Software Requirements Specification (SRS)

1. Introduction

1.1 Purpose

The purpose of this document is to define the functional and non-functional requirements of a Cyber Threat Intelligence Dashboard. This dashboard provides real-time monitoring and visualization of network threats.

1.2 Scope

The dashboard monitors live network activity, displays malware/attack types, IP addresses, blocked ports, and system logs in a dark, hacker-themed UI.

1.3 Intended Audience

Security analysts, cybersecurity students, project developers, and evaluators.

2. Overall Description

2.1 Product Perspective

A standalone dashboard using modern web or Python technologies to analyze real-time threat intelligence.

2.2 User Needs

- View threats in real-time
- Monitor logs and IP activity
- Understand threat trends

2.3 Assumptions and Dependencies

- Browser support
- Tailwind, Recharts, or Python backend
- Node.js/npm required for development

3. Functional Requirements

ID	Requirement
FR1	Display real-time threat alerts
FR2	Show active IPs and blocked ports
FR3	Maintain a log of events
FR4	Display attack types (Malware, Port Scan, etc.)
FR5	Visualize threat trends via graphs
FR6	Auto-refresh data every few seconds

FR7	Allow backend integration for live data

4. Non-Functional Requirements

ID	Requirement
NFR1	Dark hacker-style UI
NFR2	Responsive design
NFR3	Live chart updates
NFR4	Modular and extendable
NFR5	Quick loading (<3 seconds)

5. UI Design Overview

- Dark-themed interface with Tailwind (Zinc theme)
- Cards for threats, IPs, and ports
- Line chart using Recharts
- Scrollable logs
- Placeholder for user activity panel

6. Tools & Technologies

Category	Tools
Frontend	Next.js, Tailwind CSS, shadcn/ui, Recharts
Backend	Python (optional - Flask/FastAPI)
Data source	Simulated logs or packet capture
IDE	VS Code
Version Control	Git (optional)

7. Future Enhancements

- Integration with sniffers like scapy/pyshark
- User authentication system
- WebSocket support for real-time updates
- Threat severity ranking