

IoT Shield

Students: Max Gleiberman, Julian Hernandez, Elizabeth Hechavarria, Nathan Mahabeer
Instructor/Faculty: Seyedmasoud Sadjadi, Florida International University

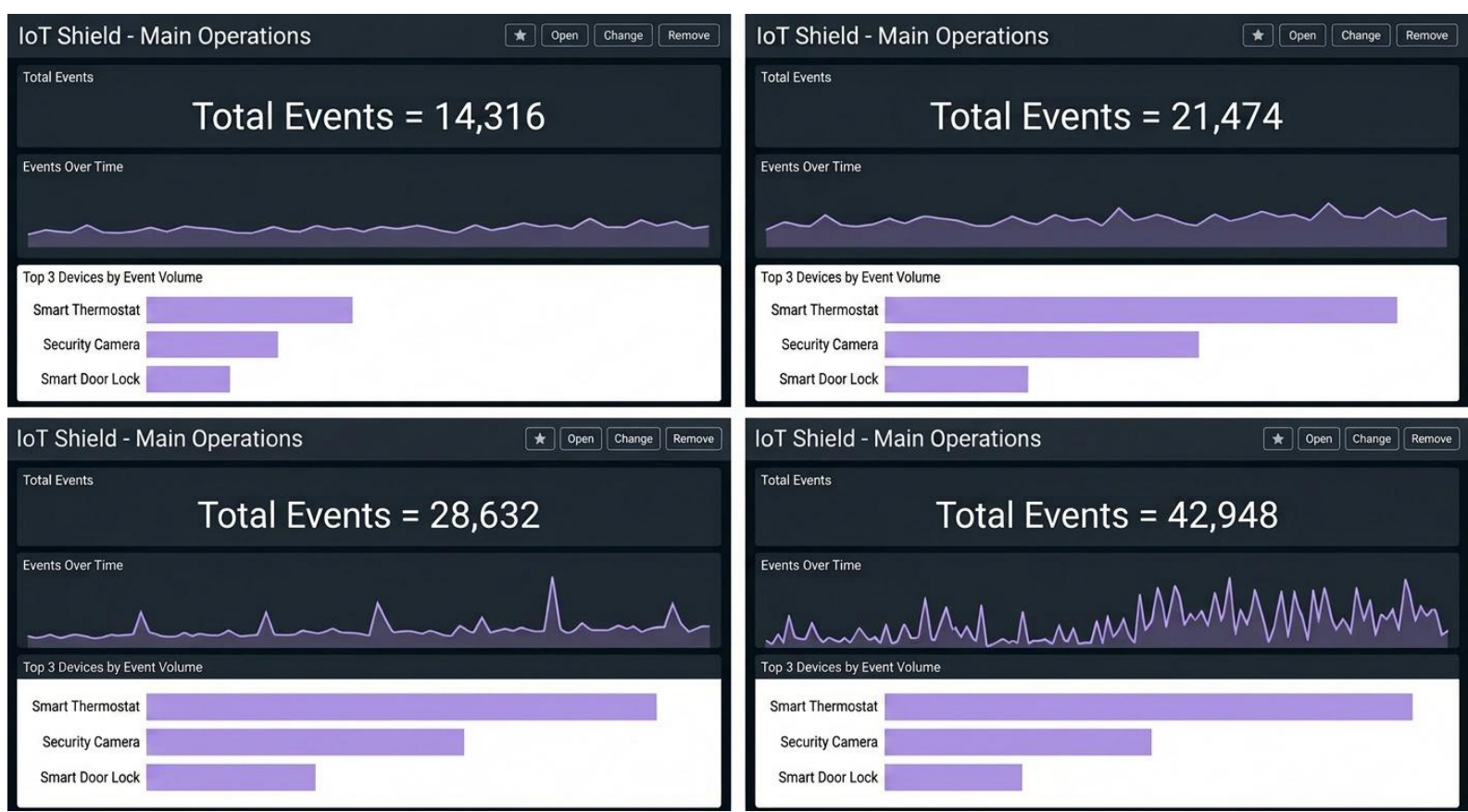
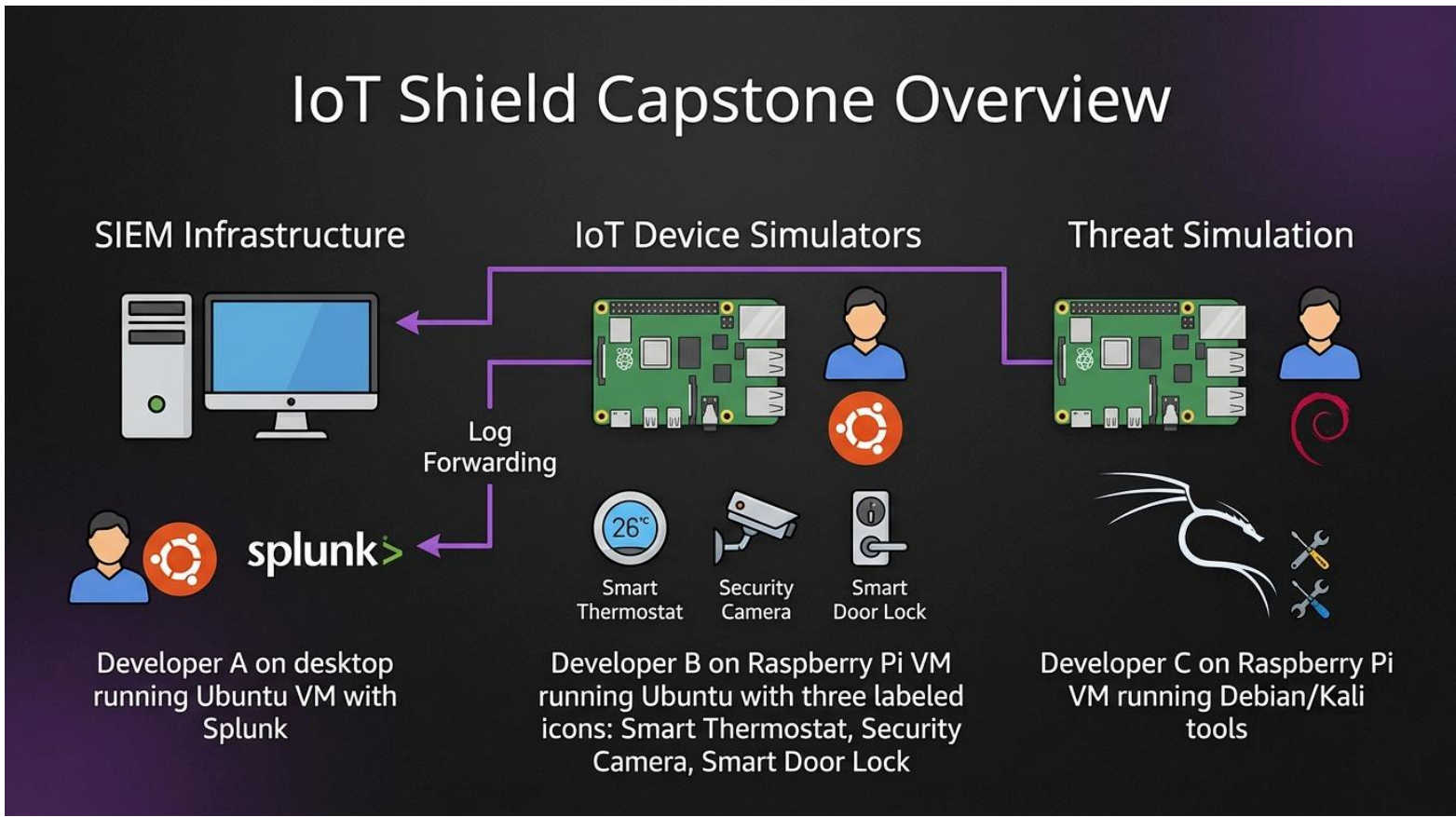
PROBLEM

In modern cybersecurity environments, especially those involving IoT devices, traditional SIEM systems often rely on powerful hardware and complex infrastructure, making them inaccessible for lightweight, low-cost deployments. This project addresses the challenge of using a Raspberry Pi, which is a compact, energy-efficient device, to host virtual machines and forward logs to a centralized SIEM system. The goal is to determine whether such a setup can reliably simulate network traffic, detect threats, and maintain real-time log ingestion without compromising performance or security. Limitations in OS compatibility, resource constraints, and Splunk’s inability to run natively on ARM64 architecture present significant hurdles, prompting the need for innovative solutions that balance functionality with hardware efficiency.

SOLUTION

- The solution developed in the IoT Shield project is a hybrid monitoring environment combining lightweight Raspberry Pi hardware with Splunk Enterprise SIEM on a desktop PC.
- Raspberry Pi hosts two virtual machines — one simulating IoT devices, one executing cyberattack scenarios.
- Achieves real-time log forwarding and centralized analysis across both VMs.
- Custom Splunk detection rules and dashboards monitor brute-force attempts, data exfiltration, port scans, and unauthorized access.
- Offloads heavy SIEM processing to the desktop, keeping the Pi focused on cost-effective IoT and threat simulation.
- Demonstrates a secure, replicable model for monitoring IoT environments.

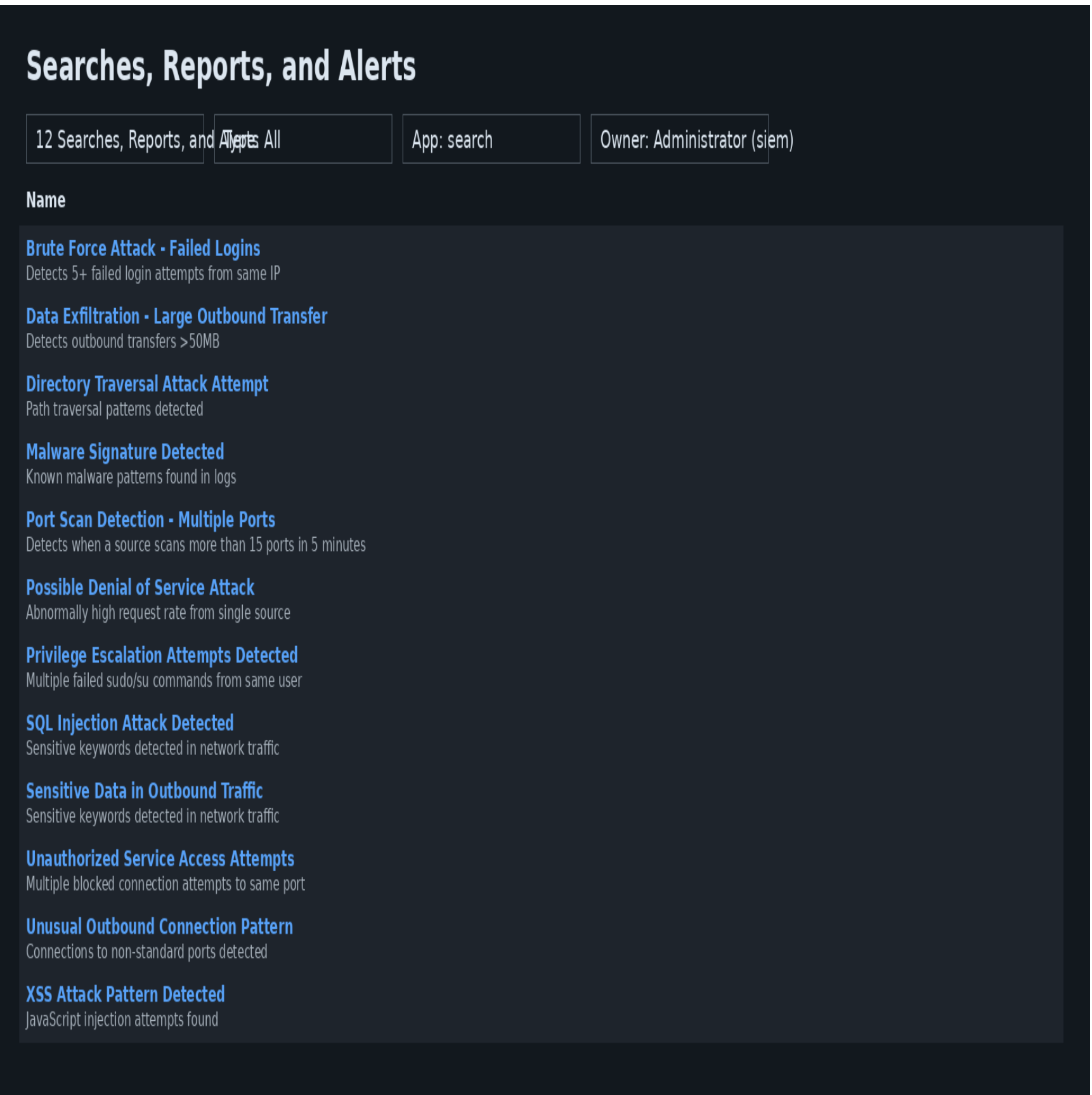
SYSTEM DESIGN & MAIN DASHBOARD



CURRENT SYSTEM

- SIEM platforms need powerful hardware, limiting use in lightweight IoT setups.
- Splunk Enterprise cannot run natively on Raspberry Pi’s ARM64 architecture.
- Monitoring depends on desktop/server machines for log ingestion and analysis.
- IoT devices lack direct SIEM integration, reducing visibility into threats.
- Resource limits on small devices prevent full SIEM hosting.
- Traditional monitoring is manual and fragmented, slowing real-time detection.
- The IoT Shield project addresses these gaps by combining Raspberry Pi for simulation with desktop-hosted Splunk for centralized analysis.

OBJECT DESIGN

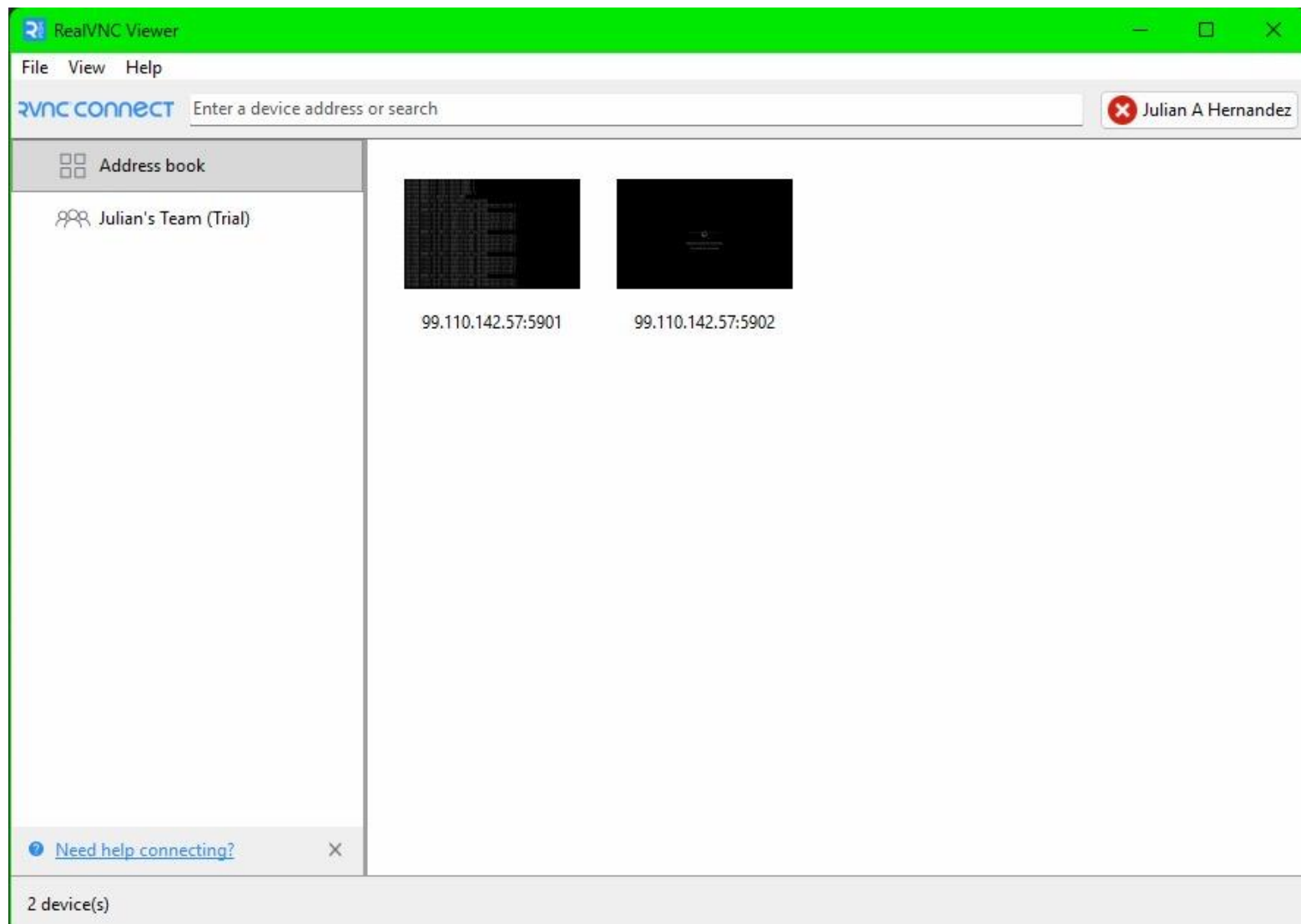


SUMMARY

- Developed a production-quality cybersecurity monitoring system integrating Splunk SIEM, IoT simulators, and threat simulation tools.
- Configured a Raspberry Pi to host two VMs: one generating IoT traffic and one simulating cyberattacks.
- Implemented custom detection rules and dashboards in Splunk to monitor brute-force attempts, data exfiltration, and unauthorized access.
- Validated system performance using htop monitoring, IoT Shield dashboards, and remote access via RealVNC Viewer.
- Ensured secure architecture with port forwarding, firewall rules, and encrypted log transmission.
- Demonstrated that Raspberry Pi can reliably forward logs to Splunk, though full SIEM hosting requires desktop infrastructure.

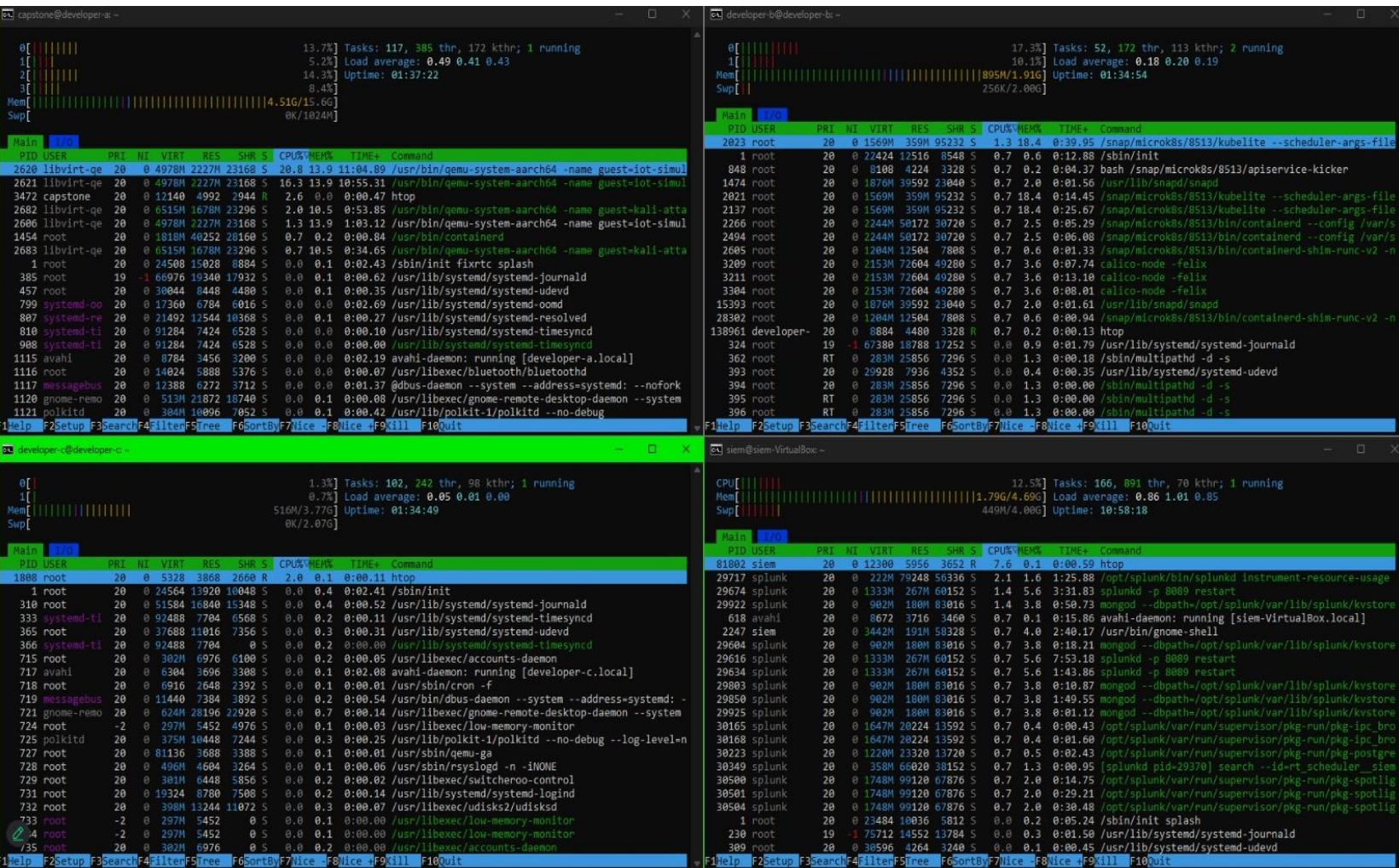
REQUIREMENTS

- Raspberry Pi 5 (16GB RAM, NVME SSD)
- Ubuntu Desktop 24.04.3
- Splunk Enterprise 10.0.1
- Python 3.10.12 with requests & urllib3
- Debian Linux with Nmap, Hydra, Wireshark
- RealVNC Viewer for remote access
- Durable network and firewall configuration



IMPLEMENTATION

The IoT Shield system was implemented over six development sprints, integrating Splunk SIEM, IoT simulators, and threat simulation tools across virtual machines. Raspberry Pi hosted two VMs—one generating IoT traffic and the other simulating cyberattacks—while forwarding logs to a Splunk instance on a desktop PC.



CONTRIBUTIONS

- Built IoT Shield using Raspberry Pi VMs for IoT traffic and attack simulation, with logs forwarded to Splunk Enterprise.
- Developed custom detection rules and dashboards to identify brute-force attempts, data exfiltration, port scans, and unauthorized access.
- Validated performance with htop monitoring, dashboards, and remote access tools, ensuring secure architecture with firewalls and encrypted log transmission.
- Demonstrated feasibility of lightweight IoT simulation while highlighting the need for desktop infrastructure for full SIEM hosting.

ACKNOWLEDGEMENT

The material presented in this poster is based upon the work supported by Florida International. We/I thank Florida International University for his/her/their assistance and mentorship that I/we received throughout the senior design project.