2

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
|  | | | | |
|  | Project Plan  Threat systems Pty Lltd  ``````````````````````````````````````````````````` |  |  |  |

## Table of Contents

[Table of Contents 3](#_Toc97379332)

[1 Introduction 4](#_Toc97379333)

[Project Name 4](#_Toc97379334)

[Project Description 4](#_Toc97379335)

[Projected Time 4](#_Toc97379336)

[Stakeholders 4](#_Toc97379337)

[Project Team 4](#_Toc97379338)

[Project Deliverables 4](#_Toc97379339)

[2 Project Management 5](#_Toc97379340)

[Management Objectives 5](#_Toc97379341)

[Project Controls 5](#_Toc97379342)

[Technical Processes 5](#_Toc97379343)

[Risk Management 5](#_Toc97379344)

[3 Project Timeline 6](#_Toc97379345)

[Gantt chart 6](#_Toc97379346)

[Activity List 6](#_Toc97379347)

[Milestones 6](#_Toc97379348)

[Resources 6](#_Toc97379349)

[4 Costs 7](#_Toc97379350)

# 1 Introduction

## Project Name

Threat Systems Pty Ltd - Cyber Solution

## Project Description and Key Components

IT security monitoring solution for Threat Systems Pty Ltd, Cyber analysis, Testing on Virtual Machines provided by client and planning and implementation of the solution. Reviewing of existing policies and potentially updating these.

## Projected Time

8 weeks based on VU23220 deadline.

## Stakeholders

**Internal Stakeholders:**

* **James G (Project Manager):** Oversees the project, manages resources, coordinates tasks, and ensures that timelines and objectives are met. Also responsible for communication with the client and team.
* **Damien W (Security Analyst):** Responsible for configuring and monitoring the SIEM tool and analysing security logs.
* **Daniel B (IT Support Specialist):** Assists with setting up virtual machines, installing necessary software, and providing ongoing technical support.
* **John Samami (Network Engineer):** Ensures network configurations are correctly set up and supports data collection and traffic analysis.
* **Peter N (Vulnerability Analyst):** Conducts vulnerability scans, analyses results, and provides recommendations for mitigating security gaps.
* **Kubashen N (Documentation Specialist):** Manages project documentation, compiles reports, and prepares presentations for the client.

**2. External Stakeholders:**

* **Threat Systems Pty Ltd Management:** The client, particularly those managing the IT service team, will evaluate the success of the proof-of-concept and its potential for full implementation.
* **IT Service Team at Threat Systems:** The internal team that is overwhelmed and will benefit directly from a successful SIEM implementation.
* **End-users of Threat Systems:** Staff and management using the IT systems whose productivity is currently impacted by the existing IT challenges.
* **Third-party Managed Service Provider (potential future role):** This is the role we will potentially take on if the proof of concept is successful, making this stakeholder role important for future considerations.

## Project Team

|  |  |  |  |
| --- | --- | --- | --- |
| Name: | Role in team: | Responsible for: | Reports to: |
| James | Project Manager | Overall project management resource allocation, stakeholder communication, and problem-solving | Executive Management |
| Damien | Security Analyst | SIEM tool management(Splunk), threat analyst, log management, and cybersecurity incident identification | James G |
| John | Network Engineer | Network configuration, data traffic analysis, and network troubleshooting | James G |
| Daniel | IT Specialist | Virtual machine setup, software installation, system configuration, and technical support | James G |
| Peter | Vulnerability Analyst | Vulnerability scanning, security assessments, gap analysis, and mitigation strategies | James G |
| Kubashen | Documentation Specialist | Technical writing, documentation management, report compilation, and presentation preparation | James G |

## Project Deliverables

**Proof of Concept:**

**Splunk SIEM Deployment:** Install and configure Splunk on two virtual machines to monitor and analyse system data and network traffic. Ensure that the SIEM tool effectively detects and logs security events.

**Vulnerability Scan Report:** Conduct vulnerability scans using Qualys or another tool, analyse the results, and provide a detailed report. The report will highlight identified security gaps, potential risks, and recommendations for remediation.

**Employee Training:** Develop and deliver training sessions for key employees on how to use the Splunk SIEM tool effectively. This includes creating training materials, conducting workshops, and ensuring that staff are proficient in monitoring and responding to security events.

**Long-term Milestones:**

**Implementation Plan for Full Deployment:** Create a comprehensive plan for rolling out the SIEM solution across the entire head office. This plan will include a step-by-step guide for deployment, resource allocation, timeline, and a detailed Gantt chart outlining key phases and milestones.

**Recommendations for Future Expansions**: Provide strategic recommendations for scaling the SIEM solution as the company grows. This will cover potential expansions to other offices, integration with additional security tools, and upgrades to the IT infrastructure to support the increased data load and security requirements.

# Project Management

## Management Objectives

Assumptions

* Theres a number of Stakeholders involved.  
  It’s a project which is going to take 8 weeks including testing
* Splunk and Virtual machines provided by the client
* We will require access to the clients network  
  Access to necessary hardware
* No changes to be implemented whilst this project is undertaken  
  Full co-operation and access to their systems
* Not IT savvy

Constraints

**1. Time Constraints:**

* **Proof of Concept (PoC):** The PoC must be completed by session 9/10, with the final implementation plan expected by week 16/17

**2. Budget Constraints:**

* **Adherence to Budget:** The project must adhere to any budget constraints set by Threat Systems Pty Ltd, limiting the resources and potential solutions that can be deployed

**3. Technical Constraints:**

* **System Compatibility:** Ensuring that the SIEM tool (Splunk) and any other software used are compatible with the existing IT infrastructure of Threat Systems Pty Ltd
* **Performance Impact:** The SIEM solution must not negatively impact the performance of the existing systems, requiring careful planning and optimisation

**4. Resource Constraints:**

* **Limited IT Resources:** The current IT team at Threat Systems is already at capacity, so the solution must be low-maintenance and should not add additional strain on the team **5.**

**5. Compliance Constraints:**

* **Compliance Standards:** The project must meet Essential 8 Maturity Level 1 compliance standards in the short term and plan for ISO 27001 compliance within 36 months

**6. Proof of Concept Limitations:**

* **Scope of PoC:** The PoC is limited to deploying Splunk on two virtual machines provided by Threat Systems, which might not fully represent the scale or complexity of a full deployment
* **Virtual Environment:** The demonstration will be conducted in a virtualised environment, which may not capture all the nuances of a real-world deployment.

## Project Controls

Monitoring Procedures

To ensure the project deliverables stay on track, we will use project management software like Trello to organise tasks, milestones, and deadlines. A Gantt chart will provide a visual timeline, helping us monitor progress and adjust as needed. We’ll also maintain a milestone checklist and set up automated reminders for upcoming deadlines.

Weekly progress meetings will be held to review completed tasks, address roadblocks, and plan for the coming week. After each meeting, a concise progress report will be shared with stakeholders. To manage risks, a risk register will be maintained and reviewed regularly, ensuring mitigation strategies are in place.

Quality assurance will involve peer reviews and testing after each milestone to ensure deliverables meet required standards. Any changes to the project scope or timelines will be managed through a formal change control process, with a change log tracking all modifications.

Communication will be streamlined through designated channels like Microsoft Teams, with regular updates and reports provided at key milestones. All project documentation will be stored in a centralised, easily accessible repository to keep track of changes.

Finally, performance metrics and KPIs will be tracked using the project management software, providing a real-time overview of the project’s status and ensuring it remains on course.

## Technical Processes

Agile, for this project

Involves stakeholders, regular feedback from them, flexibility to adapt to changes, incremental approach

Software/Hardware

**Project Management Software**

Trello or Jira: For tracking tasks, milestones, and team performance.

Microsoft Teams or Slack: For team communication and collaboration. Essential for real-time communication, file sharing, and project updates.

**Security Information and Event Management (SIEM)**

Splunk SIEM: The core tool for gathering, analysing, and visualising system data and network traffic. Splunk will also be used for setting up alerts and generating reports on security events.

**Scanning and Penetration Testing Tools**

Qualys: Our vulnerability scanning tool to identify security gaps in the system. This tool will be used to conduct a basic vulnerability assessment as part of the Proof of Concept.

Kali Linux: For penetration testing and security auditing, to identify and exploit vulnerabilities in the virtual environment.

**Virtual Machines**

VMware or VirtualBox: Virtualization software to create and manage the virtual machines (VMs) used for our Proof of Concept. Two VMs will be provided by Threat Systems, and these will host the Splunk SIEM, data collection, and vulnerability scanning processes.

Virtual Machines Configuration: One VM will act as the client, another as the attacker, and the third as the monitor for the attack. This setup is crucial for testing the SIEM tool's effectiveness in a controlled environment.

**Network Monitoring and Traffic Analysis**

Wireshark: A network protocol analyser used to capture and interactively browse the traffic running on a computer network. It will be essential for analysing network traffic and ensuring that data collection is accurate.

Network Switches and Routers: Necessary for managing and analysing network traffic between the virtual machines and the rest of the IT infrastructure.

**Data Backup and Recovery**

Backup and Recovery Software: To ensure data integrity and availability during the project, a reliable backup solution is necessary. This software will help in backing up configuration files, logs, and other critical data.

External Hard Drives or NAS: For storing backups and ensuring that data is available for recovery in case of any issues.

## Risk Management

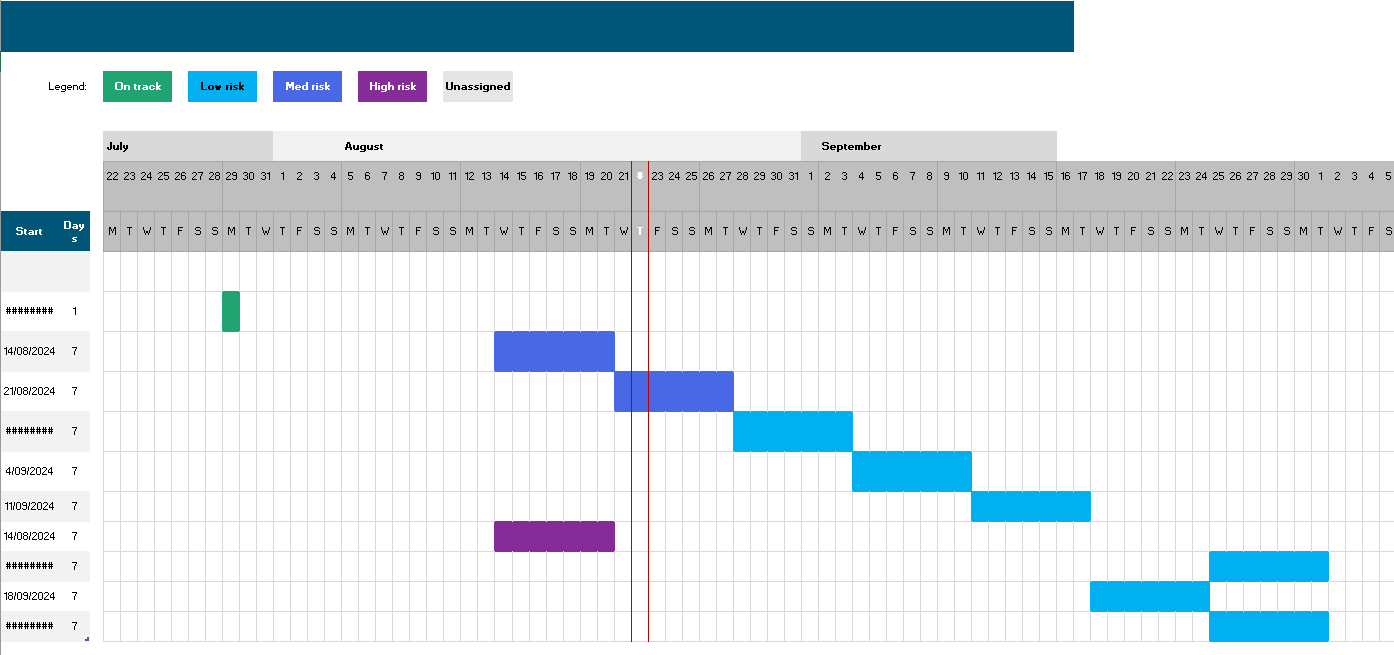
This project has an internal policy on risk management which include 3 possible responses, these include:

* Avoid the risk, in which we take every possible step to avoid the risk altogether.
* Mitigate the risk, in which we take actions to lessen the impact or chance of the risk occurring. If the risk relates to availability of resources, we then must draw up a new agreement.
* Accept the risk, should the risk be so small the effort to do anything or has very minimal impact then we will accept the risk as our own.

|  |  |  |  |
| --- | --- | --- | --- |
| **Risk** | **Probability** | **Impact** | **Controls** |
| Splunk error | medium | High | Pre testing config setup before milestone |
| Tech issues including Vmware issues | medium | High | As above |
| Non co-operation from stakeholders or IT | low | low | Clear communication early between stakeholders and IT |
| Data access issues | medium | medium | Ensuring necessary permissions in advance |
| Time management/Deadlines | low | medium | Planning and Reviewing |

# Project Implementation

## Gantt chart



## Activity List

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| **TASK NO** | **TASK NAME** | **DURATION** | **RESOURCE** | **PREDECESSORS** |
| 1 | Creating and setting up Splunk | 1 week |  | 0 |
| 2 | VM Setup | 1 week |  | 1 |
| 3 | Vulnerability scan | 1 week |  | 2 |
| 4 | Scan report | 1 week |  | 3 |
| 5 | Proof of concept demo | 1 week |  | 4 |
| 6 | Implementation plan for deployment | 1 week |  | 1/0 |
| 7 | Documentation | 1 week |  | 6 |
| 8 | Training | 1 week |  | 5 |
| 9 | Final report | 1 week |  | 6 |
| 10 | Insert more as required…. |  |  |  |

## Milestones

What are the key points in your timeline? Both proof of concept and large-scale implementation.

Week 1-2 setup and config of Splunk SIEM

Week 3 conduct vulnerability scan and analyse results

Week 4-5 prepare proof of concept and demonstration

Week 6 -7 Develop full implementation plan

Week 8- 10 Training documentation preparation

## Resources

Software and Hardware has being outlined already above

**Human Resources**

**Defined roles and responsibilities**

**Interconnecting virtual images**

Virtual machines for testing and deploying

**Intrusion Detection/Prevention Systems (IDS/IPS) systems**

Systems to monitor and prevent unauthorised access

**Security information and event management (SIEM) Tool**

Splunk for analysing and monitoring security events

**End Point Protection (EPP)**

Tools for protecting devices from threats

**Wireshark**

Software for analysing the network

**Configuring firewalls**

Setting up incoming and outgoing network traffic

**Introductory red and blue teaming exercises**

Simulated attacks and defense to improve security

**Models of Cyber Security for an organisation**

Frameworks and strategies to protect IT infrastructure, NIST, CIS etc.

**Components of a Cyber Security Operation Centre (CSOC)**

Centralised unit for monitoring and managing security

# Costs

Proof of Concept(POC) Costs

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| **Name/Resource** | **Description** | **Time/Qty** | **Unit Price** | **Total Cost** |
| **Splunk SIEM License** | Software for monitoring (trial) | 1 x License | $2,000 | $2,000 |
| **VM Licenses** | Virtual Machines for Testing (trial) | 2 x Licenses | $750 | $1,500 |
| **Project Management License** | Software for task/project management | 6 users | $10/user | $60 |
| **Personnel Costs (POC)** | Splunk Engineer, Network Engineer, etc. | 240 hours total | Varies | $7,400 |
| **Training Material** | Manuals, guides for 20 users | 20 users | $50 | $1,000 |
| **Nessus Pro** | Vulnerability scanner for testing (trial) | Trial version | $1,000 | $1,000 |
| **Data Storage** | Temporary storage for POC logs and data | Cloud storage (POC) | $1,500 | $1,500 |
| **Contingency (10%)** | To cover unexpected expenses | - | - | **$1,546** |
| **Total POC Costs** |  |  |  | **$17,006** |

**Large-Scale Deployment Costs**

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| **Name/Resource** | **Description** | **Time/Qty** | **Unit Price** | **Total Cost** |
| **Splunk SIEM License** | **Full software deployment** | **1 x License** | **$4,000** | **$4,000** |
| **VM Licenses** | **Virtual Machines for Deployment** | **10 x Licenses** | **$1,500** | **$15,000** |
| **Project Management License** | **Software for task/project management** | **6 users** | **$10/user** | **$60** |
| **Personnel Costs (Large-Scale)** | **Splunk Engineer, Network Engineer, etc.** | **400 hours total** | **Varies** | **$12,300** |
| **Training Material** | **Manuals, guides for 100 users** | **100 users** | **$50** | **$5,000** |
| **Nessus Pro** | **Full version for vulnerability scanning (yearly license)** | **1 x License** | **$7,500** | **$7,500** |
| **Maintenance & Support** | **Ongoing support contracts for Splunk SIEM** | **3 months** | **$1,500/month** | **$4,500** |
| **Licensing & Subscription Renewals** | **Annual renewal for Splunk SIEM and other tools** | **1 year** | **$3,000** | **$3,000** |
| **Data Storage** | **Additional storage for large-scale deployment logs and data** | **Cloud storage (Yearly)** | **$3,000** | **$3,000** |
| **Post-Deployment Training** | **Additional training sessions for all staff** | **100 users** | **$2,000** | **$2,000** |
| **Compliance and Auditing Costs** | **External audits for ISO 27001 compliance** | **1 audit** | **$8,000** | **$8,000** |
| **Integration Costs** | **Integration with other security tools** | **1 project** | **$4,000** | **$4,000** |
| **Network Infrastructure Upgrades** | **Upgrading network hardware to support SIEM deployment** | **1 upgrade project** | **$5,000** | **$5,000** |
| **Contingency (10%)** | **To cover unexpected expenses** | **-** | **-** | **$4,386** |
| **Total Large-Scale Costs** |  |  |  | **$48,246** |

The costs were drafted considering both the immediate needs for the proof of concept and the larger-scale implementation. The primary expenses include the licensing fees for the Splunk SIEM software and virtual machine licenses, which are essential for the cybersecurity solution's setup and testing. Personnel wages are calculated based on the estimated 400 hours required to complete the project, including setup, testing, and documentation. Training materials are budgeted for 100 end-users to ensure comprehensive onboarding. The project management software is also considered, with a license cost for six users, allowing efficient task management throughout the project. These costs account for the initial setup and provide a foundation for scaling up the solution across the organization, ensuring long-term viability and effectiveness.

Additionally, a 10% contingency fund has been incorporated into the budget to cover any unforeseen expenses that may arise during the project. This ensures that the project remains on track financially, even in the face of unexpected challenges. The costs outlined provide not only for the initial setup and proof of concept but also establish a robust foundation for scaling the solution across the organization. This approach supports long-term viability and effectiveness, with flexibility to adapt as the project evolves.