|  |  |  |  |  |
| --- | --- | --- | --- | --- |
|  | | | | |
|  | Testing & Verification Plan Thread Systems PTY LTD  John Samami  James G  Damien W  Daniel B  Kubashen N  Peter N |  |  |  |

## Table of Contents

[Table of Contents 3](#_Toc98779685)

[Introduction 4](#_Toc98779686)

[Document Scope 4](#_Toc98779687)

[System Overview 4](#_Toc98779688)

[System Feedback 4](#_Toc98779689)

[System Changes 4](#_Toc98779690)

[General Testing Procedures 5](#_Toc98779691)

[Testing Deliverables 5](#_Toc98779692)

[Testing Environment 5](#_Toc98779693)

[Systems Test plan 5](#_Toc98779694)

# Introduction

## 

## Document Scope

The goal of this testing and verification plan is to confirm that the SIEM solution implementation for Threat Systems Pty Ltd satisfies both functional and non-functional requirements.

This plan will specifically evaluate the SIEM solution’s capacity to effectively monitor, log, and alert on security incidents within the head office’s IT infrastructure.

## System Overview

The testing methodology for this project involves both manual and automated testing of the SIEM system's ability to collect, process, and analyze data from various IT assets within the Threat Systems Pty Ltd network.

The SIEM solution, using Splunk, will be deployed on two virtual machines (VMs) to gather system data and network traffic, which will be tested for accuracy, completeness, and performance.

## System Feedback

Feedback from the client indicated that the initial design of the SIEM solution was solid, but there were concerns regarding the scalability and the ability to integrate with existing IT infrastructure.

The client also requested more thorough testing on how well the system handles large volumes of data and whether it can support real-time monitoring.

Additions and Highlighting of the Security of our proposed solution due to feedback and concerns from client.

## 

## System Changes

Based on the feedback, the following changes were made:

* Enhanced data processing capabilities within the SIEM system to handle larger data volumes.
* Additional integration points were added to allow for better interaction with the existing IT infrastructure.
* Real-time monitoring capabilities were improved to ensure timely detection and reporting of security events.
* Splunk now ingests sign-in logs and email logs to detect excessive declines and phishing emails, respectively.
* Password requirements were implemented.
* 8 Characters in length minimum
* Uppercase, lowercase, numbers, and characters required
* No password reset needed unless password is compromised.
* Roles with different permissions set up that can be modified as per the clients' requirements.

# General Testing Procedures

## 

## Testing Deliverables

The deliverables for this project will include:

* A fully configured and operational Splunk instance on two VMs.
* Test logs and reports demonstrating the successful detection, logging, and alerting of security events.
* Documentation detailing the setup, configuration, and testing procedures for the SIEM system.

## Testing Environment

The testing environment consists of two virtual machines configured with the Splunk SIEM solution. These VMs simulate the IT environment at Threat Systems Pty Ltd and will be used to capture system data and network traffic from various IT assets.

## Automated testing

Automated testing will be conducted using Splunk’s built-in testing and monitoring tools.

The software will be used to continuously monitor the flow of data and system performance, ensuring that the SIEM solution remains responsive and effective under varying conditions.

# Systems Test plan

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| ID | Module/Section | Test | Expected Result | Actual Result |
| 1 | Virtualisation | 2 interconnected devices have been setup and are sending data to a monitoring instance | Monitoring instance receives data from devices and logs information as per specification | Working as expected |
| 2 | Data Collection | Verify that Splunk correctly collects and logs data from the Surface Pro 6 devices used by management staff | All logs are accurately recorded and stored |  |
| 3 | Data Processing | Test Splunk's ability to handle large volumes of data from the 44 desktop PCs | Data is processed without loss or delay |  |
| 4 | Real-time Monitoring | Ensure that real-time alerts are triggered for any suspicious activity detected by Splunk | Alerts are sent immediately upon detection |  |
| 5 | Integration | Check the integration of Splunk with the file server and network storage drives | Successful integration with no data loss |  |
| 6 | Security Event Detection | Test Splunk's ability to detect specific security events (e.g., unauthorized access attempts) | Events are detected and logged as expected |  |
| 7 | Data Reporting | Verify that Splunk generates accurate and timely reports based on collected data | Reports match the data logs and are delivered on schedule |  |
| 8 | System Performance | Assess the performance of the SIEM system under peak load conditions | System remains stable and responsive |  |
| 9 | User Access Control | Test user access control policies within the Splunk system | Only authorized users can access and modify SIEM settings |  |
| 10 | System Scalability | Evaluate the scalability of the SIEM solution to handle future expansions | System can be scaled up without significant reconfiguration |  |
| 11 | Backup &  Recovery | Verify the system's ability to back up and recover data without loss. | Data is fully recoverable from backups without any corruption. |  |
| 12 | Latency Test | Measure the response time of the system under various loads. | System maintains acceptable response times under different loads |  |
| 13 | Failover Testing | Simulate a system failure and ensure the failover system activates properly. | The system should seamlessly switch to a backup without data loss |  |
| 14 | Compliance Testing | Ensure the solution adheres to industry compliance standards (e.g., GDPR, HIPAA). | All compliance requirements are met without any violations. |  |
| 15 | User Experience Testing | Assess the ease of use and user interface intuitiveness. | Users should be able to navigate the system easily without extensive training. |  |
| 16 | Network Impact Testing | Evaluate the impact of the system on network bandwidth. | Minimal disruption to network performance. |  |
| 17 | Security Compliance Testing | Verify compliance with internal security policies (e.g., PCI-DSS, ISO 27001). | All security policies are adhered to without exceptions. |  |
| 18 | Data Encryption | Verify that data is encrypted both in transit and at rest. | All sensitive data should be securely encrypted. |  |
| 19 | Log Retention Testing | Ensure logs are retained as per policy. | Logs are stored for the required duration and are accessible for audits |  |
| 20 | Red and Blue Team Exercises | Conduct Red Team and Blue Team exercises. | The system should detect and respond to simulated attacks effectively |  |