devices
   (Profinet, 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:
- 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

DTS SOLUTION
smart solution for the smart business
Knowledge on how service flow across your infrastructure.

BUILD A SECURITY SERVICES CATALOG
• Understanding the service flows will allow you to VISUALIZE...

..... HEAT MAP .....
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
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

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:

<table>
<thead>
<tr>
<th>Compliance Category</th>
<th>Compliance Status and Risk</th>
</tr>
</thead>
<tbody>
<tr>
<td>Account Management</td>
<td></td>
</tr>
<tr>
<td>Configuration Management and Backup</td>
<td></td>
</tr>
<tr>
<td>Logging and Monitoring</td>
<td></td>
</tr>
<tr>
<td>Secure Management Access</td>
<td></td>
</tr>
<tr>
<td>Device Configuration</td>
<td></td>
</tr>
</tbody>
</table>

Compliant

Non-Compliant / Medium Risk

Non-Compliant / High Risk
Sample: Firewall GAP Analysis Report

GAP Findings Summary

The tables below summarize the GAP analysis findings:

**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**

1.2 Centralized User Authentication

All non-root accounts should be centrally managed and delegated using an Authentication Server like Radius or Tacacs. Use of Radius and Tacacs Server. User system accounts should only be created on the centralized authentication server and not locally on the device.

---

DTS SOLUTION
smart solution for the smart business
## Appendix B – Juniper SRX Configuration Commands

<p>| | |</p>
<table>
<thead>
<tr>
<th></th>
<th></th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>1. User Account Management</strong></td>
<td></td>
</tr>
<tr>
<td>1.1 Hostname Configuration</td>
<td>Set system hostname (Hostname)</td>
</tr>
<tr>
<td>1.2 Local User Account</td>
<td>Set system login user (user-name) class (user class) authentication plain-text-password (Enter) (Enter password for specific user account)</td>
</tr>
</tbody>
</table>
| 1.3 Radius Server Configuration | Set system radius-server (server IP address) port 1812 secret (radius secret key)  
set system radius-server (server IP address) source-address (src-interface-IP)  
set system radius-server (server IP address) retry (1 .. 10)  
set system authentication-order radius  
inset system authentication-order radius before password  
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  
set system syslog host (syslog server IP) any any  
set system syslog host (syslog server IP) change-log none  
set host (syslog server IP) interactive-commands alert  
set host (syslog server IP) source-address (syslog src-interface)  
set host (syslog server IP) structured-data  
set system syslog file default-log-messages any any  
set authorization info  
set system syslog file interactive-commands interactive-commands any  
set system syslog file security authorization info  
set system syslog file security conflict-log info  
set system syslog file security interactive-commands info  
set system syslog file traffic-log any any  
set system syslog file traffic-log match ntpflow  
set system syslog file cli-commands authorization info  
set system syslog file cli-commands interactive-commands info  
set system syslog file traffic-denied any any  
set system syslog file traffic-denied match "session denied"  
set system syslog file default-log-messages any any  
set system syslog file default-log-messages structured-data  |

### 4.5 Implicit Deny Rule exist and is Logged

```
set nat enable
```

### 4.6 Add comment to FW Policy

Below is an example firewall policy with a comment:

```
config firewall policy
edit 2
  set srcintf "Links to Core"
  set dstintf "Uplink-XXXX"
  set srcaddr "all"
  set dstaddr "all"
  set action accept
  set comments "Change Request 34232"
  set schedule "always"
  set service "ANY"
  set logtraffic enable
  set nat enable
end
```

### 4.7 NTP Server Configuration

```
config system ntp
  config ntpserver
    edit 1
      set ntpv3 enable
      set server "XX.YY.201.2"
    next
e2
    set ntpv3 enable
    set server "XX.YY.201.3"
    next
  end
  set ntpsync enable
  set syncinterval 60
end
```
ADVANCED THREAT CASES - ENVIRONMENT

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

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

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

<table>
<thead>
<tr>
<th>ID</th>
<th>Threat Case Development</th>
</tr>
</thead>
<tbody>
<tr>
<td>INTOFF</td>
<td>International Offices – Global MPLS</td>
</tr>
<tr>
<td>SSLVPN</td>
<td>Juniper SSL VPN</td>
</tr>
<tr>
<td>NATIONAL</td>
<td>IPVPN – National MPLS IPVPN</td>
</tr>
<tr>
<td>WIRELESS</td>
<td>Wireless Infrastructure</td>
</tr>
<tr>
<td>VOIPUC</td>
<td>Voice over IP</td>
</tr>
<tr>
<td>VSAT</td>
<td>VSAT – Satellite</td>
</tr>
<tr>
<td>DIGPKI</td>
<td>PKI and X.509 Digital Certificates (systems threat case)</td>
</tr>
<tr>
<td>AAA</td>
<td>AAA (systems threat case)</td>
</tr>
<tr>
<td>HIPS</td>
<td>HIPS (system threat case and ePO integration)</td>
</tr>
<tr>
<td>EXECACC</td>
<td>Executive Account Monitoring</td>
</tr>
<tr>
<td>SAP</td>
<td>SAP Router and SAP Privilege Activity Monitoring</td>
</tr>
<tr>
<td>COMPLIANCE</td>
<td>Compliance and Best Practices Configuration</td>
</tr>
<tr>
<td>NAC</td>
<td>Network Admission Control –</td>
</tr>
</tbody>
</table>
ADVANCED THREAT CASES - ENVIRONMENT

• To define threat cases per environment ...
  .... Eventually .... Should .... Include .... All .... Environment .....
Develop Threat Cases – RHEL

1. Preamble

ATTENTION
Audit configuration changes were tested on RHEL 5.0.0.2. For other versions, configurations may differ. Please consult the vendor’s documentation for the platform on the corresponding audit configuration steps.

2. Prerequisites

<table>
<thead>
<tr>
<th>#</th>
<th>Document Title</th>
</tr>
</thead>
<tbody>
<tr>
<td>1</td>
<td>Unix and Powerbroker – STRM Integration</td>
</tr>
<tr>
<td>2</td>
<td>Unix Systems – Threat Cases</td>
</tr>
<tr>
<td>3</td>
<td>root access for audit settings modifications</td>
</tr>
</tbody>
</table>

3. Audit description

RHEL audit has the following mechanism of writing audit trail: binary mode and dispatcher mode. Log file mode write log entries to a log file stored on the disk space, whereas dispatcher mode forwards the event to a dispatch, 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:
   ```bash
   aus2arch -m
   ```

2. Audit daemon status can be verified with the following command:

DTS SOLUTION
smart solution for the smart business
Develop Threat Cases – RHEL

NOTE
Entries must be specified to the exact word, as QRadar/STRM parser expects % 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
   # STRM rules
   # Module, comment out if loaded previously
   $ModLoad im_file
   # work directory
   $WorkDirectory /var/lib/rsyslog $ where to place spool files
   # Input audit file
   $InputFile /var/log/audit/audit.log
   #InputFileStats in audit.stats
   $InputFileTag audit
   $InputFileFacility local10
   #InputFileSecurity logname
   #InputFileFilterLevel 10
   $InputRunFileMonitor
   # Send messages
   local6.debug &@$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.

<table>
<thead>
<tr>
<th>#</th>
<th>EventID</th>
<th>Meaning</th>
</tr>
</thead>
<tbody>
<tr>
<td>1</td>
<td>SYSCALL</td>
<td>At a job has been added</td>
</tr>
<tr>
<td>2</td>
<td>SYSCALL</td>
<td>At a job has been removed</td>
</tr>
<tr>
<td>3</td>
<td>CONFIG_CHANGE</td>
<td>Audit configuration change was detected</td>
</tr>
<tr>
<td>4</td>
<td>USER_END</td>
<td>A cron job has finished</td>
</tr>
<tr>
<td>5</td>
<td>SYSCALL</td>
<td>A cron job has been added</td>
</tr>
<tr>
<td>6</td>
<td>SYSCALL</td>
<td>A cron job has been removed</td>
</tr>
<tr>
<td>7</td>
<td>SYSCALL</td>
<td>An admin user is being removed from /etc/group group</td>
</tr>
<tr>
<td>8</td>
<td>SYSCALL</td>
<td>A group has been changed</td>
</tr>
<tr>
<td>9</td>
<td>ADD_GROUP</td>
<td>A group has been created</td>
</tr>
<tr>
<td>10</td>
<td>DEL_GROUP</td>
<td>A group has been removed</td>
</tr>
<tr>
<td>11</td>
<td>SYSCALL</td>
<td>A user is being removed from /etc/group group</td>
</tr>
<tr>
<td>12</td>
<td>SYSCALL</td>
<td>A password has been changed for the current user</td>
</tr>
<tr>
<td>13</td>
<td>SYSCALL</td>
<td>Write to /etc/security/environ</td>
</tr>
</tbody>
</table>
| 14 | SYSCALL | Write to /etc/security/group
| 15 | SYSCALL | Write to /etc/security/limits
| 16 | SYSCALL | Write to /etc/security/login.cfg
| 17 | SYSCALL | Write to /etc/security/passwd
| 18 | SYSCALL | Write to /etc/security/user
| 19 | SYSCALL | Change user’s attributes |
| 20 | ADD_USER | Create a user |
| 21 | SYSCALL | Lock a user |
| 22 | USER_AUTH | User login to the system |
| 23 | DEL_USER | Delete a user |

*RHEL auditing of specific objects is only possible with parsing of certain parameters of specific audit events. Therefore, all custom audit events are marked EVENT and depend on its parameters contents.
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
Sample SCADA/ICS Dashboard
Sample SCADA/ICS Dashboard
Sample SCADA/ICS Dashboard
## Offense Management Naming Convention

### Proposed Offense Naming Convention

![](image)

### Index

<table>
<thead>
<tr>
<th>Index</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>AAA</td>
<td><strong>Environment / Infrastructure Zone</strong>&lt;br&gt;&lt;br&gt;• This is the environment / infrastructure zone where the offense has taken place.&lt;br&gt;• Typical environment / infrastructure zone include:&lt;br&gt;  o Firewall / Perimeter and DMZ and Extranet&lt;br&gt;  o Business Internet Services&lt;br&gt;  o Home Internet Services&lt;br&gt;  o Routers – Core Network / LTE&lt;br&gt;  o Web Service – Web hosting in DMZ&lt;br&gt;  o Active Directory – UserSegment&lt;br&gt;  o Enterprise Device&lt;br&gt;  o SDWAN / C2 Device</td>
</tr>
<tr>
<td>BBB</td>
<td><strong>Infrastructure Device Type</strong>&lt;br&gt;&lt;br&gt;• This is the device type(s) where the offense has been triggered.&lt;br&gt;• Typical device type include:&lt;br&gt;  o Network – Switch / Router&lt;br&gt;  o Security – FW, IPS, WAF, Anti-V, Vulnerability Management, AAA, IAM&lt;br&gt;  o Web Services – II, Apache&lt;br&gt;  o Database – Oracle, SQL&lt;br&gt;  o Application and Presentation – Middleware&lt;br&gt;  o Legacy – Mainframes / VAS / MVS and RTUs&lt;br&gt;  o Telecommunication</td>
</tr>
<tr>
<td>CCC</td>
<td><strong>Offense Category</strong>&lt;br&gt;&lt;br&gt;• This is the offense category that is assigned to the offense customized based on Aramco’s threat detection rules.&lt;br&gt;• Typical offense categories include:&lt;br&gt;  o Unauthorized Access</td>
</tr>
</tbody>
</table>

---

DTS SOLUTION<br>smart solution for the smart business
Offense Management Workflow

1. DATA AGGREGATION - SRTM
   Assigned Role: SOC Analyst
   - Log Collection
   - Log Parsing
   - Log Normalization

2. INCIDENT IDENTIFICATION
   Assigned Role: SOC Analyst
   - NEW INCIDENT NOTICED
   - OFFENSE CREATED

3. INVESTIGATION
   Assigned Role: SOC Analyst & System Owner
   - Investigate Service Impacted
   - Make Forensic Search
   - Check Compliance Templates

4. INCIDENT COORDINATION
   Assigned Role: SOC Analyst
   - Ticket
   - Close offense with ticket

5. OFFENSE CLOSURE
   Assigned Role: SOC Analyst
   - Close offense and update ticketing system

6. REPORT GENERATION
   Assigned Role: SOC Analyst
   - Coordinate with Service Center

7. IP WATCHLIST
   Assigned Role: SOC Analyst
   - Environment
   - Bad IP Reputation
   - Relevant
   - ACTION 1
     - ACTION 2
     - ACTION 3
Security Operations Center

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
SOC Wiki – SIEM Threat Cases

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:

<table>
<thead>
<tr>
<th>AAA.RSA.001 - UNIX Security Monitoring</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Threat Cases</strong></td>
</tr>
<tr>
<td><strong>AAA.RSA.001 - Excessive Reject Message</strong></td>
</tr>
<tr>
<td><strong>AAA.RSA.002 - Unauthorized user trying to authenticate with token</strong></td>
</tr>
<tr>
<td><strong>AAA.RSA.003 - Unauthorized user trying to authenticate with expired or disabled token</strong></td>
</tr>
<tr>
<td><strong>AAA.RSA.004 - Passcode Reuse Attack Replay</strong></td>
</tr>
<tr>
<td><strong>AAA.RSA.005 - Abnormal Behaviour of PIN change</strong></td>
</tr>
<tr>
<td><strong>AAA.RSA.006 - Unusual number of Account Lockout</strong></td>
</tr>
<tr>
<td><strong>AAA.RSA.007 - RSA Admin Account Created</strong></td>
</tr>
</tbody>
</table>

AAA.RSA.001 - UNIX

AAA.RSA.001 - Excessive Reject Message

<table>
<thead>
<tr>
<th><strong>Threat Case ID:</strong></th>
<th>AAA.RSA.001</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Description:</strong></td>
<td>Excessive Reject Message</td>
</tr>
<tr>
<td><strong>Device Type:</strong></td>
<td>RSA Authentication Manager</td>
</tr>
<tr>
<td><strong>Threat Violation:</strong></td>
<td>Policy Violation</td>
</tr>
<tr>
<td><strong>Threat Criticality:</strong></td>
<td>Medium</td>
</tr>
<tr>
<td><strong>Threat Category:</strong></td>
<td>Access Brute Force Attempt</td>
</tr>
<tr>
<td><strong>Threat Log Source:</strong></td>
<td>RSA Authentication Manager</td>
</tr>
<tr>
<td><strong>Action Required:</strong></td>
<td>Notify AMD Support</td>
</tr>
<tr>
<td><strong>Responsible Group:</strong></td>
<td>AMD</td>
</tr>
<tr>
<td><strong>STRM Implementation Comments:</strong></td>
<td>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</td>
</tr>
<tr>
<td><strong>General Comments:</strong></td>
<td>A brute attempt to a single device (user or admin authentication) using same username. Best practices are 10 incorrect login attempts should lock a user account.</td>
</tr>
<tr>
<td><strong>Correlation:</strong></td>
<td>TBA</td>
</tr>
<tr>
<td><strong>Payload:</strong></td>
<td>TBA</td>
</tr>
</tbody>
</table>
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 Levels (SALs) in Critical Infrastructure

- Functional Requirements
- Security Levels
  - Based on 4 x Security Levels

<table>
<thead>
<tr>
<th>IEC 62443 / ISA-99</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>SL 1</strong></td>
</tr>
<tr>
<td>Protection against casual or coincidental violation</td>
</tr>
<tr>
<td><strong>SL 2</strong></td>
</tr>
<tr>
<td>Protection against intentional violation using simple means</td>
</tr>
<tr>
<td><strong>SL 3</strong></td>
</tr>
<tr>
<td>Protection against intentional violation using sophisticated means</td>
</tr>
<tr>
<td><strong>SL 4</strong></td>
</tr>
<tr>
<td>Protection against intentional violation using sophisticated means with extended resources</td>
</tr>
</tbody>
</table>

**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**
- Capability SLs
- Control System features

---

**DTS SOLUTION**
smart solution for the smart business
Security Assurance Level

Achieved SL vs. Target SL

- Access control (AC)
- Resource availability (RA)
- Use control (UC)
- Data integrity (DI)
- Data confidentiality (DC)
- Restrict data flow (RDF)
- Timely response to an event (TRE)

Achieved Security Level
Target Security Level