Problem Statement 4 -Security Dashboard for Enhanced Data Protection

Problem Statement	Develop a comprehensive security dashboard with the following features to enhance data protection within the organization.
Pain Points	**Analysis and Alerting of Malicious PII Access:** Implement a real-time analysis and alerting system for detecting malicious behavior related to Personally Identifiable Information (PII) access. The system should provide immediate alerts when unauthorized access or suspicious activities are detected based on threshold. **Detailed User Behavior Report Tool:** Develop a one-click tool to download a detailed user behavior report based on reported AWB (Data Leak) cases. The tool should extract relevant information, such as user activities, data accessed, and timestamps, providing a comprehensive report for further investigation. **Dormant Users Dashboard:** Build a dashboard listing dormant users within the company. Identify users who have not been active for an extended period and present this information in an easily understandable format. This feature aids in proactive user management and security.

Problem Statement 4 -Security Dashboard for Enhanced Data Protection

Expected Solution	The expected output of the hackathon should be a fully functional Security Dashboard that integrates the specified features. This includes: > Real-time analysis and alerting module for PII access. > One-click tool for downloading detailed user behavior reports. > Dashboard listing dormant users.
Metrics to chase	**PII Access Monitoring Metrics:** Number of real-time alerts triggered. False positive/negative rates. Average response time to alerts. **System Security Posture Metrics:** Tool's download success rate. Time taken to generate a detailed report. Accuracy of extracted information. **Dormant Users Dashboard Metrics:** Number of dormant users identified. Frequency of dashboard updates.

Shiprocket

“CyberKnights”

Dec - 2023

Vinod Kumar
Aviral Singh
Vinay Somawat
Salamuddin
Richa Upadhyay
Bhupendra Rawat

Shiprocket

Security Dashboard for PII Data Monitoring

- Need to detect and Monitor suspicious activities related to Personally Identifiable Information (PII) access in real-time by providing an alert monitoring system.
- Monitor and analyze reported cases of data leaks (AWB cases) by providing a tool that can generate detailed information about AWB and PII accessed by internal Users .
- Proactively manage user accounts and enhance security by identifying dormant users who haven't been active for an extended period.

Research and Analysis

Review & Analysis:

- Explored problem statement internally and externally.
- Analyzed current PII data access within our system.

Discussions:

- Engaged with champions and cybersecurity experts.
- Gained practical insights and identified key system requirements.

Case Studies:

- Examined current PII cases and manual reporting solutions.

Insights Gained:

- Holistic problem understanding.
- Expert perspectives for informed decision-making.
- Real-world case studies informing our solution.

Solution Overview

Introducing Cyberरक्षक

Key Features:

PII Surveillance Dashboard:
- Real-time detection and monitoring functionality.
- Monitors APIs exposing Potential PII Data.

User Tracking at AWB Level:
- Tracks user activities based on AWB level PII access.
- Provides comprehensive insights into user behavior.

Alert Generation:
- Generates alerts for users accessing alarming rates of PII.
- Ensures proactive response to potential security threats.

Advantages:

- Enhanced Visibility: Real-time surveillance for PII exposure.
- User Behavior Insights: AWB level tracking for detailed user analysis.
- Proactive Security: Immediate alerts for suspicious user activities.

Cyberरक्षक

- Dashboard
- All AWB List
- Settings

Overview

This slide provides information regarding the security breached by internal users regarding PII details

Currently Active Users

0
Admin

Dormant Users

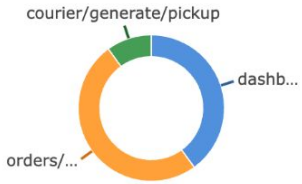
0
Not Logged In
(since last 30 days)

23
Logged In
(after 30 days)

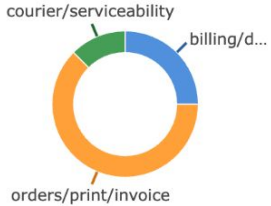
7
Viewed PII Details

Breach Severity Levels

Low



Medium



High

Screen with high PII breach

products
orders

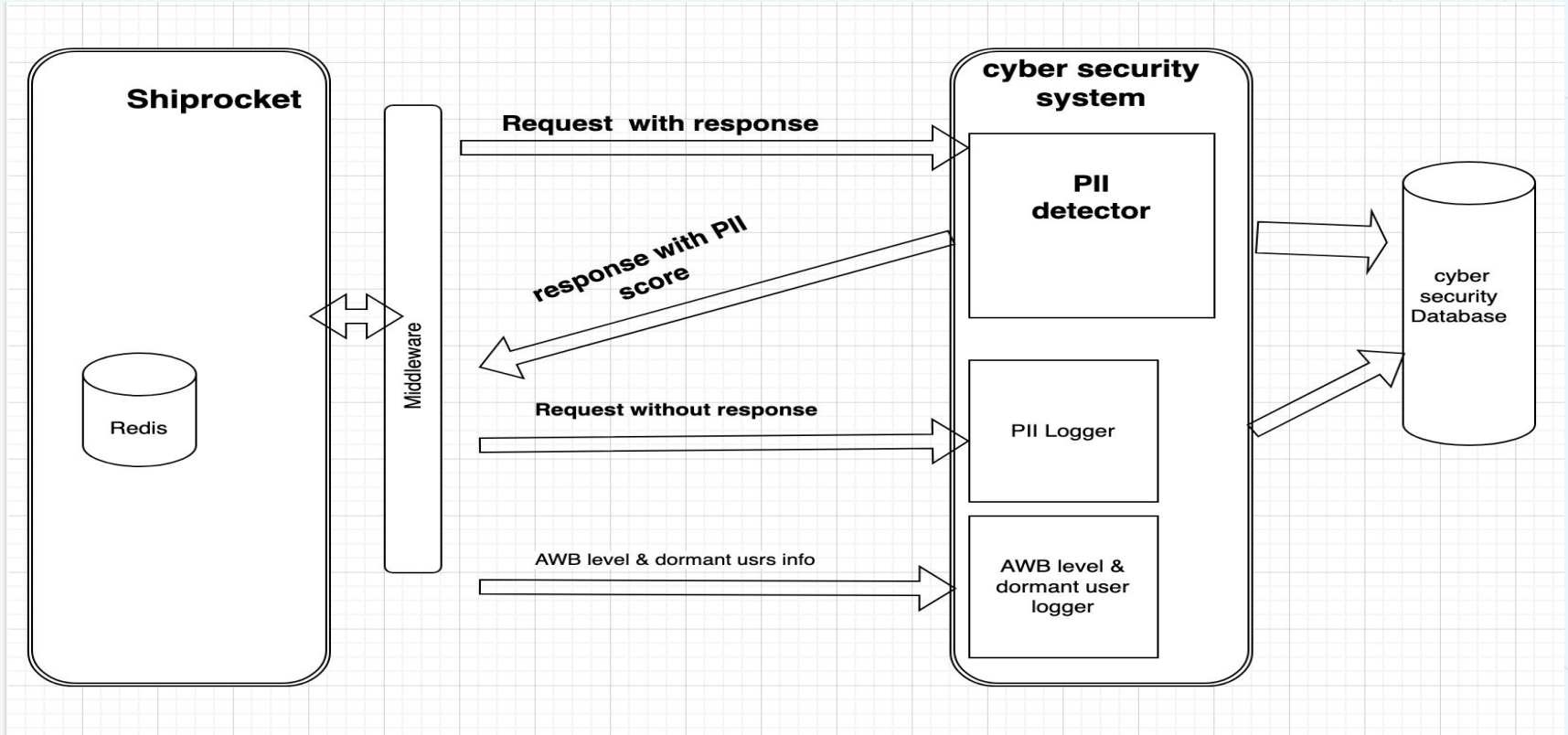
1 / 3

List of High Risk Users

PII Access by User Roles

Technical Architecture

Tech stack Front end : Angular , Backend : Laravel PHP



Business Opportunity and Future Scope

Innovation and Improvement:

Reporting and auto action if found PII breached .

Business Expansion:

Can be extended as a separate business solution to detect PII data over apis.

Enhance role based access to panel.

Shiprocket

Q&A