INTRODUCTION TO THREAT HUNTING WITH ZU

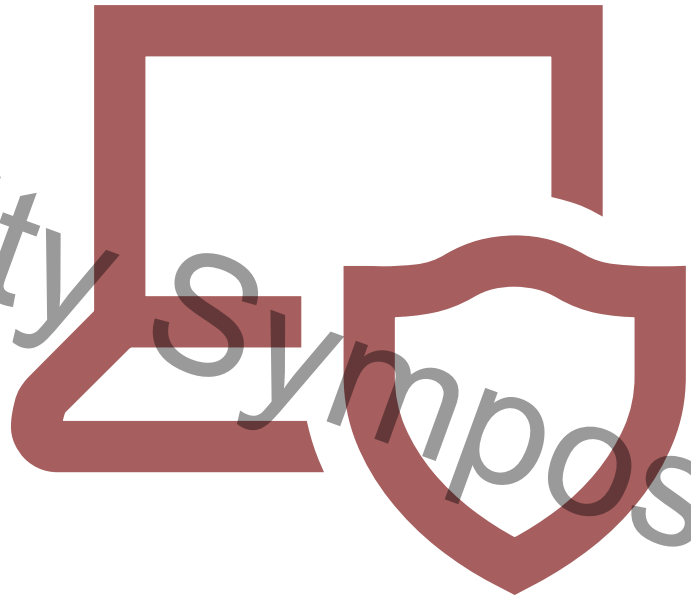
Deep Ramanayake
Xavier University

AGENDA

- Introduction to Threat Hunting
- Zeek and Suricata Command Line Analysis
- ZUI: Graphical User Interface for Data Exploration
- ZUI Walkthrough
- Conclusion

INTRODUCTION TO THREAT HUNTING

- What is Threat Hunting?
- Proactive approach to cybersecurity
- Identifying and mitigating threats before they cause harm
- Importance of data exploration in threat hunting



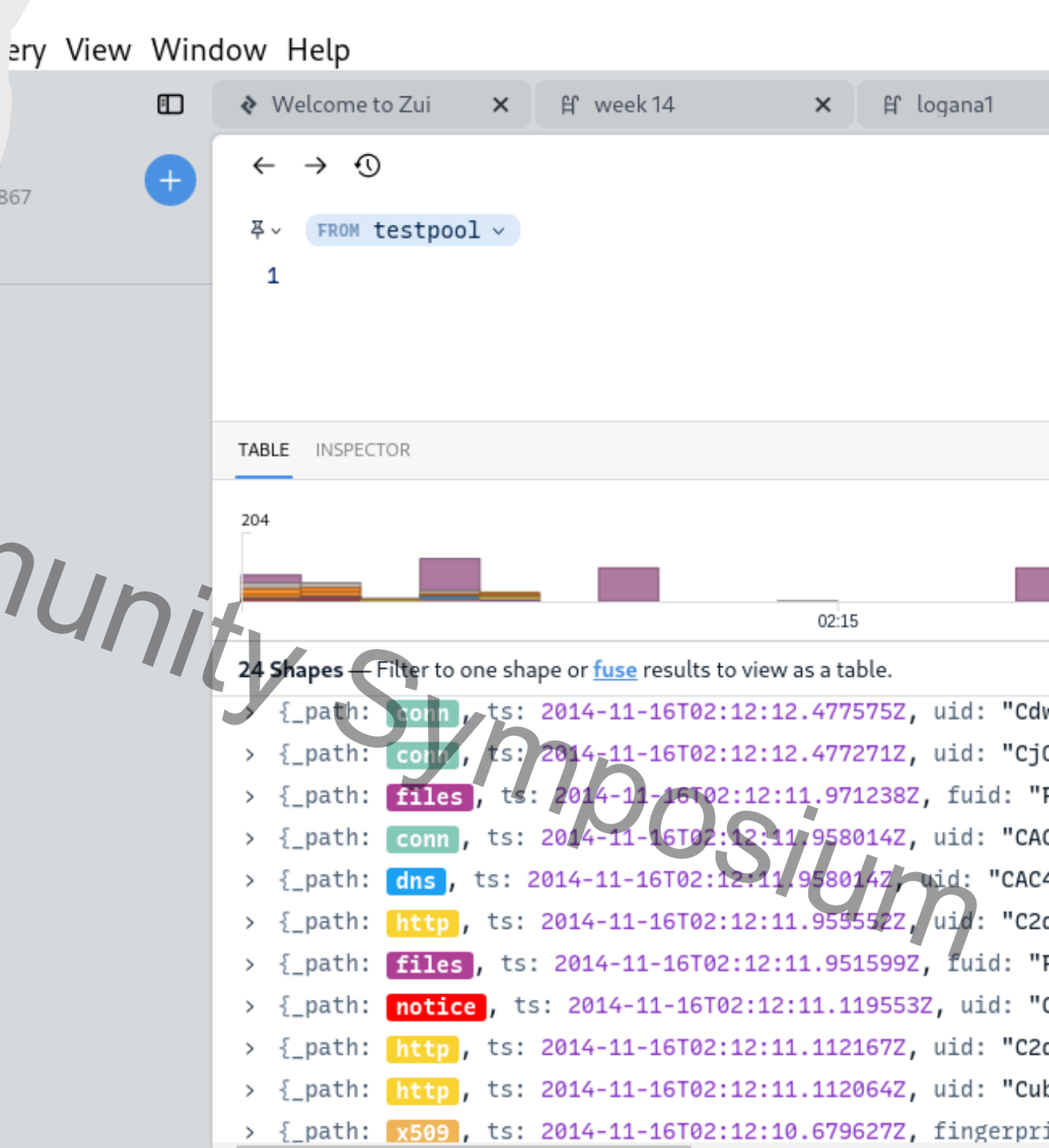
https://mitre-attack.github.io/attack-navigator/?ref=fr33s0ul.tech

ZEEK AND SURICATA COMMAND LINE ANALYSIS

- Overview of Zeek and Suricata
- Command line analysis for network security monitoring
- Benefits of understanding command line analysis
- Preparation for advanced threat hunting techniques

ZUI: GRAPHICAL USER INTERFACE FOR DATA EXPLORATION

- Introduction to ZUI (formerly called Brim)
- Purpose: Graphical interface for exploring data in Zed lakes
- Features:
  - Visual representation of data
  - Streamlined data analysis
  - Intuitive user interface



ZUI WALKTHROUGH - PART 1

Accessing ZUI interface

Overview of main components:

- Search Bar
- Data Panels

Importing data into ZUI

EXPLORING DATA USING ZUI:

Filter and query capabilities

Data manipulation techniques

Identifying patterns and anomalies

DEMO: THREAT HUNTING WITH ZUI

Live demonstration of ZUI interface

Analyzing sample data sets

Identifying potential threats

CONCLUSION

Recap of key points:

- Importance of threat hunting
- Zeek and Suricata command line analysis
- Introduction to ZUI for data exploration

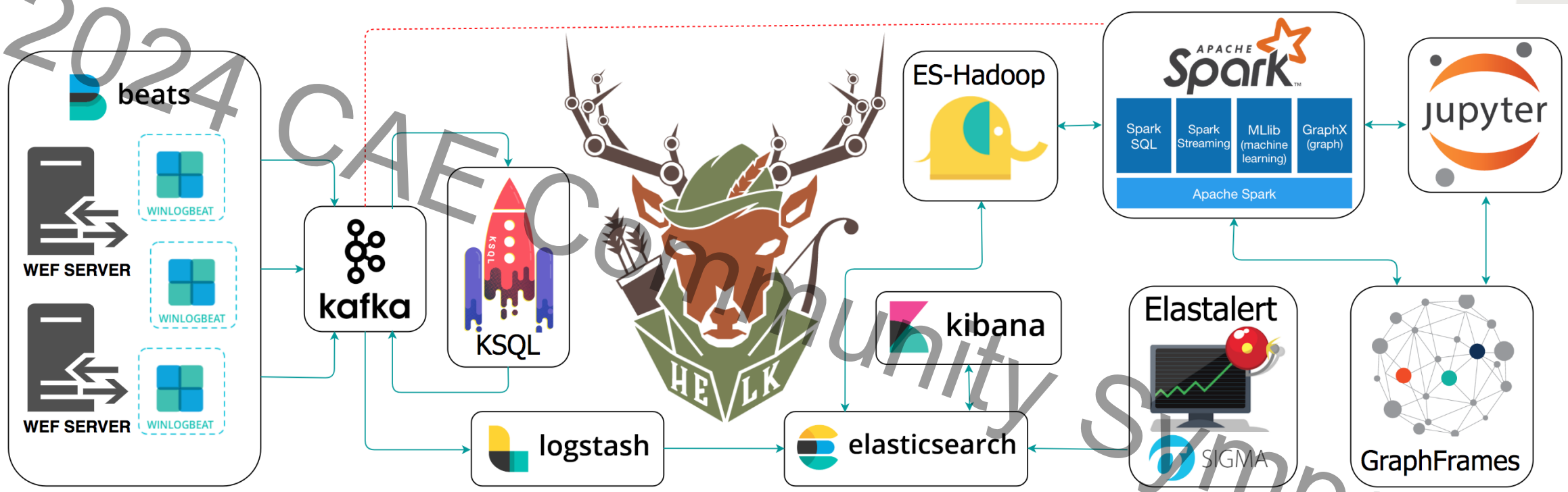
Encouragement to explore further:

- Practice Zeek and Suricata command line analysis
- Explore ZUI for advanced threat hunting techniques

2024 CAE Community Symposium

Q & A

OPEN-SOURCE THREAT HUNTING PLATFORM



An open-source Hunting Elastic Stack (HELK) is used as a central data analytics tool. The outputs of the HELK feed hunting trigger phase. In this project, HELK is used to monitor network traffic and device logs, detect anomalies and their correlated components, detect MITRE ATT&CK TTPS, and trigger the threat hunting phase.

https://github.com/Cyb3rWard0g/HELK?ref=fr33s0ul.tech