SOC Project: Complete Implementation Guide

Automated Threat Detection & Incident Response Framework

Comprehensive Implementation Guide with Splunk, Wazuh, MITRE ATT&CK;, and Jira Integration

Generated on July 29, 2025

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 Prerequisites

Before beginning the SOC project implementation, ensure all prerequisites are met:

- Administrative access to all servers and network infrastructure
- Valid licenses for Splunk Enterprise and Jira
- Cloud platform accounts with API access (AWS, Azure, GCP)
- Network diagrams and IP addressing scheme
- Security policies and compliance requirements documentation
- Team contact information and escalation procedures

1.5 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

1.6 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

1.7 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 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.

Stage	Component	Function
Data Collection	Cloud APIs, Log Sources	Gather security events and logs
Data Processing	Splunk Indexers	Parse, index, and enrich data
Analysis	Splunk Search Heads	Correlate and analyze security events
Detection	Detection Rules	Identify security threats and anomalies
Response	Wazuh Active Response	Automated threat response actions
Management	Jira Integration	Incident tracking and workflow

2.3 Network Architecture

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

- Security VLAN (VLAN 100): Dedicated network for SOC tools
- Management VLAN (VLAN 200): Administrative access to tools
- Data VLAN (VLAN 300): Data collection and processing
- DMZ: External-facing components with restricted access

Chapter 3: Environment Setup

3.1 Server Preparation

Proper server preparation is essential for successful SOC implementation. This section covers the step-by-step process for preparing your environment.

1. Update system packages and apply security patches
2. Configure network interfaces and IP addressing
3. Set up firewall rules and security groups
4. Create dedicated user accounts for SOC tools
5. Configure DNS resolution and time synchronization
6. Install required system dependencies

3.2 Network Configuration

Configure network settings to ensure proper communication between SOC components and external data sources.

Network Configuration Commands:

```
# Configure network interfaces
sudo ip addr add 192.168.100.10/24 dev eth0
sudo ip route add default via 192.168.100.1

# Configure firewall rules
sudo ufw allow 22/tcp
sudo ufw allow 8000/tcp
sudo ufw allow 1514/tcp
sudo ufw enable
```

3.3 User Account Setup

Create dedicated user accounts for SOC tools with appropriate permissions and security controls.

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

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