# APIARY

A user-friendly blocklist and safelist management interface

Duke | Code+

## Context

- Designed to be a user-friendly interface for managing blocklists and safelists
- Built on top of an existing backend system, with core functionality already in place
- Prior UI was under development but failed to meet usability standards
- Project goal is to improve upon the previous version with enhanced UX and streamlined design

## Objectives

- Improve the usability and accessibility of blocklist/safelist management
- Streamline workflows for security analysts and IT administrators
- Provide intuitive visual feedback for system actions and status
- Ensure consistency and clarity across all user interactions
- Address shortcomings of the previous UI through user-centered design
- Deliver a stable, scalable, and responsive front-end interface

## Key Features

- Add, remove, update, or delete entries across blocklists and safelists, including IPs, URLs, and domain names
- Modify evolving fields like TLP levels and confidence scores as threat intelligence changes
- Assign tags to entries from a predefined list or create new ones for custom organization
- Search across all columns and filter results easily to find the data you need
- A quick access dashboard to view high-level summaries and recent activity at a glance
- Designed for simplicity, speed, and clarity in security operations

**Watch APIARY's Demo**

## Next Steps

Now we look to prepare APIARY for open-source release by cleaning and documenting the codebase, developing onboarding materials, and coordinating with Duke OIT and ITSO to finalize licensing and deployment strategies. We also aim to promote adoption across other universities and explore opportunities for future enhancements to support broader cybersecurity needs.