MICHIGAN STATE UNIVERSITY

Project Plan Presentation

Enhanced MISP User Interface

The Capstone Experience

Team GM

Noah Anderson

Marven Nadhum

Alex Richards

Jake Rizkallah

Jordyn Rosario

Department of Computer Science and Engineering

Michigan State University

Fall 2021

From Students…

…to Professionals

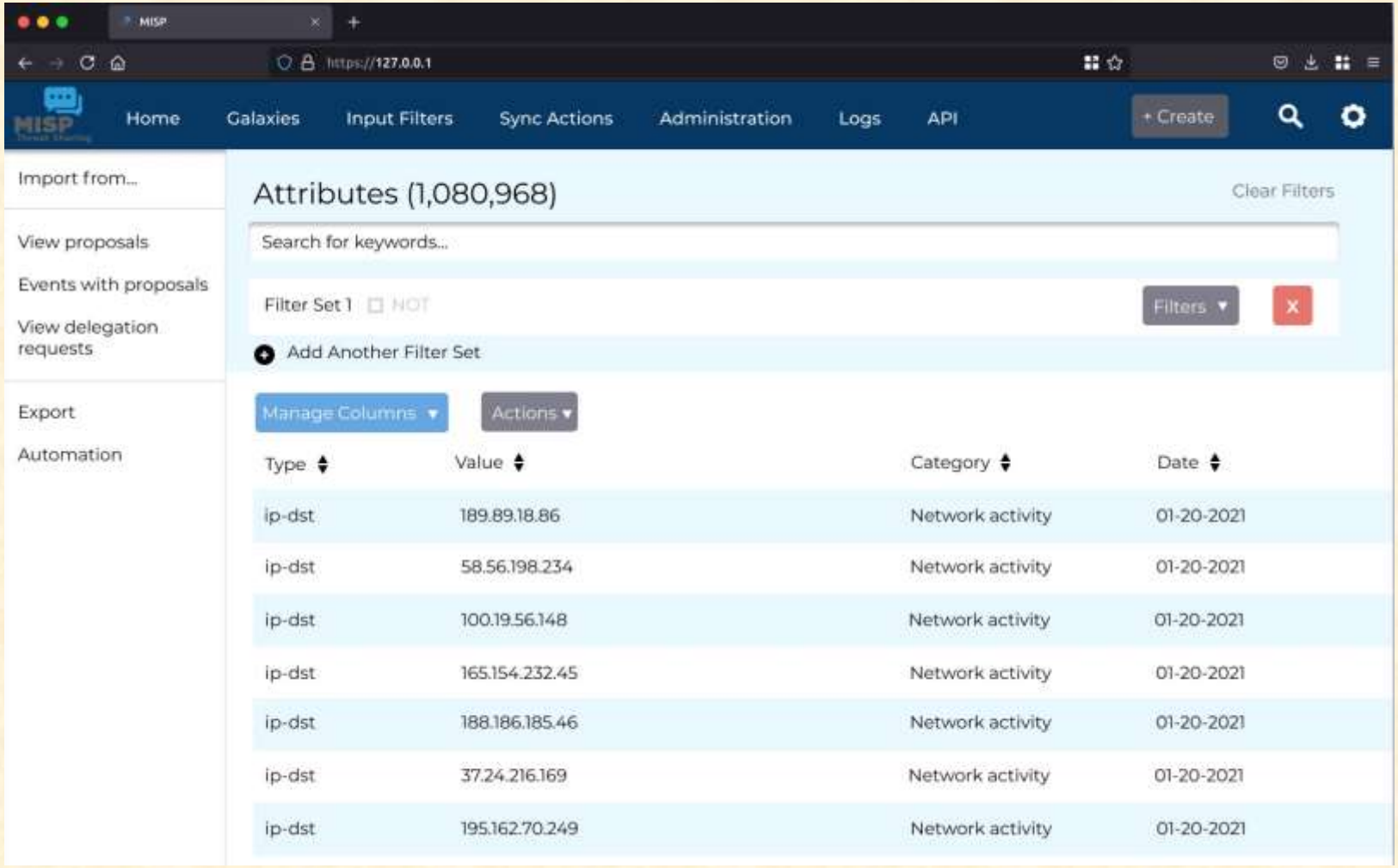
Functional Specifications

- Redesign UI for GM analysts to create a more user-friendly system
- Improve search functionality to allow for more complex searches
- Improve MISP contextualization

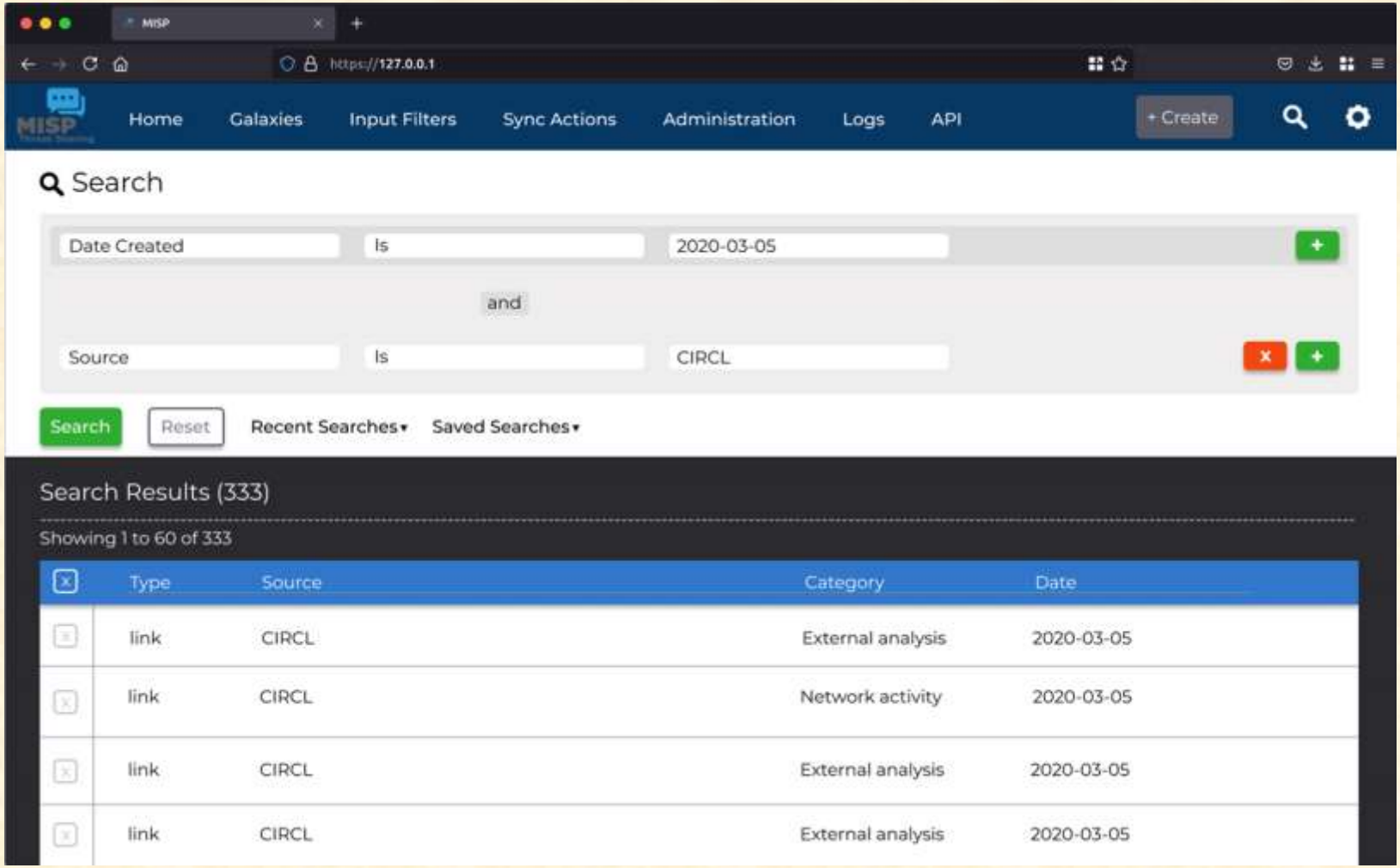
Design Specifications

- Improved Search Functionality
  - Allowing of wildcard searches
  - Boolean operators on searches, allowing nested searches
- Better Contextualization
  - Give comments hyperlinks to go back to the page that was commented on
  - Attribute descriptions readily available from feed page
  - Manage and add feeds directly
- UI Overhaul
  - Improve site navigation, allow for easier ways to go back to previous locations
  - Allow for all columns to be reordered or removed
  - Improve sorting functionality of feed tables

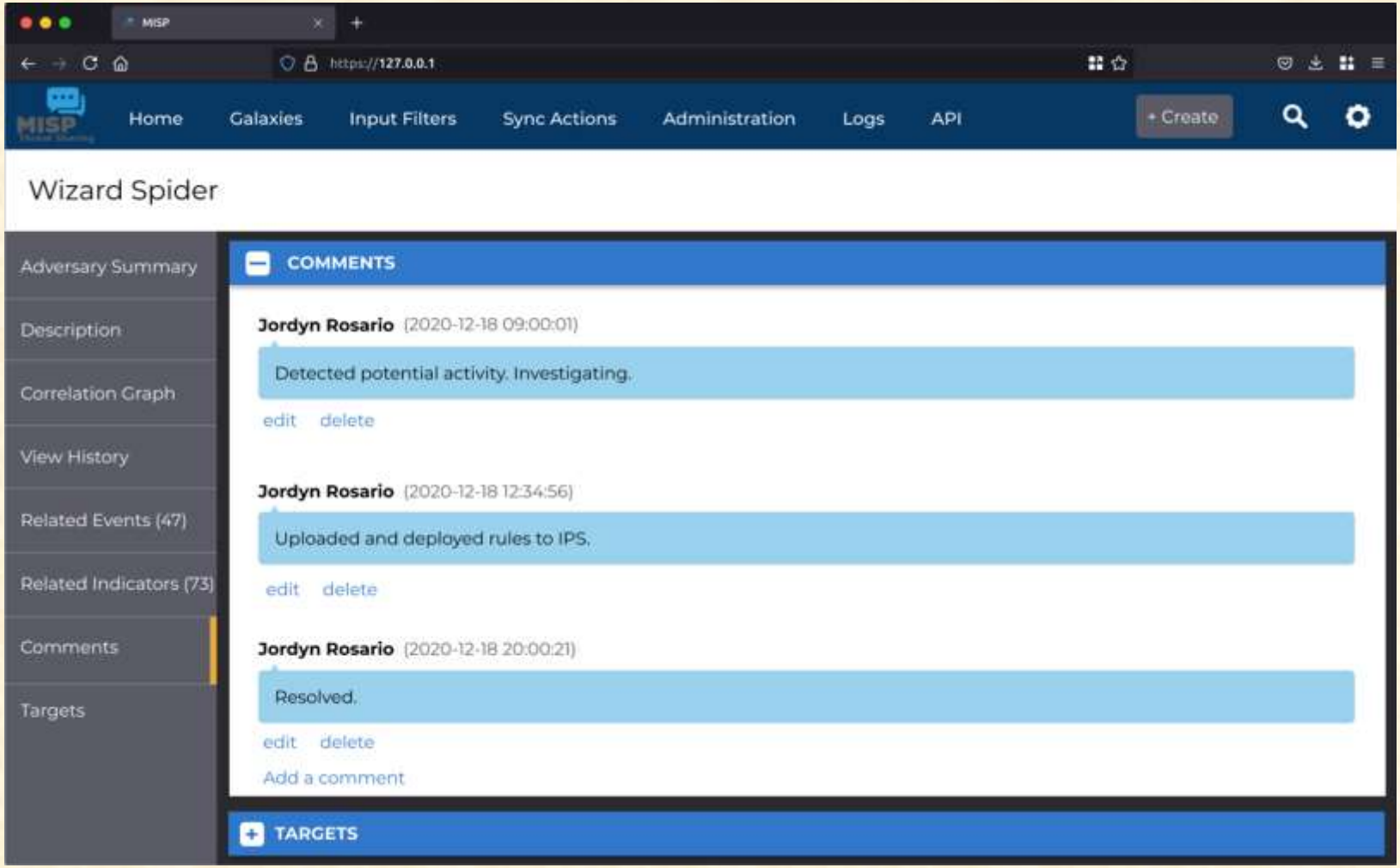
MISP Attribute Search



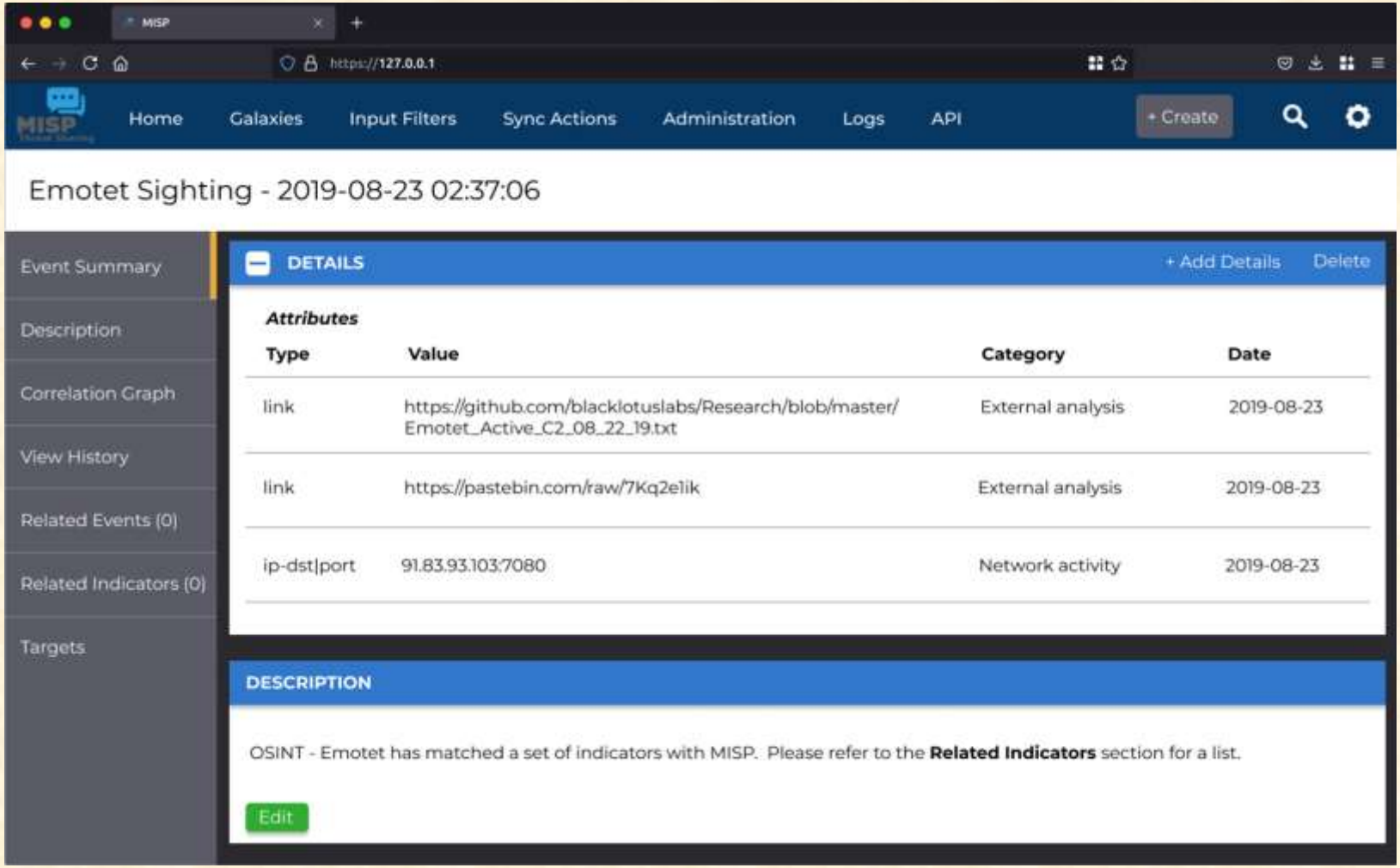
MISP Nested Search Results



MISP Comment Page



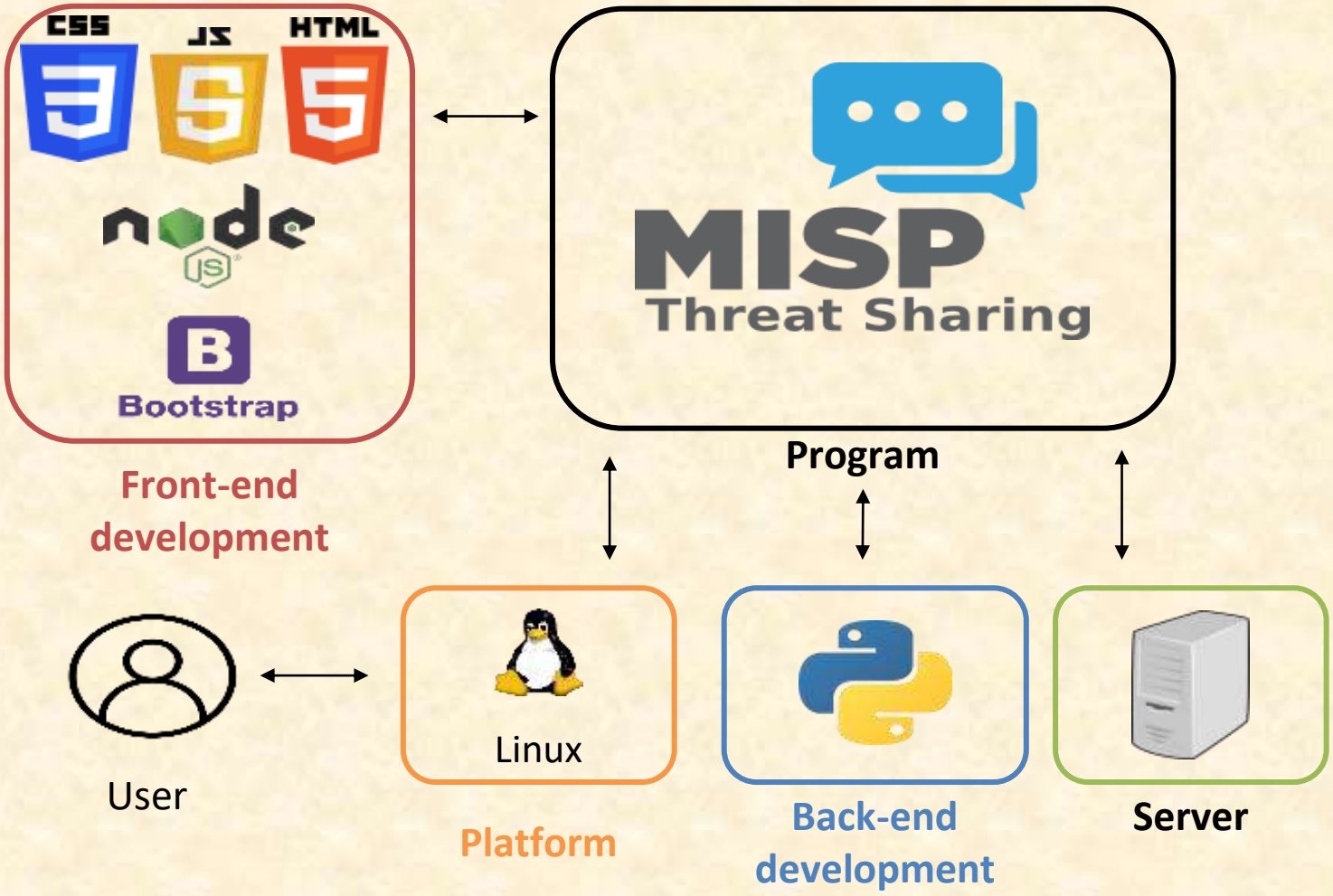
MISP Event Page



Technical Specifications

- Python to work on back end
- Bootstrap/CSS is being used for front end design changes
- HTML/Javascript is being used to change the actual web pages
- Linux VM to install and run MISP

System Architecture



System Components

- Hardware Platforms
  - Linux VM
- Software Platforms / Technologies
  - Version Control:
    - GitHub
  - Front End:
    - Atom: HTML/Bootstrap/CSS/JavaScript
  - Back End:
    - PyCharm: Python

Risks

- Implementing Automation for Contextualization
  - Feeds need to be automatically ported into MISP with tags and attributes intact, we are unsure how to read the feeds and work with the feeds structure
  - The OpenAPI is flexible, and there are fragments of automation in different PyModules that we will examine and use as a reference
- Implementing Wildcard Searches
  - Search function needs to be overhauled to allow wildcard characters
  - MISP has a Rest client for admins that uses HTTP to perform many actions, including wildcard searches. We will use this source code to derive our implementation in the search bar for the general user
- Ease of Use
  - MISP's GUI must be easy to use for the security analysts compared to the previous version without creating new design flaws such as inconsistent page design, lack of contrast, and bad information architecture
  - Consistent contact with the client and multiple iterations of the GUI to ensure the interface is what they want

Questions?