Table of Contents:

1. Introduction

1.1 Problem to Solve
1.2 Goals
1.3 Scope
1.4 Research Questions and Subquestions
1.5 Research Strategies to be Used
1.6 Deliverables

2. Getting Started

2.1 System Requirements
2.2 Installation
2.3 User Roles and Permissions
2.4 Logging In

3. Dashboard

3.1 Threat Level Overview
3.2 Network Security Status
3.3 Alerts and Notifications
3.4 Real-time Threat Data

4. Data Collection and Analysis

4.1 Snort Log File Scanning
4.2 Uploading Log Files to Websnort
4.3 Sending API Calls to Websnort
4.4 Receiving Data in the Application

5. Visualization

5.1 Thermometer Visualization

6. Security Controls

6.1 Encryption and Authentication
6.2 Access Controls
6.3 Authorization and User Management

7. User Interface and Training

7.1 Intuitive and User-Friendly Design
7.2 Training and Support

8. Monitoring and Incident Response

8.1 Procedures for Monitoring
8.2 Incident Handling and Reporting

9. Feedback and Continuous Improvement

9.1 Feedback Mechanisms
9.2 Evaluation and Improvement

10. Troubleshooting
10.1 Frequently Asked Questions
10.2 Common Issues and Solutions

1.1 Problem to Solve

The Infralab Threat Thermometer is a cyber threat thermometer application designed to address the problem of visualizing current threat levels and network security status for FHICT INFRALAB. This section provides an overview of the goals and scope of the project.

1.2 Goals

The goals of the Infralab Threat Thermometer project are to provide a secure and efficient method of collecting and analyzing cyber threat data and to visualize it using a thermometer-based interface.

1.3 Scope

The scope of the project includes the development of an application that integrates with Snort, a popular intrusion detection system, to scan network logs. The log files are then uploaded to Websnort, a web-based interface for analyzing and storing log data. The Infralab Threat Thermometer application sends API calls to Websnort to retrieve the analyzed data, which is then visualized using a thermometer-based interface.

1.4 Research Questions and Subquestions

The research questions and subquestions that guided the project are outlined in this section, providing a framework for the development of the application.

Main question:

What can be done to develop an effective and secure cyber threat thermometer system to display recent threat levels and the state of FHICT INFRALAB's network security?

Sub-questions:

A. How can FHICT INFRALAB identify and categorize the major security risks and threats it faces?

B. In order to provide an accurate and effective threat assessment for FHICT INFRALAB, what critical data points and metrics must be collected and analyzed in real time?

C. How can FHICT INFRALAB's existing infrastructure be adapted to support the Infralab Threat Thermometer system?

D. In order to make the Infralab Threat Thermometer system secure and reliable, what are the key security aspects relevant to the chosen technology?

E. What encryption and authentication mechanisms should be implemented to protect the Infralab Threat Thermometer system against potential attacks and unauthorized access?

F. To ensure staff are able to effectively use and interpret the threat information provided by the Infralab Threat Thermometer system, how can the system be designed to provide an intuitive and user-friendly interface for FHICT INFRALAB staff? What training and support will be needed?

G. To detect and respond to any security incidents or breaches, what procedures should be in place to monitor and maintain the Infralab Threat Thermometer system?

H. What feedback mechanisms should be established to ensure that the Infralab Threat Thermometer system remains an accurate and effective tool for managing cybersecurity risks within FHICT INFRALAB and how can it be evaluated and continuously improved over time?

1.5 Research Strategies Used

The research strategies employed during the project include literature review, case studies, expert interviews, surveys, and iterative user-centered design approach:

- Perform a literature review to identify existing research and best practices in cybersecurity threat monitoring and management systems, as well as relevant technical and security aspects.

- Analyze case studies of similar organizations and industries to identify common cybersecurity threats and risks, as well as effective approaches to monitoring and managing threats.

- Interview cybersecurity and threat management experts to gain insight into emerging trends, best practices, and potential challenges related to the development and implementation of the Infralab Threat Thermometer.

- Conduct surveys to get feedback on staff and other stakeholders' needs and preferences regarding threat monitoring and management, as well as their level of awareness of cybersecurity risks.

- Using an iterative and user-centered design approach, develop a prototype of the Infralab Threat Thermometer system that gathers feedback from stakeholders.

- Identify areas for improvement and optimization of the Infralab Threat Thermometer system through testing and validation, and gather feedback from stakeholders.

- Develop a risk mitigation plan to address the risks associated with the Infralab Threat Thermometer system by conducting a risk assessment.

- Perform a security audit of the Infralab Threat Thermometer system to identify potential security gaps and vulnerabilities and develop recommendations for improving its security and resilience.

1.6 Deliverables

The deliverables of the project include project plan, design document, user manual, presentation, demo, and the actual software, the Cyberthreat Thermometer application.

2.Getting Started

2.1 System Requirements

Before installing and using the Infralab Threat Thermometer application, ensure that your system meets the following requirements, including hardware, software, and network specifications:
----------in work----------

2.2 Installation

This section provides step-by-step instructions for installing the application on your system, including the installation of Snort, Websnort, and the Infralab Threat Thermometer application.

----------in work----------

2.3 User Roles and Permissions

Learn about the different user roles and permissions within the application and understand the access levels and responsibilities associated with each role.

----------in work----------

2.4 Logging In

Find instructions on how to log in to the Infralab Threat Thermometer application using your credentials and navigate the user interface.
----------in work----------

3. Dashboard

3.1 Threat Level Overview

The threat level overview section provides a visual representation of the current threat levels. Learn how to interpret the threat levels and understand their implications for network security.

----------in work----------

3.2 Network Security Status

Explore the network security status section to view the current status and identify potential vulnerabilities. Learn how to interpret the security status indicators and take appropriate actions.

----------in work----------

3.3 Alerts and Notifications

Understand how the application notifies users about critical alerts and security notifications. Learn how to configure alert preferences and respond to notifications effectively.

----------in work----------

3.4 Real-time Threat Data

Discover how to access and interpret real-time threat data collected by the application. Understand the different metrics and data points provided and leverage this information for informed decision-making.

----------in work----------

4.Collection and Analysis

4.1 Snort Log File Scanning

Learn how to configure the Snort intrusion detection system to scan network logs effectively. Understand the log file format and ensure proper configuration for accurate threat detection.

----------in work----------

4.2 Uploading Log Files to Websnort

Find instructions on how to upload the scanned log files to Websnort for further analysis. Learn about the file upload process and the supported formats.

----------in work----------

4.3 Sending API Calls to Websnort

Understand how the Infralab Threat Thermometer application sends API calls to Websnort to retrieve analyzed data. Learn about the API endpoints and the required parameters.

----------in work----------

4.4 Receiving Data in the Application

Discover how the application receives and processes data retrieved from Websnort. Learn about the data structure and how it is utilized for visualization.

----------in work----------

5. Visualization

5.1 Thermometer Visualization

Learn how to interpret and navigate the thermometer-based visualization in the application. Understand the color-coding and temperature ranges used to represent threat levels effectively.

----------in work----------

6. Security Controls

6.1 Encryption and Authentication

Understand the encryption and authentication mechanisms implemented in the Infralab Threat Thermometer application. Learn how data transmission is secured and how user authentication is enforced.
----------in work----------

6.2 Access Controls

Explore the access controls implemented within the application. Learn how to manage user permissions, restrict unauthorized access, and ensure data confidentiality.

6.3 Authorization and User Management

Understand the user authorization and management features within the application. Learn how to create and manage user accounts, assign roles, and modify user settings.

7. User Interface and Training

7.1 Intuitive and User-Friendly Design

Learn about the design principles followed to provide an intuitive and user-friendly interface for FHICT INFRALAB staff. Understand the navigation, layout, and interactive elements of the application.

7.2 Training and Support

Discover the training and support resources available for FHICT INFRALAB staff. Learn how to utilize the application effectively and address any questions or issues that may arise.

8. Monitoring and Incident Response

8.1 Procedures for Monitoring

Understand the procedures in place for monitoring the Infralab Threat Thermometer application. Learn how to configure monitoring settings and receive alerts for potential security breaches.

8.2 Incident Handling and Reporting

Learn how to handle security incidents and report them appropriately within the application. Understand the incident response workflow and the steps to take when a security breach is detected.

9. Feedback and Continuous Improvement

9.1 Feedback Mechanisms

Discover the feedback mechanisms established to gather user input and improve the Infralab Threat Thermometer application. Learn how to provide feedback, suggestions, and report issues encountered.

9.2 Evaluation and Improvement

Understand how the application is evaluated and continuously improved based on user feedback and ongoing monitoring. Learn about the processes in place for implementing updates and enhancements.

10. Troubleshooting

10.1 Frequently Asked Questions

Find answers to frequently asked questions about the Infralab Threat Thermometer application. This section covers common inquiries and provides troubleshooting tips.

10.2 Common Issues and Solutions

Explore a list of common issues that users may encounter while using the application. Find step-by-step solutions to resolve these issues effectively.

11. Glossary

Refer to the glossary for definitions of key terms and concepts used throughout the user manual. This section provides clarity and ensures a common understanding of terminology.

12. Conclusion
13.

Conclude the user manual with a summary of the application's capabilities and benefits. Emphasize the importance of utilizing the Infralab Threat Thermometer to enhance network security within FHICT INFRALAB.

Note: This user manual provides a comprehensive guide to understanding and utilizing the Infralab Threat Thermometer application. It is essential to refer to this manual for accurate information and guidance during the application's installation, configuration, and usage.