|  |
| --- |
| Project POSTMORTEM |
| Threat Systems PTY LTD Cyber Solution  John Samami  James G  Damien W  Daniel B  Kubashen N  Peter N |



Table of Contents

[Group Name 1](#_Toc97384652)

[Introduction 4](#_Toc97384653)

[Background to the project 4](#_Toc97384654)

[Operational Review 4](#_Toc97384655)

[Lessons learned 4](#_Toc97384656)

[Project Management Issues 5](#_Toc97384657)

[What processes were most effective? 5](#_Toc97384658)

[What processes were least effective? 5](#_Toc97384659)

# Introduction

## Background to the project

This project aimed to design and implement a comprehensive cybersecurity solution for Threat Systems Pty Ltd, with a focus on deploying a Splunk SIEM (Security Information and Event Management) tool. The solution was designed to enable real-time monitoring, analysis, and protection of the company's IT infrastructure. The project was divided into two phases: a Proof of Concept (PoC) and a plan for full-scale deployment. The primary objectives were to identify and address security vulnerabilities, enhance compliance with Essential 8 and ISO 27001 standards, and improve the efficiency of the company’s overburdened IT team.

**Project Achievements:** Key accomplishments of the project include:

* **Proof of Concept (PoC) for Splunk SIEM:** Successfully configured and tested Splunk on two virtual machines to demonstrate its capabilities.
* **Vulnerability Assessment:** Performed thorough vulnerability scans, identifying critical security gaps and providing actionable mitigation strategies.
* **Training Delivery:** Delivered training sessions to key personnel on using the Splunk tool for effective monitoring and incident response.
* **Implementation Plan:** Developed a detailed plan for the full-scale deployment of Splunk at Threat Systems' head office, along with strategic recommendations for future expansion.

## Operational Review

**Timeframes:** The project was successfully completed within the planned 8-week schedule, covering both the Proof of Concept (PoC) and the development of the full-scale deployment plan. Weekly milestones were met, although minor delays occurred during configuration and testing due to system compatibility issues.

**Scope:** The project adhered closely to the original scope, focusing on the deployment of Splunk on two virtual machines, conducting vulnerability scans, and providing employee training. There was a slight expansion in scope after identifying critical vulnerabilities during testing, leading to the inclusion of additional security measures.

**Cost:** The project was initially underquoted significantly, but this was addressed, and the project remained within the revised budget. Contingency funds were used to cover unforeseen expenses, such as extra network hardware and a software license upgrade. Additionally, there was a slight increase in personnel costs due to overtime required during the testing and training phases.

**Quality Expectations:** All deliverables met or exceeded the expected quality standards. The SIEM system demonstrated high accuracy in detecting security events. The vulnerability assessment identified several significant risks, all of which were addressed in the final report. Employee training was well-received, with participants gaining confidence in using the Splunk tool.

## Lessons learned

**Communication is Key:** Clear and consistent communication between stakeholders, especially the internal IT team, was essential for smooth collaboration. In the future, more detailed kickoff meetings with client IT staff should be scheduled to avoid minor delays, such as those caused by permission issues.

**Testing Should Start Early:** One key takeaway was the importance of initiating testing phases earlier. While the PoC was ultimately successful, delays due to technical issues (e.g., misconfigured virtual machines) could have been reduced by involving network engineers sooner in the process.

**Resource Allocation:** We initially underquoted the project costs, primarily because we underestimated the need for specialized personnel, such as Splunk engineers and network engineers. This oversight led to higher expenses than originally planned. Additional costs were incurred for network hardware and software licenses, which were not fully anticipated. In future projects, a more thorough assessment of required specialized skills and their associated costs will be essential for accurate budgeting. Additionally, we underestimated the level of hands-on support required for configuring and integrating Splunk. Allocating more time and resources for these specialized tasks will help ensure smoother deployment and better coordination with the client’s IT team.

**Agile Flexibility is Crucial:** Agile project management proved effective for adapting to changes in real-time, such as adding additional security measures during testing. For future projects, adopting a more Agile approach from the outset could improve flexibility and responsiveness to evolving requirements.

Project Management Issues

## What processes were most effective?

**Agile Methodology:** This approach enabled continuous feedback and iterative improvements. Regular stand-up meetings and sprint reviews allowed the team to quickly adapt to challenges as they arose.

**Risk Management:** The team’s proactive use of a risk register and frequent risk reviews helped prevent significant delays. For example, early testing of the Splunk configuration identified potential issues, allowing the team to resolve them ahead of deployment.

**Microsoft Teams for Collaboration:** Microsoft Teams proved to be an effective tool for communication and collaboration. It enabled seamless coordination between team members, ensuring everyone stayed informed and aligned with project goals.

## What processes were least effective?

**Initial Time Allocation for Network Configuration:** The initial estimates for network and virtual machine configuration were too optimistic. More thorough technical preparation and consideration of potential configuration issues should be factored into future project plans.

**Documentation Process:** The documentation phase took longer than anticipated because the Documentation Specialist was not involved early enough. In future projects, involving documentation personnel earlier will ensure smoother knowledge transfer and more efficient record-keeping.

**Client Feedback Delays:** Delays were encountered due to the need for resubmissions after initial documents and approvals were deemed unacceptable by the client. To address this in future projects, ensuring thorough reviews and validation of submissions before presenting them to the client can help reduce the likelihood of rejections and speed up the feedback process.