

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

Attributes (1,080,968) Clear Filters

Search for keywords...

Filter Set 1 NOT Filters X

+ Add Another Filter Set

Manage Columns Actions

Type	Value	Category	Date
ip-dst	189.89.18.86	Network activity	01-20-2021
ip-dst	58.56.198.234	Network activity	01-20-2021
ip-dst	100.19.56.148	Network activity	01-20-2021
ip-dst	165.154.232.45	Network activity	01-20-2021
ip-dst	188.186.185.46	Network activity	01-20-2021
ip-dst	37.24.216.169	Network activity	01-20-2021
ip-dst	195.162.70.249	Network activity	01-20-2021



MISP Nested Search Results

The screenshot displays the MISP web interface. The search bar contains the following criteria:

- Date Created is 2020-03-05
- and
- Source is CIRCL

Buttons for Search, Reset, Recent Searches, and Saved Searches are visible below the search bar.

Search Results (333)
Showing 1 to 60 of 333

Type	Source	Category	Date
link	CIRCL	External analysis	2020-03-05
link	CIRCL	Network activity	2020-03-05
link	CIRCL	External analysis	2020-03-05
link	CIRCL	External analysis	2020-03-05



MISP Comment Page

The screenshot shows a web browser window displaying the MISP (Malware Information Sharing Platform) interface. The browser's address bar shows the URL `https://127.0.0.1`. The MISP navigation menu includes links for Home, Galaxies, Input Filters, Sync Actions, Administration, Logs, and API, along with a '+ Create' button and search and settings icons. The main content area is titled 'Wizard Spider' and features a sidebar on the left with navigation options: Adversary Summary, Description, Correlation Graph, View History, Related Events (47), Related Indicators (73), Comments, and Targets. The 'Comments' section is active, showing a list of three comments by 'Jordyn Rosario' with timestamps and edit/delete options. The first comment is 'Detected potential activity. Investigating.' (2020-12-18 09:00:01), the second is 'Uploaded and deployed rules to IPS.' (2020-12-18 12:34:56), and the third is 'Resolved.' (2020-12-18 20:00:21). An 'Add a comment' link is visible at the bottom of the comments list. Below the comments, a 'TARGETS' section is partially visible.

Wizard Spider

Adversary Summary

Description

Correlation Graph

View History

Related Events (47)

Related Indicators (73)

Comments

Targets

COMMENTS

Jordyn Rosario (2020-12-18 09:00:01)
Detected potential activity. Investigating.
edit delete

Jordyn Rosario (2020-12-18 12:34:56)
Uploaded and deployed rules to IPS.
edit delete

Jordyn Rosario (2020-12-18 20:00:21)
Resolved.
edit delete
Add a comment

TARGETS



MISP Event Page

The screenshot displays the MISP (Malware Information Sharing Platform) interface. The browser address bar shows the URL `https://127.0.0.1`. The navigation menu includes Home, Galaxies, Input Filters, Sync Actions, Administration, Logs, and API. A '+ Create' button and search icons are visible on the right. The main content area is titled 'Emotet Sighting - 2019-08-23 02:37:06'. On the left, a sidebar menu lists options: Event Summary, Description, Correlation Graph, View History, Related Events (0), Related Indicators (0), and Targets. The main panel is divided into two sections: 'DETAILS' and 'DESCRIPTION'. The 'DETAILS' section features a table with columns for Type, Value, Category, and Date. The 'DESCRIPTION' section contains a text block and an 'Edit' button.

Event Summary

Description

Correlation Graph

View History

Related Events (0)

Related Indicators (0)

Targets

DETAILS + Add Details Delete

Attributes

Type	Value	Category	Date
link	https://github.com/blacklotuslabs/Research/blob/master/Emotet_Active_C2_08_22_19.txt	External analysis	2019-08-23
link	https://pastebin.com/raw/7Kq2elik	External analysis	2019-08-23
ip-dst port	91.83.93.103:7080	Network activity	2019-08-23

DESCRIPTION

OSINT - Emotet has matched a set of indicators with MISP. Please refer to the **Related Indicators** section for a list.

Edit

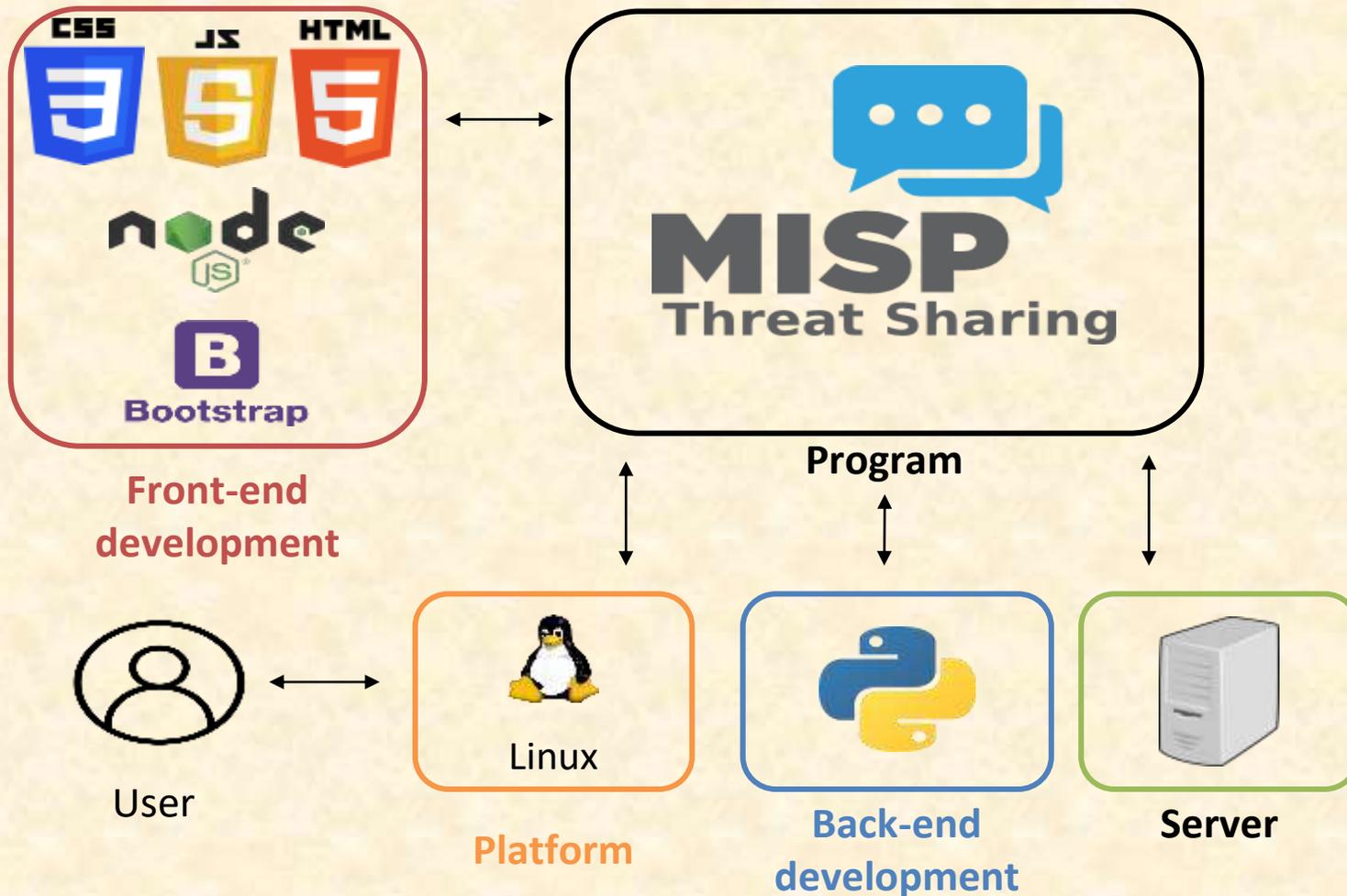


Technical Specifications

- 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?

?

?

?

?

?

?

?

?

?

