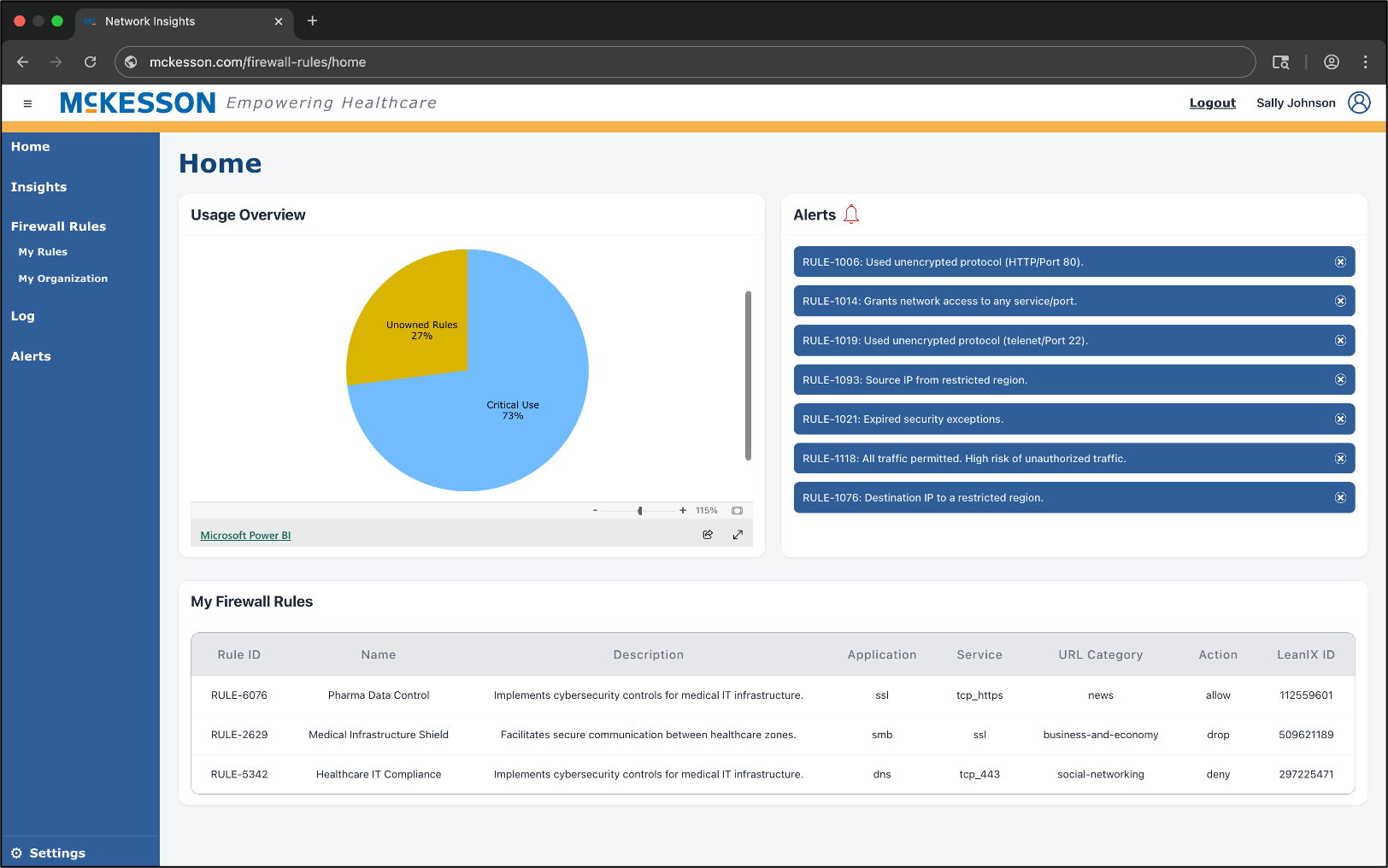
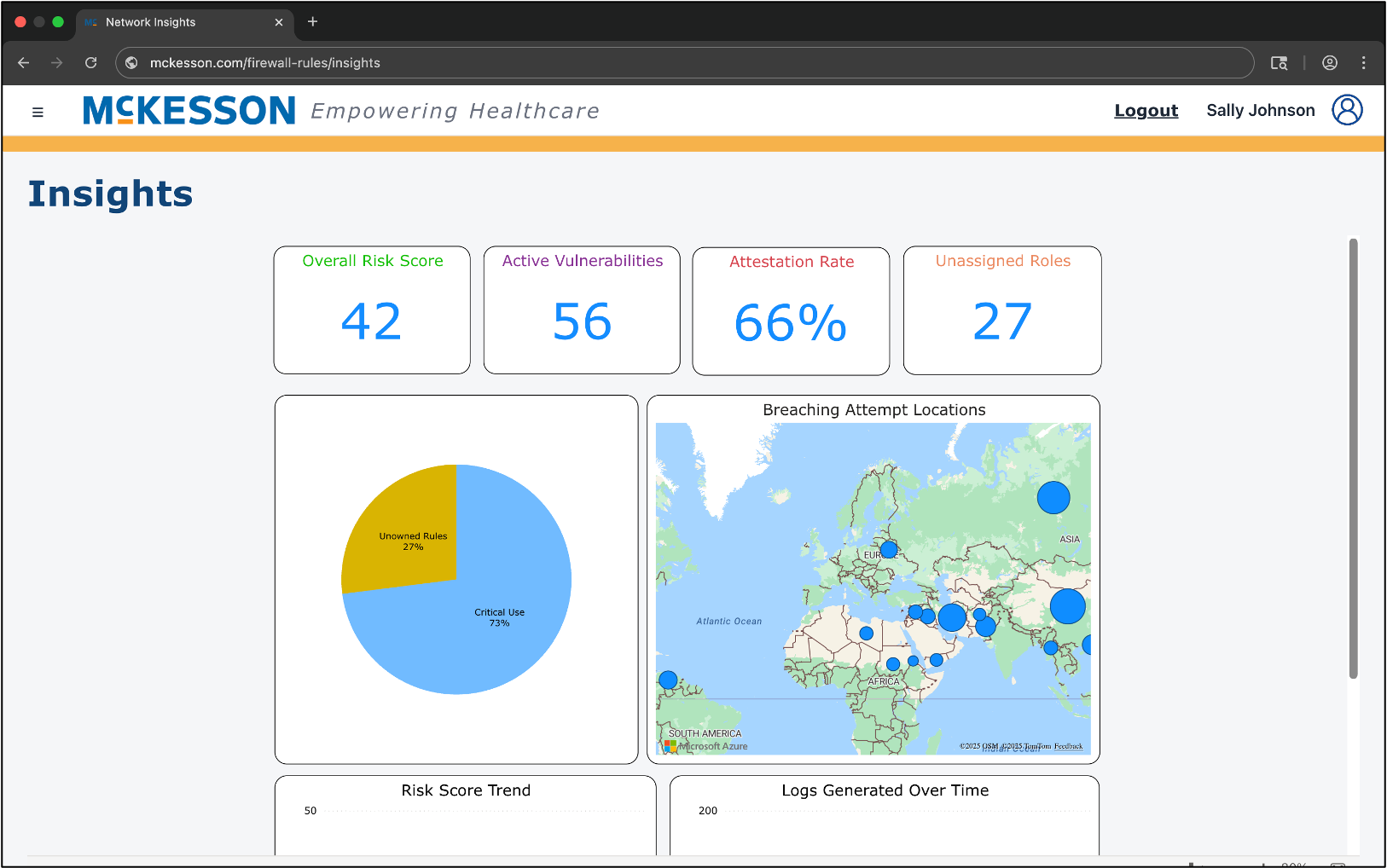
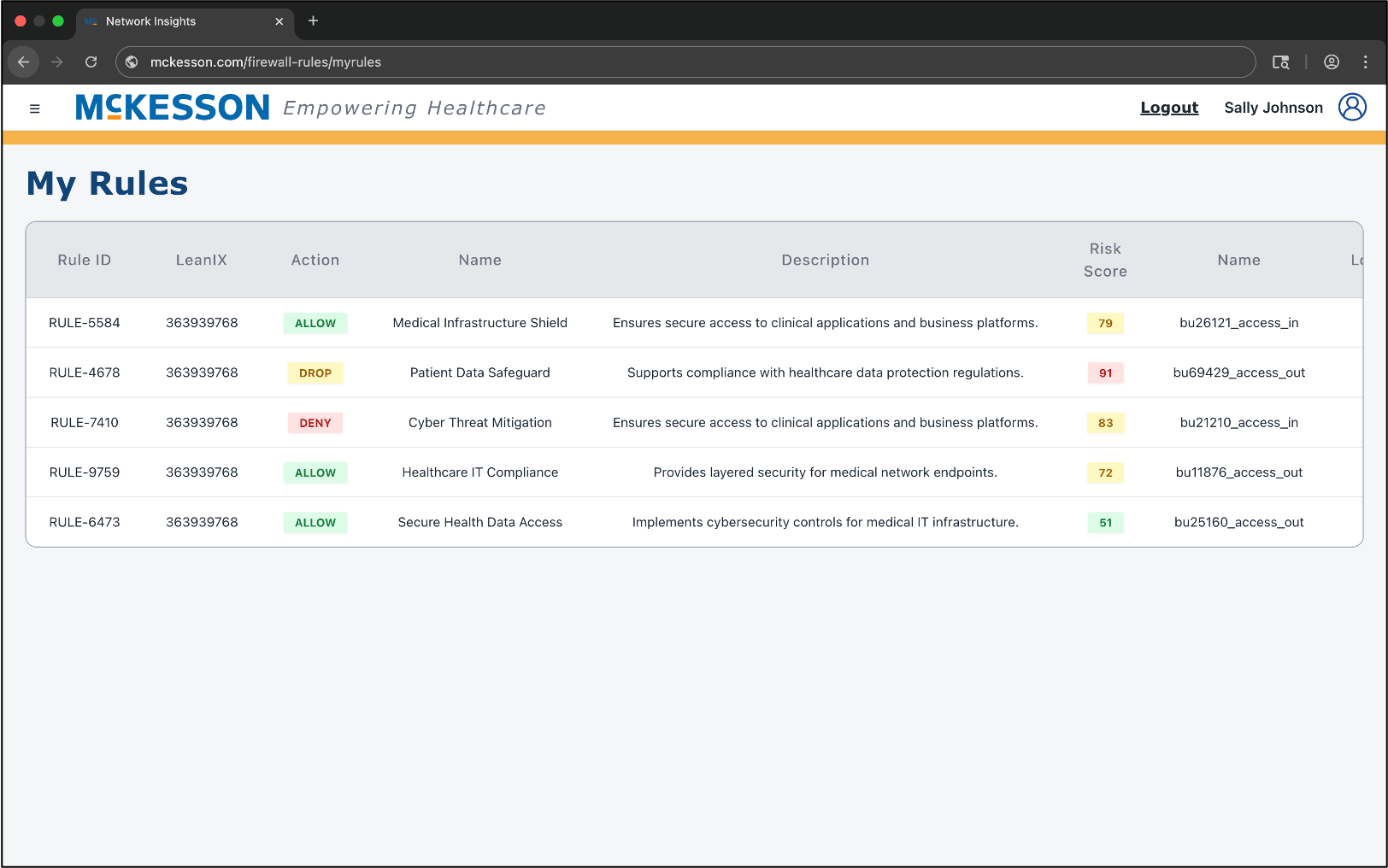
Design Day Booklet Team Page







PAGE N + 18



McKesson

Project Sponsors

Taylor Bolton

Phoenix, Arizona

Antony Mathew

Detroit, Michigan

Spencer Searle

Detroit, Michigan

Kim Steen

Phoenix, Arizona

Michigan State University

Team Members (left to right)

Dev Khakhar

Rajkot, Gujarat, India

Karena Lam

Novi, Michigan

Aneesh Kapole

Pune, Maharashtra, India

Aisha Latif

Shelby Township, Michigan

Conner O’Sullivan

Alexandria, Virginia

Divya Nadella

Novi, Michigan



McKesson is a Fortune 10 healthcare company that distributes pharmaceutical supplies and provides patient care across the world. By integrating technology services into healthcare, McKesson emphasizes the importance of patient outcomes.

To protect sensitive data and prevent interferences in crucial operations, healthcare industries rely on secure cybersecurity initiatives. Organizations rely on firewalls to prevent malicious actors from gaining access to their network. A firewall rule is a directive for a firewall which controls the network’s traffic. Detecting vulnerabilities in firewall rules is essential to maintaining a secure digital environment.

The Intelligent Network Security for High-Risk Traffic system provides an interactive and convenient way for McKesson employees to view and mitigate firewall rule risks and threats.

The web interface allows business and technology owners to manage firewall rules that relate to their applications. This authorizes managers to assign rules to their subordinates, making sure they are monitored in case of threats, while also regulating their own rules.

The system relies on a risk engine which analyzes attributes of firewall rules to determine their vulnerabilities. When suspicious behavior or anomalies are detected with our risk engine, alerts and attestations are sent out to the rule’s owner, prompting them to act against these threats.

The webpage includes a dashboard that monitors rule usage and risk trends over time. The data is stored in a secure database which is integrated with the webpage through visualized graphs and charts that are easy-to-read.

The application is constructed using Python and Flask as the back end and PostgreSQL as the database to analyze firewall rules. The front end is built with React and Power BI.

CSE498 | 8:00 a.m. – Noon Computer Science and Engineering, Third Floor | 3200/3300 Hallway

McKesson

Intelligent Network Security for High-Risk Traffic