Project Scope Thread Systems PTY LTD

John Samami

James G

Damien W

Daniel B

Kubashen N

Peter N

High LEvel Scope

Contents

[Introduction 2](#_Toc96181297)

[Project Team 2](#_Toc96181298)

[Project Manager 2](#_Toc96181299)

[Project Scope 2](#_Toc96181300)

[Project Objectives 2](#_Toc96181301)

[Project Deliverables 2](#_Toc96181302)

[Problem solving methodology 2](#_Toc96181303)

[Resources 3](#_Toc96181304)

[Personnel 3](#_Toc96181305)

[Hardware 3](#_Toc96181306)

[Software 3](#_Toc96181307)

[Project Constraints 3](#_Toc96181308)

[Time 3](#_Toc96181309)

[Key milestones 3](#_Toc96181310)

[Restrictions 3](#_Toc96181311)

[Technical 3](#_Toc96181312)

[Establishing the Success of the Project 3](#_Toc96181313)

[Team performance system 3](#_Toc96181314)

[Further research and background information 4](#_Toc96181315)

# Introduction

The Scope document outlines what is to be expected of the project and what we are intending to do throughout the project. Completion of this scope document forms the start of the work planning documentation.

## Project Team

## Project manager - James G

## Role: Oversees entire project, coordinates tasks, manage resources, ensures timelines are met, maintains communication with stakeholders, managers and solves problems/

## Security Analyst - Damien W

## Role: Configures and monitors the SIEM tool, analyses security logs, identifies potential threats, and ensures the security of the IT systems.

## IT Support Specialist - Daniel B

## Role: Assists with the setup of virtual machines, installs necessary software, configures data inputs, and provides technical support throughout the project

## Network Engineer - John Samami

## Role: Ensures network configurations support data collection, manages network traffic analysis, and resolves any network-related issues that arise during the project.

## Vulnerability Analyst - Peter N

## Role: Conducts vulnerability scans, analyses scan results, identifies security gaps, and provides recommendations for mitigating vulnerabilities.

## Documentation Specialist - Kubashen N

## Role: Manages project documentation, compiles reports, ensures all project activities are well-documented, prepares presentations, and assists in creating the final implementation plan

## 

## Project Manager

James G - oversee the project and ensure deadlines are met and the brief and scope are met accordingly.

# Project Scope

## Project Objectives

## Implement a SIEM tool (Splunk) on two virtual machines.

## Gather and forward system data and network traffic.

## Perform a basic vulnerability scan.

## Demonstrate the effectiveness of the SIEM solution to the client.

## Plan for full implementation and future expansion if the PoC is successful.

## 

## Project Deliverables

**Proof of Concept Demonstration**: Deployment of Splunk on two PCs, with data collection and vulnerability scanning.

**Implementation Plan**: A detailed plan for rolling out the SIEM solution across the entire head office, including recommendations for future expansion.

**Documentation**: Reports on the PoC findings, configuration details, and vulnerability scan results.

## Problem solving methodology

* Requirement Analysis: Understand client needs and existing IT infrastructure.
* Research and Planning: Identify the best SIEM tool (Splunk) and plan its deployment.
* Setup and Configuration: Configure Splunk on virtual machines and set up data forwarding.
* Vulnerability Assessment: Conduct a basic vulnerability scan to identify potential issues.
* Testing and Validation: Ensure the solution works as intended and meets client requirements.
* Feedback and Improvement: Gather client feedback and make necessary adjustments.

# Resources

## Personnel

## Project Manager: James G

## Subject Matter: Project management, resource allocation, stakeholder communication, and problem-solving skills.

## Security Analyst: Damien W

## Subject Matter: SIEM tools (especially Splunk), cybersecurity principles, threat analysis, and log management.

## IT Support Specialist: Daniel B

## Subject Matter: Virtual machine setup, software installation, system configuration, and technical support.

## Network Engineer: John Samami

## Subject Matter: Network configuration and management, data traffic analysis, and network troubleshooting.

## Vulnerability Analyst: Peter N

## Subject Matter: Vulnerability scanning tools, security assessment, gap analysis, and mitigation strategies.

## Documentation Specialist: Kubashen N

## Subject Matter: Technical writing, documentation management, report compilation, and presentation preparation.

## 

## Hardware

Two PCs (virtual machines) provided by Threat Systems for testing.

## Software

Splunk SIEM tool for data collection and analysis.

Vulnerability scanning software (e.g., Qualys).

# Project Constraints

## Time

**Proof of Concept (PoC) Completion**: Estimated to be completed by session 9/10.

**Final Implementation Plan:** Estimated to be completed by week 16/17.

## 

## Key milestones

**Project Initiation and Planning (Weeks 1-2):**

Define project scope and objectives.

Identify required resources and team roles.

**Requirement Analysis and System Setup (Weeks 3-4):**

Analyse client requirements and existing infrastructure.

Set up virtual machines and install Splunk.

**Splunk Configuration and Data Collection (Weeks 5-6):**

Configure Splunk for data collection from two PCs.

Begin data forwarding and monitoring.

**Vulnerability Assessment (Weeks 7-8):**

Conduct a basic vulnerability scan using Splunk.

Document findings and prepare for PoC demonstration.

**Proof of Concept Demonstration (Session 9/10):**

Present PoC to the client, showcasing data collection, monitoring, and vulnerability assessment.

Gather feedback and make necessary adjustments.

**Implementation Planning (Weeks 11-14):**

Develop a detailed plan for full-scale implementation.

Include recommendations for future expansion.

**Final Implementation Plan Presentation (Weeks 15-16/17):**

Present the final implementation plan to the client.

Obtain approval and prepare for full-scale rollout.

## 

## Restrictions

**Budget**: Adhere to any budget constraints set by Threat Systems Pty Ltd.

**Compliance:** Ensure all activities comply with company policies and industry regulations.

**Resource Availability:** Work within the availability of provided virtual machines and other resources.

## 

## Technical

* **System Compatibility:** Ensure that Splunk and any other software used are compatible with the existing IT infrastructure.
* **Security:** Maintain high-security standards during the PoC and implementation to prevent any data breaches or vulnerabilities.
* **Performance:** Ensure that the SIEM solution does not negatively impact the performance of the existing systems.

# Establishing the Success of the Project

**Project Timeline Management:** Use Gantt charts to outline project phases and milestones. Regularly review progress and adjust timelines as needed.

**Quality Management:** Implement a quality assurance process to ensure all deliverables meet client standards. Conduct regular reviews and testing.

## Team performance system

**Project Management Software:** Use tools like Jira or Trello to track tasks, milestones, and team performance.

**Documentation and Tracking:** Maintain detailed project documentation, including meeting notes, task assignments, and progress reports.

**Performance Reviews:** Regularly review team performance and provide feedback to ensure continuous improvement.

# Further research and background information

|  |  |  |
| --- | --- | --- |
| Team member name | Question for client/instructor | New Information obtained |
| James G | How will success be measured for the PoC? | **Success for the Proof-of-Concept (PoC) will be measured by:**  **Successful Deployment:**  Installation and configuration of Splunk on two VMs.  Proper data forwarding without data loss or corruption.  **Functionality of SIEM Tool:**  Effective collection and analysis of system data and network traffic.  Detection, alerting, and logging of discrepancies in real-time.  **Vulnerability Scanning:**  Conducting a basic vulnerability scan on the VMs.  Identification and reporting of vulnerabilities.  Providing recommendations for remediation.  **Compliance and Reporting:**  Generating reports that meet company policies and compliance standards.  Customization and automation of reporting.  **User and Management Satisfaction:**  Positive feedback from IT service team and management.  Demonstration of reduced workload for the IT service team.  Performance Metrics:  Minimal disruption to VM operations due to the SIEM tool.  Demonstration of scalability for future expansion.  Security Incident Detection and Response:  Detection of simulated or real security incidents.  Effective response to incidents using the SIEM tool.  Documentation and Knowledge Transfer:  Comprehensive documentation of setup, configuration, and usage.  Knowledge transfer session for the IT service team. |
| Damien W | Are there any specific compliance standards we need to consider for Threat Systems Pty Ltd? | Our short-term aim is to achieve Essential 8 Maturity Level 1 compliance. However, we will be aiming to achieve ISO 27001 compliance within the next 36 months. |
| Daniel B | What are the preferred communication channels with the client? | We will prefer regular updates on the progress through emails and Microsoft Teams channel. |
| John Samami | Can we get a detailed network topology for better planning? | We are currently undergoing a digital transformation by adopting a cloud-first approach, which is causing our network topology to evolve. This PoC should be independent of our current network topology and vendor-specific technologies. |
| Peter N | Are there specific vulnerabilities or threats we should prioritise? | We are prioritising the following areas:  Phishing and Social Engineering  Ransomware  Unpatched Software  Insider Threats  Weak Passwords  Data Breaches  Malware and Viruses  Network Security  Physical Security  Third-Party Risks  Cloud Security  Risk and Policy Management  Regulatory Compliance |
| Kubashen N | Are there any existing documentation standards we need to follow? | We will be following NIST/SANS standards for Incident Response. For compliance, we are aiming for Essential 8 Maturity Level 1 in the short term and ISO 27001 within the next 36 months. |