SOC Project Implementation Guide

A Comprehensive Guide to Building and Operating a Professional Security Operations Center

Author: Shayshab Azad

https://www.patreon.com/info_sec

Complete Implementation Guide for Security Operations Centers

Including Architecture, Configuration, Automation, and Best Practices

Table of Contents

Chapter 1: Introduction & Overview

1.1 Project Objectives

The SOC (Security Operations Center) Project represents a comprehensive security monitoring and incident response framework designed for modern cloud and hybrid environments. This enterprise-grade solution implements automated threat detection, incident management, and response capabilities using industry-standard tools and frameworks.

- Establish real-time threat detection across cloud and on-premises environments
- Implement automated incident response and ticket management
- Provide comprehensive security monitoring with MITRE ATT&CK; integration
- Create a scalable and maintainable security operations platform
- Enable compliance with industry standards and regulations

1.2 Technology Stack Overview

The SOC project integrates four core technologies to provide comprehensive security monitoring and incident response capabilities:

Tool	Purpose	Key Features
Splunk Enterprise	SIEM Platform	Log aggregation, real-time monitoring, advanced search
Wazuh	EDR Solution	Endpoint detection, file integrity monitoring, active response
MITRE ATT&CK	Threat Intelligence	Attack technique mapping, threat categorization
Jira	Incident Management	Ticket creation, workflow automation, team collaboration

1.3 System Requirements

The SOC project requires specific hardware and software configurations to ensure optimal performance and reliability. The following requirements are minimum specifications for a production environment.

Component	Minimum Specs	Recommended Specs
Splunk Server	8 CPU cores, 16GB RAM, 500GB storage	16 CPU cores, 32GB RAM, 1TB SSD
Wazuh Manager	4 CPU cores, 8GB RAM, 100GB storage	8 CPU cores, 16GB RAM, 200GB SSD
Jira Server	4 CPU cores, 8GB RAM, 100GB storage	8 CPU cores, 16GB RAM, 200GB SSD
Network	1Gbps connectivity	10Gbps backbone, redundant paths

1.4 Project Timeline

The SOC project implementation is divided into five phases, each building upon the previous phase to create a comprehensive security operations center.

Phase	Duration	Key Activities
Phase 1: Foundation	Week 1-2	Environment setup, tool installation, basic configuration
Phase 2: Core Implementation	Week 3-4	Splunk/Wazuh config, Jira integration, cloud logs
Phase 3: Detection & Monitoring	Week 5-6	Detection rules, alerts, dashboards, MITRE integration
Phase 4: Automation & Response	Week 7-8	Automated responses, incident workflows, testing
Phase 5: Testing & Optimization	Week 9-10	Comprehensive testing, optimization, documentation

1.5 Success Metrics

The success of the SOC project implementation is measured through specific metrics across detection performance, response efficiency, and operational excellence.

Category	Metric	Target
Detection Performance	Time to Detection (TTD)	< 5 minutes
Detection Performance	False Positive Rate	< 10%
Detection Performance	MITRE ATT&CK Coverage	> 80%
Response Efficiency	Time to Response (TTR)	< 15 minutes
Response Efficiency	Automated Response Success	> 95%
Operational Excellence	System Uptime	> 99.5%
Operational Excellence	Dashboard Response Time	< 3 seconds

1.6 Key Takeaways

• The SOC project provides comprehensive security monitoring and incident response capabilities

• Four core tools work together: Splunk (SIEM), Wazuh (EDR), MITRE ATT&CK; (intelligence), Jira (management)

• Proper planning and preparation are essential for successful implementation

• Security and compliance considerations must be addressed throughout the project

• Success metrics should be established and monitored throughout the implementation

Chapter 2: Architecture & Design

2.1 SOC Architecture Overview

The SOC architecture is designed as a layered, modular system that provides comprehensive security monitoring and incident response capabilities. The architecture follows security best practices and enables scalability, maintainability, and operational efficiency.

Architecture Principles:

- Defense in Depth: Multiple layers of security controls
- Zero Trust: Verify every access attempt
- Modular Design: Independent component operation
- Scalability: Support for growth and expansion
- Security First: Built-in security controls

2.2 High-Level Architecture

The SOC high-level architecture consists of four main layers: data collection, processing and analysis, detection and response, and management and reporting.

Layer	Components	Function
Data Collection	Cloud APIs, Log Sources, Agents	Gather security events and logs from all sources
Processing & Analysis	Splunk Indexers, Search Heads	Parse, index, correlate, and analyze data
Detection & Response	Detection Rules, Wazuh Active Response	Identify threats and execute automated responses
Management & Reporting	Jira, Dashboards, Reports	Incident management and operational reporting

2.3 Data Flow Architecture

The SOC data flow follows a structured pipeline from data collection through incident response. Each component plays a specific role in the security monitoring ecosystem.

1. Data Collection: Logs and events from cloud platforms, endpoints, and network devices
2. Data Ingestion: Splunk HTTP Event Collector (HEC) receives and processes data
3. Data Indexing: Splunk indexes and stores data for fast retrieval and analysis
4. Real-time Analysis: Splunk Search Processing Language (SPL) correlates events
5. Threat Detection: Detection rules identify security threats and anomalies
6. Alert Generation: Automated alerts trigger when threats are detected
7. Incident Response: Wazuh active response executes automated actions
8. Incident Management: Jira creates and tracks incident tickets

9. Reporting: Dashboards and reports provide operational visibility

2.4 Network Architecture

The network architecture provides secure communication between SOC components while maintaining proper segmentation and access controls.

Network Segment	VLAN ID	Purpose	Components
Security Management	VLAN 100	SOC tool administration	Splunk, Wazuh, Jira management interfaces
Data Collection	VLAN 200	Log and event collection	HEC endpoints, log forwarders, agents
Analysis	VLAN 300	Data processing and analysis	Splunk indexers, search heads, correlation engines
Response	VLAN 400	Automated response actions	Wazuh active response, firewall management
DMZ	VLAN 500	External-facing components	Web interfaces, API endpoints

2.5 Security Architecture

The security architecture implements defense-in-depth principles with multiple layers of security controls to protect the SOC infrastructure and data.

Control Layer	Security Controls	Implementation
Network Security	Firewalls, IDS/IPS, VLANs	Segment network traffic, monitor for threats
Access Control	RBAC, MFA, VPN	Control access to SOC tools and data
Data Protection	Encryption, DLP, Backup	Protect data at rest and in transit
Monitoring	SIEM, EDR, Log Analysis	Monitor all SOC activities and events
Incident Response	Automation, Playbooks, Escalation	Respond to security incidents

2.6 Scalability Design

The SOC architecture is designed to scale horizontally and vertically to accommodate growth in data volume, user count, and organizational requirements.

• Horizontal Scaling: Add more Splunk indexers and search heads as data volume grows

• Vertical Scaling: Increase CPU, RAM, and storage on existing servers

• Load Balancing: Distribute traffic across multiple instances

• Clustering: Implement Splunk and Wazuh clustering for high availability

• Data Retention: Implement tiered storage for cost-effective data management

• Performance Optimization: Tune queries, indexes, and system parameters

2.7 High Availability Design

High availability ensures continuous SOC operations even during component failures or maintenance windows.

• Redundant Servers: Multiple instances of each SOC component

• Load Balancers: Distribute traffic and provide failover

• Clustered Storage: Shared storage for data persistence

• Backup Systems: Regular backups and disaster recovery

• Monitoring: Health checks and automatic failover

• Documentation: Runbooks and recovery procedures

2.8 Integration Architecture

The integration architecture defines how SOC components communicate and share data to provide comprehensive security monitoring and response capabilities.

Integration Point	Components	Protocol	Purpose
Data Collection	Splunk HEC, Cloud APIs	HTTPS, REST	Ingest logs and events
Alert Correlation	Splunk, Wazuh	Internal APIs	Correlate alerts across tools
Incident Management	Splunk, Wazuh, Jira	REST APIs	Create and track incidents
Response Automation	Wazuh, Firewall, IAM	CLI, APIs	Execute automated responses
Reporting	Splunk, Jira, Dashboards	Web APIs	Generate reports and metrics

2.9 Compliance Architecture

The compliance architecture ensures the SOC meets regulatory and industry standards for data protection, security monitoring, and incident response.

• SOC 2 Type II: Security, availability, and confidentiality controls

• ISO 27001: Information security management system

• PCI DSS: Payment card data security standards

• HIPAA: Healthcare data protection requirements

• GDPR: European data protection regulations

• NIST Cybersecurity Framework: Risk management and security controls

2.10 Design Best Practices

Follow these best practices when designing and implementing the SOC architecture to ensure security, performance, and maintainability.

1. Implement defense in depth with multiple security layers
2. Use network segmentation to isolate different components
3. Enable encryption for data at rest and in transit
4. Implement proper access controls and authentication

5. Design for scalability and high availability
6. Document all architecture decisions and configurations
7. Test disaster recovery and business continuity procedures
8. Monitor and log all system activities
9. Regularly update and patch all components
10. Conduct security assessments and penetration testing

Chapter 3: Environment Setup

3.1 Pre-Installation Planning

Proper planning is essential for successful SOC implementation. This section covers the planning phase, including requirements gathering, resource allocation, and timeline development.

1. Review system requirements and hardware specifications
2. Identify network infrastructure and connectivity requirements
3. Plan IP addressing scheme and network segmentation
4. Determine storage requirements and backup strategies
5. Identify team roles and responsibilities
6. Plan security policies and access controls
7. Develop implementation timeline and milestones
8. Prepare disaster recovery and business continuity plans

3.2 Server Preparation

Prepare the server environment for SOC tool installation. This includes operating system setup, security hardening, and performance optimization.

1. Install and configure base operating system (Ubuntu 20.04 LTS recommended)
2. Apply all security patches and updates
3. Configure network interfaces and IP addressing
4. Set up firewall rules and security groups
5. Install required system dependencies and packages
6. Configure DNS resolution and time synchronization
7. Set up logging and monitoring for the server
8. Create dedicated user accounts for SOC tools
9. Configure SSH access with key-based authentication
10. Set up backup and recovery procedures

3.3 Operating System Installation

Install and configure the base operating system with security best practices and performance optimizations for SOC operations.

```
# Download Ubuntu 20.04 LTS
wget https://releases.ubuntu.com/20.04/ubuntu-20.04.6-live-server-amd64.iso

# Create bootable USB (on another system)
```

```
sudo dd if=ubuntu-20.04.6-live-server-amd64.iso of=/dev/sdX bs=4M
status=progress

# Install with minimal packages

# Select: OpenSSH server, Basic Ubuntu server

# Configure: Static IP, hostname, user account
```

3.4 System Updates and Security

Apply all system updates and implement security hardening measures to protect the SOC infrastructure from threats.

```
# Update package lists

sudo apt update

# Upgrade all packages

sudo apt upgrade -y

# Install security updates

sudo apt dist-upgrade -y

# Install additional security packages

sudo apt install -y ufw fail2ban rkhunter unattended-upgrades

# Configure automatic security updates

sudo dpkg-reconfigure -plow unattended-upgrades
```

3.5 Network Configuration

Configure network settings to ensure proper communication between SOC components and external data sources. This includes IP addressing, routing, and firewall rules.

```
# Configure network interfaces

sudo nano /etc/netplan/01-netcfg.yaml

# Example netplan configuration:

network:

version: 2

renderer: networkd

ethernets:

eth0:

addresses:

- 192.168.100.10/24

gateway4: 192.168.100.1

nameservers:
```

```
    addresses: [8.8.8.8, 8.8.4.4]

# Apply network configuration
sudo netplan apply
```

3.6 Firewall Configuration

Configure firewall rules to protect the SOC infrastructure while allowing necessary communication for security tools and data collection.

```
# Enable UFW firewall
sudo ufw enable

# Allow SSH access
sudo ufw allow 22/tcp

# Allow Splunk web interface
sudo ufw allow 8000/tcp

# Allow Splunk management port
sudo ufw allow 8089/tcp

# Allow Wazuh manager
sudo ufw allow 1514/tcp

# Allow Wazuh cluster communication
sudo ufw allow 1516/tcp

# Allow Jira web interface
sudo ufw allow 8080/tcp

# Show firewall status
sudo ufw status verbose
```

3.7 User Account Setup

Create dedicated user accounts for SOC tools with appropriate permissions and security controls. Implement role-based access control (RBAC) for team members.

```
# Create SOC administrator account
sudo useradd -m -s /bin/bash socadmin
sudo usermod -aG sudo socadmin

# Create SOC analyst account
sudo useradd -m -s /bin/bash socanalyst
sudo usermod -aG soc socanalyst
```

```
# Set up SSH key authentication
sudo mkdir -p /home/socadmin/.ssh
sudo chmod 700 /home/socadmin/.ssh
sudo chown socadmin:socadmin /home/socadmin/.ssh

# Create SOC group
sudo groupadd soc
sudo usermod -aG soc socadmin
sudo usermod -aG soc socanalyst
```

3.8 System Dependencies

Install required system dependencies and packages for SOC tools. This includes Python, Java, and other runtime environments needed for security tools.

```
# Update package lists
sudo apt update

# Install Python and pip
sudo apt install -y python3 python3-pip python3-venv

# Install Java (required for Splunk)
sudo apt install -y openjdk-11-jdk

# Install additional dependencies
sudo apt install -y curl wget git unzip

# Install monitoring tools
sudo apt install -y htop iotop nethogs

# Install network tools
sudo apt install -y net-tools tcpdump nmap

# Verify installations
python3 --version
java -version
curl --version
```

3.9 Storage Configuration

Configure storage for SOC data, logs, and backups. Implement proper partitioning, RAID configuration, and backup strategies for data protection.

1. Partition storage for different data types (OS, applications, data, logs)
2. Configure RAID for data redundancy and performance

3. Set up logical volume management (LVM) for flexibility
4. Create mount points for SOC data directories
5. Configure disk quotas and monitoring
6. Set up automated backup procedures
7. Implement data retention policies
8. Configure storage monitoring and alerting

3.10 Security Hardening

Implement security hardening measures to protect the SOC infrastructure from threats and ensure compliance with security standards.

```
# Disable unnecessary services
sudo systemctl disable bluetooth
sudo systemctl disable cups
sudo systemctl disable avahi-daemon

# Configure SSH security
sudo nano /etc/ssh/sshd_config
# Set: PermitRootLogin no
# Set: PasswordAuthentication no
# Set: AllowUsers socadmin

# Restart SSH service
sudo systemctl restart ssh

# Configure fail2ban
sudo cp /etc/fail2ban/jail.conf /etc/fail2ban/jail.local
sudo systemctl enable fail2ban
sudo systemctl start fail2ban
```

3.11 Monitoring Setup

Set up system monitoring to track server performance, resource usage, and security events. This provides visibility into SOC infrastructure health.

```
# Install monitoring tools
sudo apt install -y sysstat iotop htop

# Configure system monitoring
sudo systemctl enable sysstat
sudo systemctl start sysstat

# Set up log rotation
```

```
sudo nano /etc/logrotate.d/soc

# Configure log monitoring
sudo apt install -y logwatch
sudo logwatch --detail High --mailto admin@company.com --range Today
```

3.12 Pre-Installation Checklist

Complete this checklist before proceeding with SOC tool installation to ensure all prerequisites are met and the environment is properly configured.

- ■ Operating system installed and updated
- ■ Network connectivity verified
- ■ Firewall rules configured
- ■ User accounts created and configured
- ■ SSH access tested with key authentication
- ■ System dependencies installed
- ■ Storage configured and mounted
- ■ Security hardening completed
- ■ Monitoring tools configured
- ■ Backup procedures tested
- ■ DNS resolution working
- ■ Time synchronization configured
- ■ System performance baseline established
- ■ Documentation updated
- ■ Team access configured

3.13 Environment Validation

Validate the environment configuration to ensure all components are working correctly and ready for SOC tool installation.

```
# Check system information
uname -a
cat /etc/os-release

# Verify network configuration
ip addr show
ip route show
ping -c 3 8.8.8.8

# Check firewall status
sudo ufw status
```

```
# Verify user accounts
id socadmin
id socanalyst

# Check disk space
df -h

# Verify system resources
free -h
nproc

# Test SSH access
ssh socadmin@localhost
```

Chapter 4: Tool Installation

4.1 Splunk Enterprise Installation

Splunk Enterprise is the primary SIEM platform for the SOC project. Follow these step-by-step instructions to install and configure Splunk Enterprise.

1. Download Splunk Enterprise from the official website
2. Extract the installation package to /opt/splunk
3. Run the Splunk installation script
4. Configure Splunk admin password
5. Start Splunk services
6. Access Splunk web interface on port 8000

Splunk Installation Commands:

```
# Download and extract Splunk
wget -O splunk.tgz 'https://download.splunk.com/products/splunk/releases/9.0.0/linux/splunk-9.0.0-17e00c557dc1-Linux-x86_64.tgz'
tar -xzf splunk.tgz -C /opt

# Start Splunk for the first time
cd /opt/splunk
./bin/splunk start --accept-license

# Set admin password
./bin/splunk edit user admin -password 'YourSecurePassword' -role admin -auth admin:changeme
```

4.2 Wazuh Installation

Wazuh provides endpoint detection and response capabilities. Install Wazuh manager and agents according to these instructions.

```
# Install Wazuh repository
curl -s https://packages.wazuh.com/key/GPG-KEY-WAZUH | sudo apt-key add -
echo 'deb https://packages.wazuh.com/4.x/apt/ stable main' | sudo tee /etc/apt/sources.list.d/wazuh.list

# Install Wazuh manager
sudo apt-get update
sudo apt-get install wazuh-manager
```

```
# Start Wazuh manager
sudo systemctl daemon-reload
sudo systemctl enable wazuh-manager
sudo systemctl start wazuh-manager
```

4.3 Jira Setup

Jira provides incident management and ticket tracking capabilities. Set up Jira Cloud or Server according to your organization's requirements.

1. Create Jira Cloud account or install Jira Server
2. Create a new project called 'Security Incidents'
3. Configure issue types: Security Incident, Security Alert, Threat Intelligence
4. Set up custom fields for MITRE ATT&CK; techniques
5. Configure user permissions and access controls
6. Generate API token for integration

Chapter 5: Splunk Configuration

5.1 Splunk Installation

Install Splunk Enterprise on the SOC server. This includes downloading the software, configuring the installation, and setting up initial access.

```
# Download Splunk Enterprise
wget -O splunk-9.0.4-419ad9369127-linux-2.6-amd64.deb \
'https://download.splunk.com/products/splunk/releases/9.0.4/linux/splunk-9.0.4-419ad9369127-linux-2.6-amd64.deb'

# Install Splunk package
sudo dpkg -i splunk-9.0.4-419ad9369127-linux-2.6-amd64.deb

# Create splunk user
sudo useradd -r -d /opt/splunk -s /bin/bash splunk

# Set ownership
sudo chown -R splunk:splunk /opt/splunk

# Start Splunk for first time
sudo -u splunk /opt/splunk/bin/splunk start --accept-license --answer-yes --no-prompt --seed-passwd admin123
```

5.2 Initial Configuration

Configure Splunk with basic settings including server name, admin password, and network settings for SOC operations.

```
# Set server name
sudo -u splunk /opt/splunk/bin/splunk set servername soc-splunk-server

# Set default hostname
sudo -u splunk /opt/splunk/bin/splunk set default-hostname soc-splunk-server

# Change admin password
sudo -u splunk /opt/splunk/bin/splunk edit user admin -password 'SecurePassword123!' -role admin -auth admin:admin123

# Enable Splunk web interface
sudo -u splunk /opt/splunk/bin/splunk enable web-server -port 8000

# Configure Splunk to start on boot
sudo /opt/splunk/bin/splunk enable boot-start -user splunk
```

```
# Restart Splunk
sudo -u splunk /opt/splunk/bin/splunk restart
```

5.3 Index Configuration

Configure Splunk indexes for different types of security data. This includes creating indexes for security events, cloud logs, and system logs.

```
# Create indexes.conf
sudo nano /opt/splunk/etc/system/local/indexes.conf

# Security events index
[security_events]
homePath = $SPLUNK_DB/security_events/db
coldPath = $SPLUNK_DB/security_events/colddb
thawedPath = $SPLUNK_DB/security_events/thaweddb
maxTotalDataSizeMB = 10000
frozenTimePeriodInSecs = 7776000
maxHotBuckets = 10
maxWarmBuckets = 300

# Cloud logs index
[cloud_logs]
homePath = $SPLUNK_DB/cloud_logs/db
coldPath = $SPLUNK_DB/cloud_logs/colddb
thawedPath = $SPLUNK_DB/cloud_logs/thaweddb
maxTotalDataSizeMB = 5000
frozenTimePeriodInSecs = 2592000

# System logs index
[system_logs]
homePath = $SPLUNK_DB/system_logs/db
coldPath = $SPLUNK_DB/system_logs/colddb
thawedPath = $SPLUNK_DB/system_logs/thaweddb
maxTotalDataSizeMB = 2000
frozenTimePeriodInSecs = 7776000
```

5.4 User and Role Management

Create user accounts and roles for SOC team members with appropriate permissions for different functions like analysis, administration, and reporting.

```
# Create SOC analyst user
```

```
sudo -u splunk /opt/splunk/bin/splunk add user soc_analyst -password
'AnalystPass123!' -role user -full-name 'SOC Analyst'

# Create SOC manager user

sudo -u splunk /opt/splunk/bin/splunk add user soc_manager -password
'ManagerPass123!' -role admin -full-name 'SOC Manager'

# Create custom role for analysts

sudo -u splunk /opt/splunk/bin/splunk add role soc_analyst_role
-srch-indexes-default security_events,cloud_logs -srch-indexes-allowed
security_events,cloud_logs,system_logs

# Assign role to user

sudo -u splunk /opt/splunk/bin/splunk edit user soc_analyst -role
soc_analyst_role -auth admin:SecurePassword123!

# List users and roles

sudo -u splunk /opt/splunk/bin/splunk list user

sudo -u splunk /opt/splunk/bin/splunk list role
```

5.5 Input Configuration

Configure data inputs to collect logs and events from various sources including system logs, network devices, and cloud platforms.

```
# Create inputs.conf

sudo nano /opt/splunk/etc/system/local/inputs.conf

# Monitor system logs

[monitor:///var/log/syslog]

index = system_logs

sourcetype = syslog

# Monitor auth logs

[monitor:///var/log/auth.log]

index = security_events

sourcetype = linux_secure

# Monitor SSH logs

[monitor:///var/log/secure]

index = security_events

sourcetype = ssh

# HTTP Event Collector (HEC)

[http://hec]

index = security_events
```

```
token = your_hec_token_here
disabled = 0
```

5.6 HTTP Event Collector Setup

Configure the HTTP Event Collector (HEC) to receive logs from external sources like cloud platforms, applications, and network devices.

```
# Enable HEC
sudo -u splunk /opt/splunk/bin/splunk http-event-collector enable -uri
https://localhost:8089 -auth admin:SecurePassword123!

# Create HEC token
sudo -u splunk /opt/splunk/bin/splunk http-event-collector create -name
'soc-hec-token' -uri https://localhost:8089 -auth admin:SecurePassword123!

# Configure HEC settings
sudo nano /opt/splunk/etc/system/local/inputs.conf

# Add HEC configuration
[http://hec]
index = security_events
token = your_generated_token_here
disabled = 0
sourcetype = _json
```

5.7 Search and Reporting Configuration

Configure search and reporting settings to optimize performance and enable advanced analytics capabilities for security monitoring.

```
# Configure search settings
sudo nano /opt/splunk/etc/system/local/limits.conf

# Search performance settings
[search]
maxout = 10
maxtotalsearchsize = 1000
max_mem_usage_mb = 2048

# Reporting settings
[reporting]
maxreports = 100
maxreportsperuser = 50
```

```
# Index search settings
[indexing]
maxmem = 2048
maxmem_high = 4096
```

5.8 Alert Configuration

Configure alerting capabilities to notify SOC team members of security events and enable automated response actions.

```
# Create alerts.conf
sudo nano /opt/splunk/etc/system/local/alert_actions.conf

# Email alert action
[email]
param.from = soc@company.com
param.to = soc-team@company.com
param.smtp_server = smtp.company.com
param.smtp_port = 587
param.sendresults = 1

# Script alert action for Jira integration
[script]
param.script = /opt/splunk/etc/apps/soc/bin/jira_alert_action.py
param.scriptargs = --jira-url https://company.atlassian.net --username
soc@company.com --api-token your_token --project-key SEC
```

5.9 Dashboard Creation

Create operational dashboards for SOC monitoring. This includes security event overview, threat detection metrics, and incident response tracking.

```
# Create dashboard directory
sudo mkdir -p /opt/splunk/etc/apps/soc/local/data/ui/nav
sudo chown -R splunk:splunk /opt/splunk/etc/apps/soc

# Create dashboard XML
sudo nano /opt/splunk/etc/apps/soc/local/data/ui/nav/default.xml

# Dashboard navigation




# Create dashboard views
```

```
sudo mkdir -p /opt/splunk/etc/apps/soc/local/data/ui/views

sudo nano /opt/splunk/etc/apps/soc/local/data/ui/views/soc_overview.xml
```

5.10 App Installation and Management

Install and configure Splunk apps for enhanced security monitoring capabilities. This includes security apps, add-ons, and custom applications.

```
# Install Splunk Enterprise Security (if licensed)

# Download from Splunk website and install

# Install Splunk App for AWS

sudo -u splunk /opt/splunk/bin/splunk install app /path/to/splunk-app-aws.tgz

# Install Splunk Add-on for Microsoft Windows

sudo -u splunk /opt/splunk/bin/splunk install app
/path/to/splunk-add-on-windows.tgz

# Install custom SOC app

sudo -u splunk /opt/splunk/bin/splunk install app /path/to/soc-app.tgz

# List installed apps

sudo -u splunk /opt/splunk/bin/splunk list app

# Enable/disable apps

sudo -u splunk /opt/splunk/bin/splunk disable app app_name

sudo -u splunk /opt/splunk/bin/splunk enable app app_name
```

5.11 Performance Tuning

Optimize Splunk performance for high-volume security data processing. This includes memory tuning, search optimization, and index management.

```
# Configure system limits

sudo nano /etc/security/limits.conf

# Add Splunk user limits

splunk soft nofile 8192

splunk hard nofile 32768

splunk soft nproc 2048

splunk hard nproc 8192

# Configure Splunk limits

sudo nano /opt/splunk/etc/system/local/limits.conf

# Memory and search limits
```