|  |  |  |  |  |
| --- | --- | --- | --- | --- |
|  | | | | |
|  | **Project Implementation Plan**  John Samami  James G  Damien W  Daniel B  Kubashen N  Peter N |  |  |  |

## Table of Contents

[Table of Contents 3](#_Toc99020875)

[Introduction 4](#_Toc99020876)

[Document Scope 4](#_Toc99020877)

[Project Methodology 4](#_Toc99020878)

[Change management 4](#_Toc99020879)

[Solution Design 5](#_Toc99020880)

[Project Phases 5](#_Toc99020881)

[Milestones 5](#_Toc99020882)

[Resources 5](#_Toc99020883)

[Verification 5](#_Toc99020884)

[Ongoing Maintenance 5](#_Toc99020885)

[System Training 6](#_Toc99020886)

[Environment setup 6](#_Toc99020887)

[Training for existing staff 6](#_Toc99020888)

[Disruptions 6](#_Toc99020889)

Introduction

## 

## Document Scope

This plan outlines the large-scale implementation of the Splunk SIEM solution across Threat Systems Pty Ltd's head office. It covers deployment phases, resource allocation, training, and ongoing support. The goal is to ensure the solution enhances security monitoring and compliance across the organization's IT infrastructure.

## 

## Project Methodology

The Agile methodology will be used for this project. Agile's iterative approach will allow for continuous feedback, flexibility, and adjustments based on Threat Systems' needs. Regular reviews and adaptations will ensure the project remains on track.

## 

## Change management

**Human Resources and Change Management Needs**  
Effective communication with stakeholders and staff is key to successful change management. This includes:

* Conducting workshops and training sessions.
* Ensuring transparency in the project's objectives and benefits.
* Providing support for staff during the transition to the new system.
* Updating policies, particularly those related to system access and security.

# Solution Design

## 

## Project Phases

**Phase 1: Initial Setup**

* Install and configure Splunk SIEM on select PCs (completed during the proof of concept).
* Allocate necessary hardware and software resources.

**Phase 2: System Deployment**

* Roll out Splunk SIEM across the entire head office, ensuring all devices are covered.
* Conduct vulnerability scans and fine-tune security settings.

**Phase 3: Employee Training**

* Conduct training sessions for IT staff and end-users on the new system.
* Provide documentation and hands-on workshops.

**Phase 4: Testing and Verification**

* Run comprehensive tests to ensure all systems are functioning correctly.
* Validate that security events are detected and reported accurately.

**Phase 5: Final Implementation and Handover**

* Finalize the rollout and transition to ongoing support.
* Document the implementation process and prepare for future expansions.

## Milestones

**Week 1-2**: Complete system configuration and deployment across initial devices.

**Week 3**: Conduct organization-wide vulnerability scans and address issues.

**Week 4-5**: Finalize proof of concept and demonstrate to stakeholders.

**Week 6-7**: Conduct staff training and prepare final documentation.

**Week 8**: Full deployment and handover.

## Resources

**Hardware**: Existing Surface Pro devices, PCs, network photocopiers, file server, domain controller, and network storage drives.

**Software**: Splunk SIEM, Qualys for vulnerability scanning, VMware for virtual environments, Wireshark for traffic analysis.

**Human Resources**: IT Support, Security Analysts, Trainers, Documentation Specialists.

## 

## Verification

**Ensuring Goals are Met**  
Verification will be achieved through:

* Regular monitoring of Splunk logs to confirm correct data capture.
* Vulnerability assessments to ensure no security gaps remain.
* Employee feedback and surveys post-training to gauge their understanding and comfort with the new system.

## Ongoing Maintenance

**Support and Maintenance Plan**

* Regular software updates for Splunk SIEM and vulnerability scanning tools.
* Routine training refreshers for IT staff.
* Periodic reviews of the security posture and adjustments to the SIEM tool configuration.
* Backup procedures for data integrity.

# System Training

## 

## Environment setup

Training will be conducted using virtual machines for simulation and practice. Resources required include:

* **Hardware**: PCs, Surface Pro devices.
* **Software**: Splunk SIEM, virtual environments, training modules.
* **Human Resources**: Trainers, IT Support.

## Training for existing staff

Staff will undergo structured training programs, including hands-on workshops and instructional materials. Records of participation and proficiency tests will be kept. New policies regarding system usage and security will also be implemented.

## 

## Disruptions

**Minimizing Disruptions**  
To ensure minimal disruption, the deployment will be phased and conducted during off-peak hours where possible. Contingency plans for unplanned disruptions include:

* Backup systems and procedures.
* Designated support personnel on standby during and after deployment.