MICHIGAN STATE
UNIVERSITY

Project Plan Presentation

Intelligent Network Security for High-Risk Traffic

The Capstone Experience

Team McKesson

Aneesh Kapole
Dev Khakhar
Karena Lam
Aisha Latif
Divya Nadella
Conner O’Sullivan

Department of Computer Science and Engineering
Michigan State University

Fall 2025

From Students…
…to Professionals

Project Sponsor Overview

- Fortune 10 pharmaceutical distributors and healthcare IT company
- Played a role in distributing vaccines during COVID 19
- Headquarter in Irving, Texas with operations across US and internationally

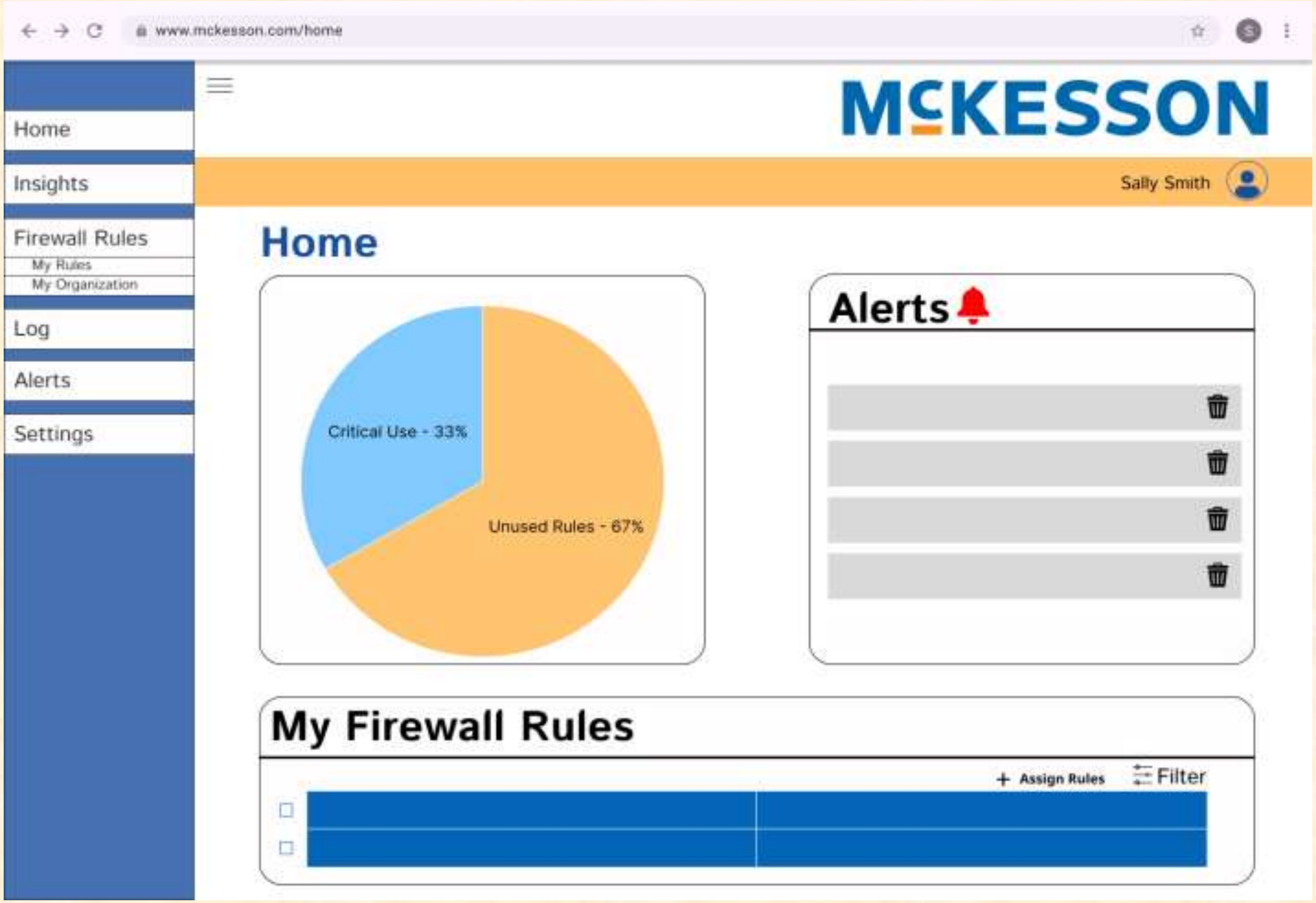
Project Functional Specifications

- Web-based application designed to centralize fire wall rule management and provide actionable insights through an intelligent risk scoring engine
- To support day-to-day decision making, the platform will include an attestation workflow, along with alerts and notifications
- Application will incorporate role based functionality aligned with Mckesson workflows

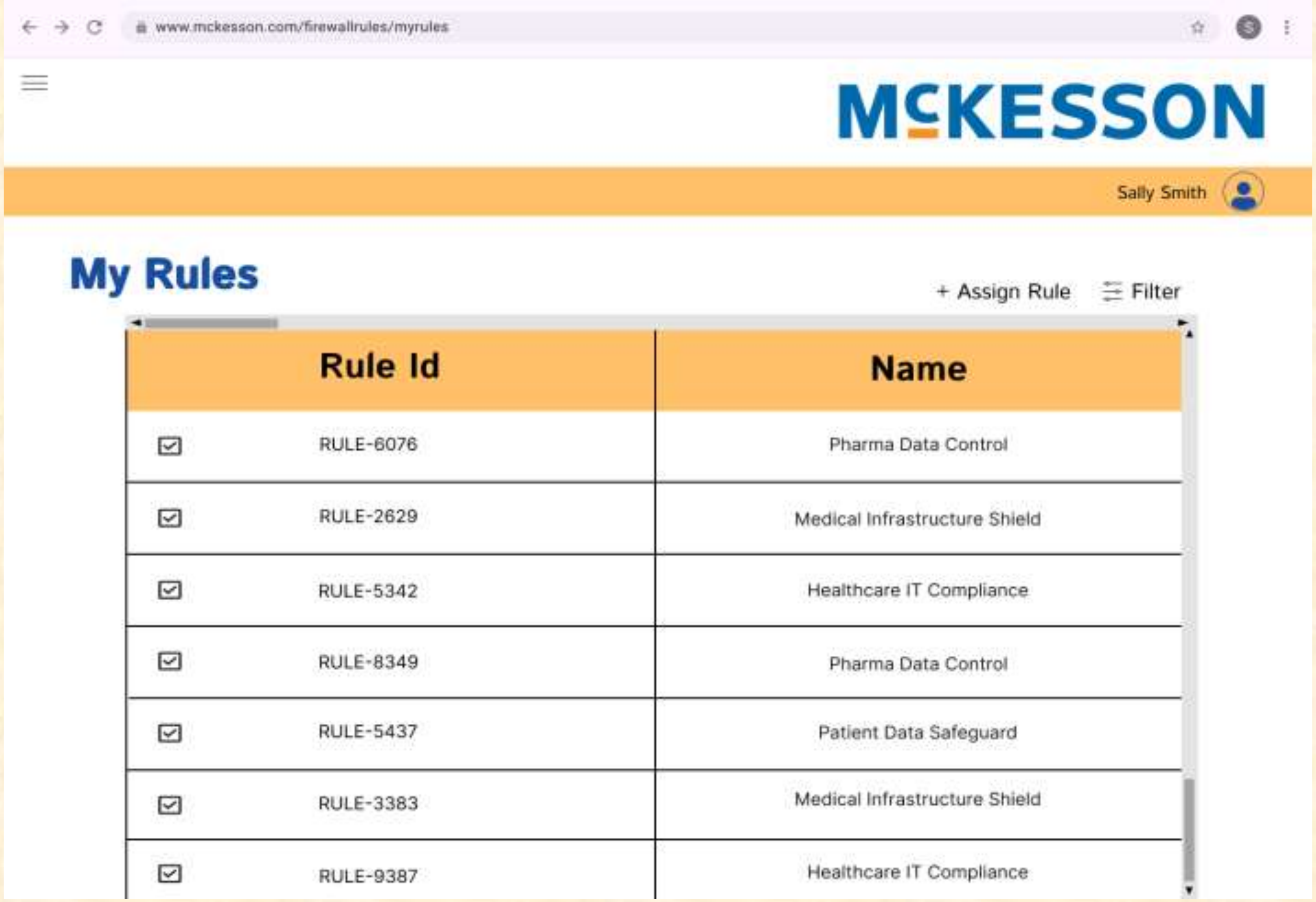
Project Design Specifications

- Home page: simplified view of dashboard, alerts, and user’s firewall rules
- Insights page: dashboards with visuals of risk scores, vulnerabilities, attestations, and unassigned rules
- My Rules page: user’s rules that depicts the rules they manage
- My Organization page: user’s subordinates’ firewall rules
- Logs page: includes all firewall logs provided by McKesson
- Alerts page: houses the history of all sent alerts

Screen Mockup: Home Page



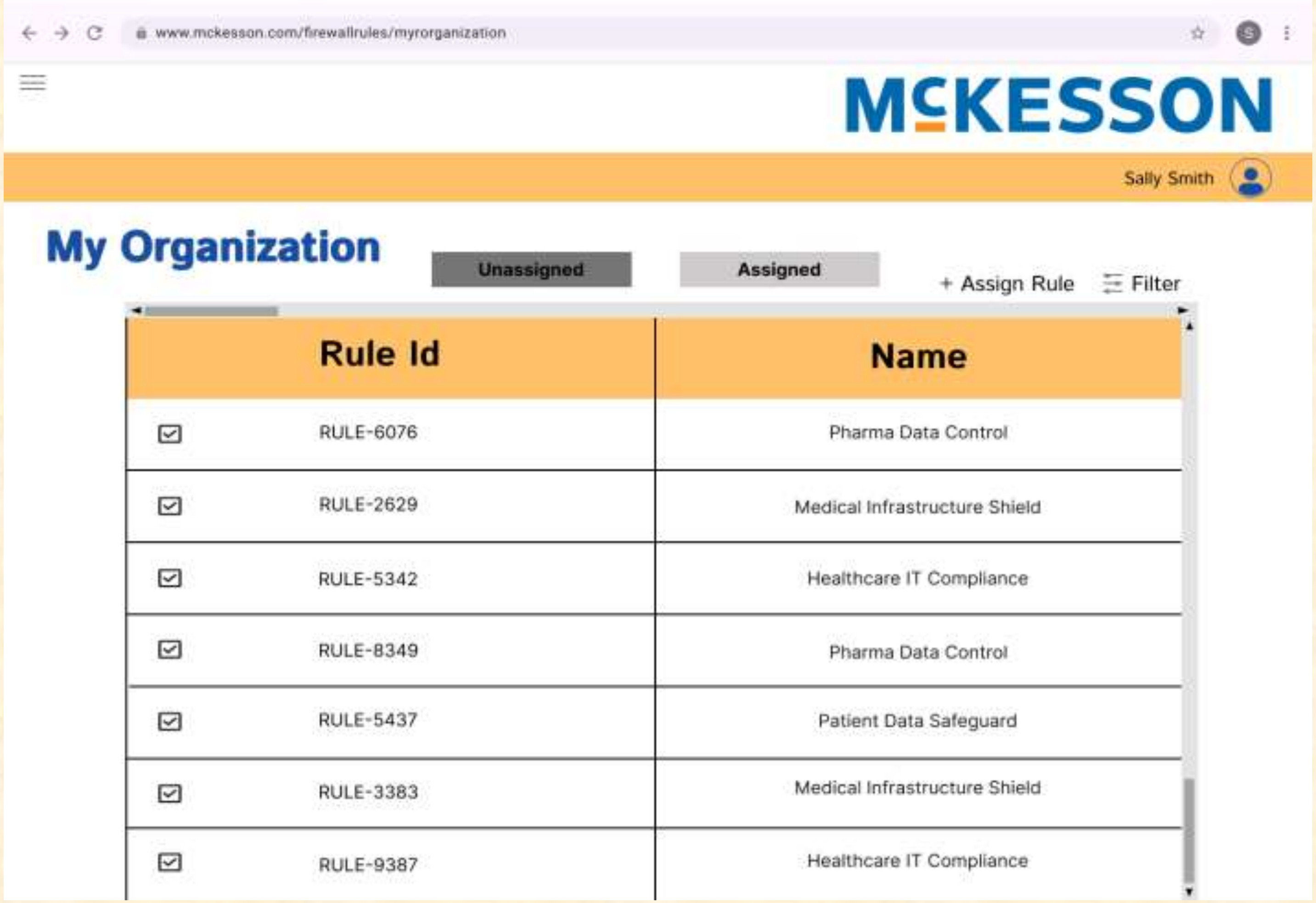
Screen Mockup: My Rules Page



My Rules

	Rule Id	Name
☑	RULE-6076	Pharma Data Control
☑	RULE-2629	Medical Infrastructure Shield
☑	RULE-5342	Healthcare IT Compliance
☑	RULE-8349	Pharma Data Control
☑	RULE-5437	Patient Data Safeguard
☑	RULE-3383	Medical Infrastructure Shield
☑	RULE-9387	Healthcare IT Compliance

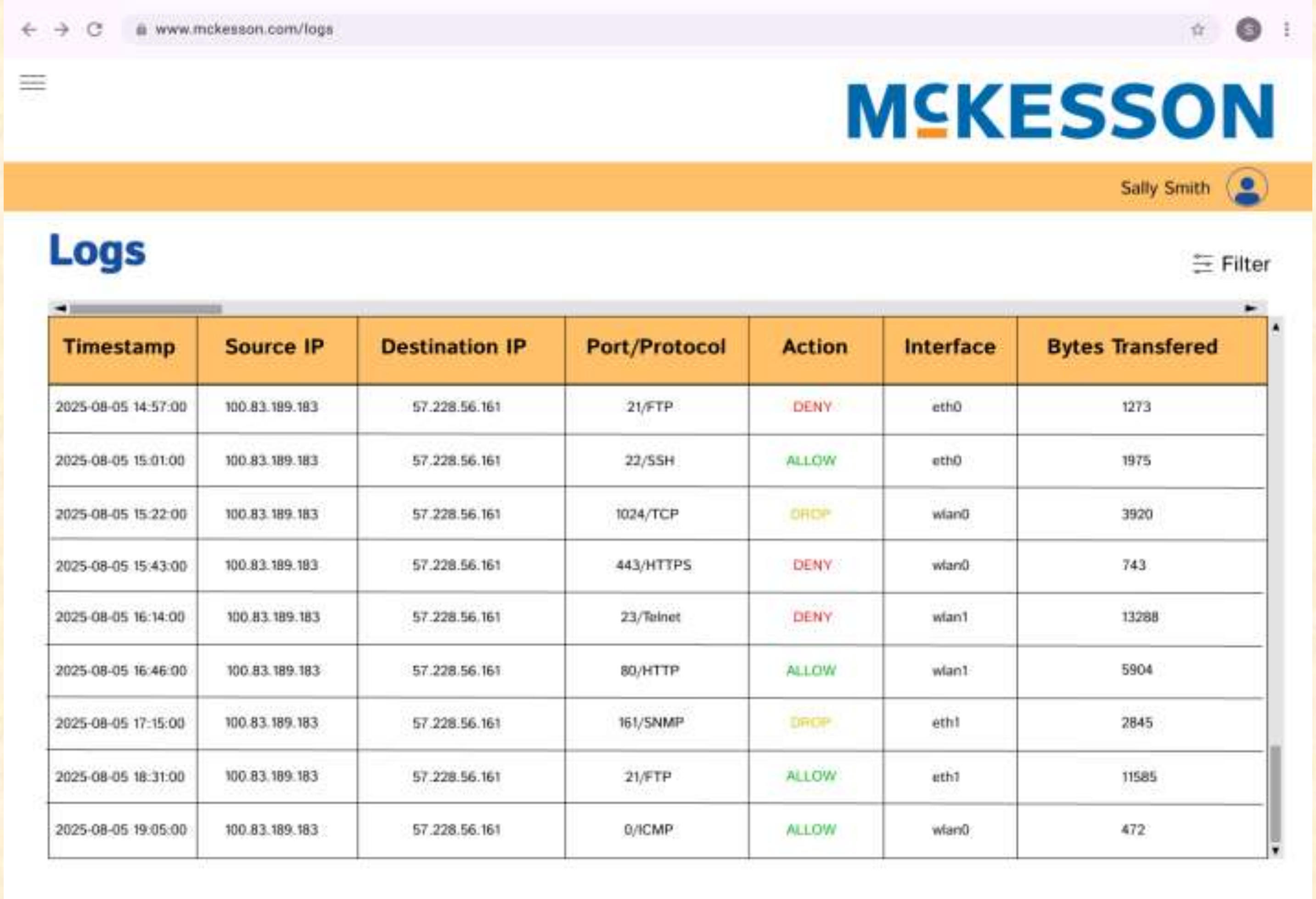
Screen Mockup: My Organization Page



My Organization

	Rule Id	Name
☑	RULE-6076	Pharma Data Control
☑	RULE-2629	Medical Infrastructure Shield
☑	RULE-5342	Healthcare IT Compliance
☑	RULE-8349	Pharma Data Control
☑	RULE-5437	Patient Data Safeguard
☑	RULE-3383	Medical Infrastructure Shield
☑	RULE-9387	Healthcare IT Compliance

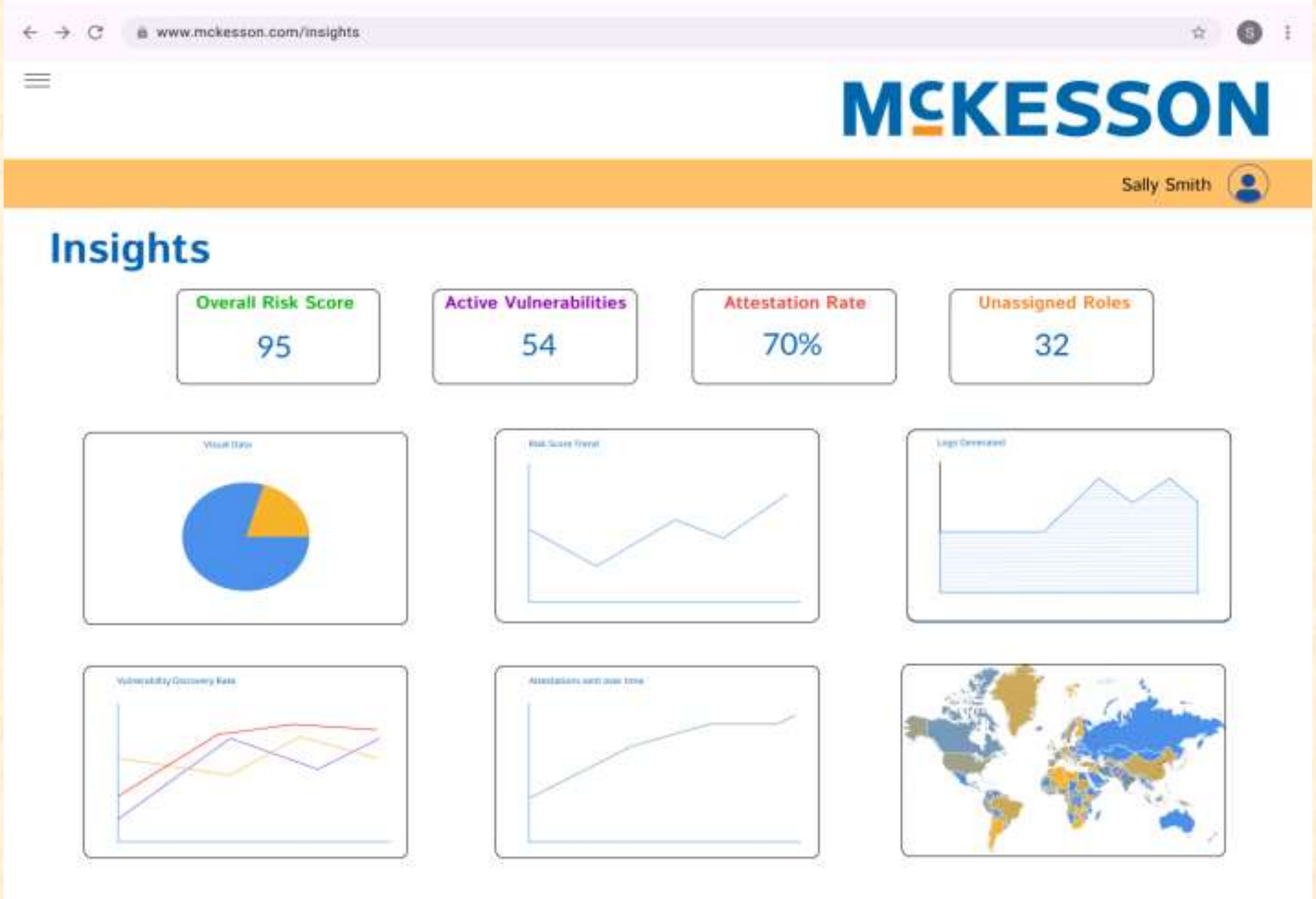
Screen Mockup: Logs Page



Logs

Timestamp	Source IP	Destination IP	Port/Protocol	Action	Interface	Bytes Transfered
2025-08-05 14:57:00	100.83.189.183	57.228.56.161	21/FTP	DENY	eth0	1273
2025-08-05 15:01:00	100.83.189.183	57.228.56.161	22/SSH	ALLOW	eth0	1975
2025-08-05 15:22:00	100.83.189.183	57.228.56.161	1024/TCP	DROP	wlan0	3920
2025-08-05 15:43:00	100.83.189.183	57.228.56.161	443/HTTPS	DENY	wlan0	743
2025-08-05 16:14:00	100.83.189.183	57.228.56.161	23/Telnet	DENY	wlan1	13288
2025-08-05 16:46:00	100.83.189.183	57.228.56.161	80/HTTP	ALLOW	wlan1	5904
2025-08-05 17:15:00	100.83.189.183	57.228.56.161	161/SNMP	DROP	eth1	2845
2025-08-05 18:31:00	100.83.189.183	57.228.56.161	21/FTP	ALLOW	eth1	11585
2025-08-05 19:05:00	100.83.189.183	57.228.56.161	0/ICMP	ALLOW	wlan0	472

Screen Mockup: Insights Page



www.mckesson.com/insights

MCKESSON

Sally Smith

Insights

Overall Risk Score 95

Active Vulnerabilities 54

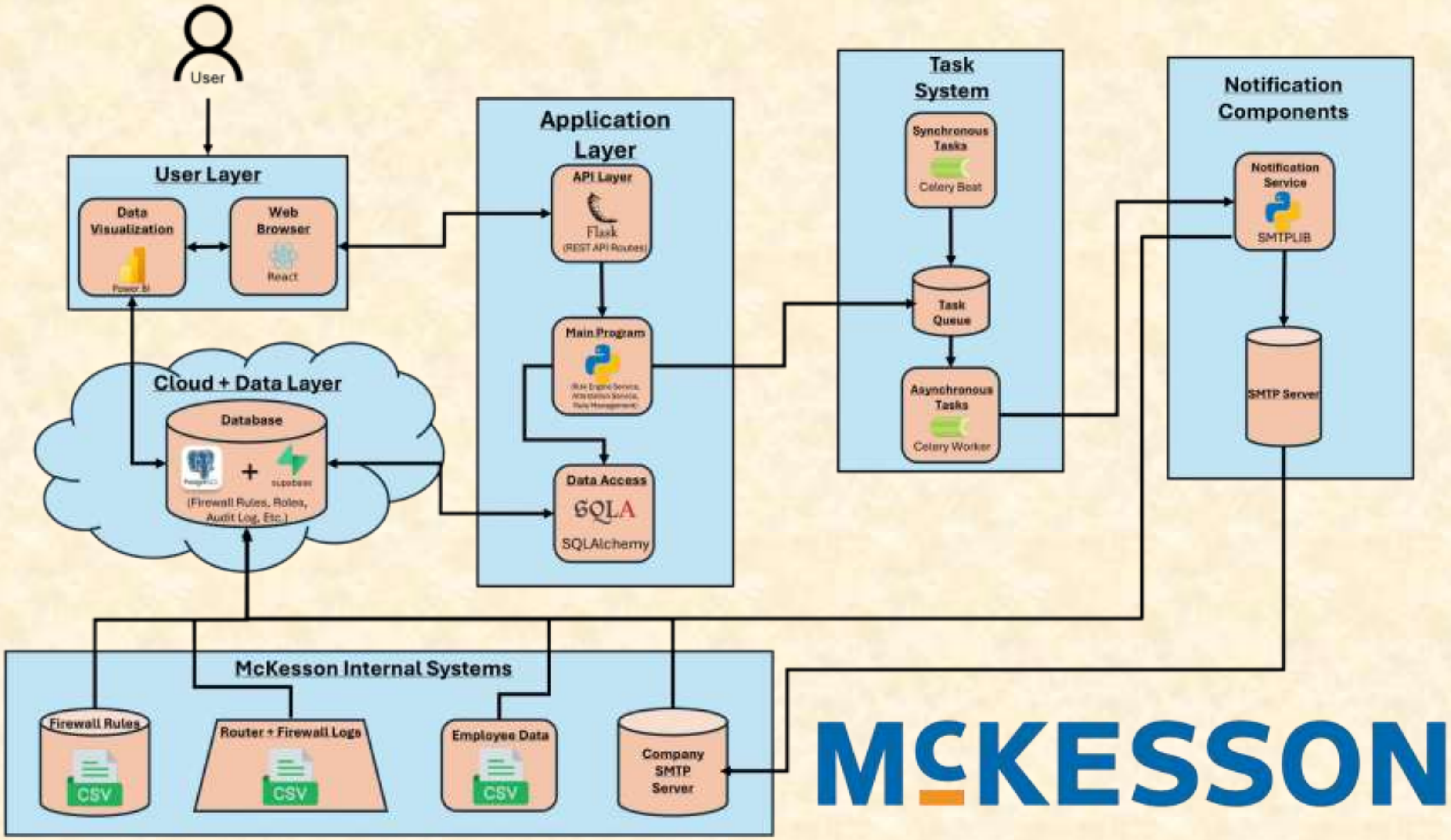
Attestation Rate 70%

Unassigned Roles 32

Project Technical Specifications

- Risk Engine:
  - Using firewall logs and firewall rule data, calculate a risk score associated with a network activity/application or rule
  - Identify unassigned roles, whether the protocol is encrypted, privilege level, segmentation of sensitive data, geo-restrictions, ports and applications accessed, and more
- Notification System:
  - Send emails to business/technology owners for rule attestations or threat alerts
- User Management:
  - Allow users to view and manage their subordinates and business units, add new employees under them, and which role they are (Business, Technology, or both)
- Rule Management:
  - Have managers be able to assign rules to subordinates and allow rules to be removed should they be depreciated

Project System Architecture



User

User Layer

Data Visualization

Power BI

Web Browser

React

Application Layer

API Layer

Flask

(REST API Routes)

Main Program

(Rule Engine Service, Attestation Service, Role Management)

Data Access

SQLA

SQLAlchemy

Task System

Synchronous Tasks

Celery Beat

Task Queue

Asynchronous Tasks

Celery Worker

Notification Components

Notification Service

SMTPLIB

SMTP Server

Cloud + Data Layer

Database

PostgreSQL + supabase

(Firewall Rules, Roles, Audit Log, Etc.)

McKesson Internal Systems

Firewall Rules

CSV

Router + Firewall Logs

CSV

Employee Data

CSV

Company SMTP Server

McKESSON

Project System Components

- Hardware Platforms
  - No special hardware
- Software Platforms / Technologies
  - Front-end: React.js (HTML, CSS)
  - Web framework & API: Flask
  - Database: PostgreSQL (hosted through Supabase)
  - Backend: Python
  - Notification and attestation systems: Celery/smtplib

Project Risks

- Risk 1: Handling Conflicting Rules
  - Multiple rules to work with, older and newer, resulting in conflicts over which to prioritize
  - Mitigation: Work with sponsor to determine rule priorities, implement a hierarchy of the importance of a rule
- Risk 2: Large Data Affecting Performance
  - McKesson has hundreds of thousands of firewall rules, working with such data can lead to slower performance
  - Mitigation: Utilize indexes within database schema to optimally store and query data as well as implementing data structures to score data efficiently
- Risk 3: Differentiation Between Roles
  - McKesson's firewall structure has roles for business and/or technology owners, but individual can be business owner for one firewall rule, and technology owner for another
  - Mitigation: System will check the user's role when they log in, edge cases will be handled by prioritizing detailed logs over simple logs
- Risk 4
  - Success of the project depends on creating a risk-engine that is not too cautious or not cautious enough
  - Mitigation: Consult sponsor to get detailed attributes for the risk engine. Utilize a hierarchy with risks that a threat could pose determined by a formula comprised of attributes sponsor needs

Questions?

? ? ? ?

? ?

? ? ?