

# INTRODUCTION TO THREAT HUNTING WITH ZUI



Deep Ramanayake  
Xavier University



**CAE**  
IN CYBERSECURITY  
COMMUNITY

# AGENDA

2024 CAE Community Symposium

Introduction to Threat Hunting



Zeek and Suricata Command Line Analysis



ZUI: Graphical User Interface for Data Exploration



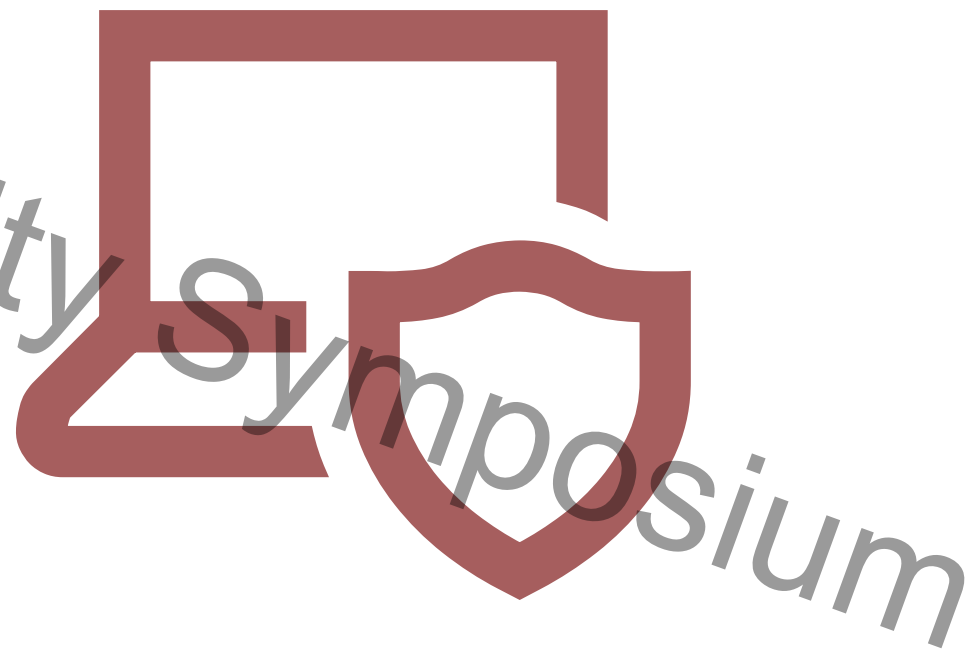
ZUI Walkthrough



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



# 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

2024 CAE Community Symposium

# 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

ery View Window Help



Welcome to Zui



week 14



logana1



FROM testpool

1

TABLE INSPECTOR

204

02:15

24 Shapes — Filter to one shape or [fuse](#) results to view as a table.

```
> {_path: conn, ts: 2014-11-16T02:12:12.4775752, uid: "Cdw  
> {_path: conn, ts: 2014-11-16T02:12:12.4772712, uid: "Cj0  
> {_path: files, ts: 2014-11-16T02:12:11.9712382, fuid: "F  
> {_path: conn, ts: 2014-11-16T02:12:11.9580142, uid: "CAC  
> {_path: dns, ts: 2014-11-16T02:12:11.9580142, uid: "CAC4  
> {_path: http, ts: 2014-11-16T02:12:11.9555522, uid: "C2c  
> {_path: files, ts: 2014-11-16T02:12:11.9515992, fuid: "F  
> {_path: notice, ts: 2014-11-16T02:12:11.1195532, uid: "C  
> {_path: http, ts: 2014-11-16T02:12:11.1121672, uid: "C2c  
> {_path: http, ts: 2014-11-16T02:12:11.1120642, uid: "Cub  
> {_path: x509, ts: 2014-11-16T02:12:10.6796272, fingerprint
```

# ZUI WALKTHROUGH - PART 1



Accessing ZUI interface



Overview of main components:

Search Bar  
Data Panels



Importing data into ZUI

2024 CAE Community Symposium

2024

# EXPLORING DATA USING ZUI:



Filter and query capabilities



Data manipulation techniques



Identifying patterns and anomalies

CAE Community Symposium

# DEMO: THREAT HUNTING WITH ZUI

Live demonstration of ZUI  
interface



Analyzing sample data sets



Identifying potential threats

2024

CAE

Community

Symposium



# CONCLUSION

2024 CAE Community Symposium

Recap of key points:

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

Encouragement to explore further:

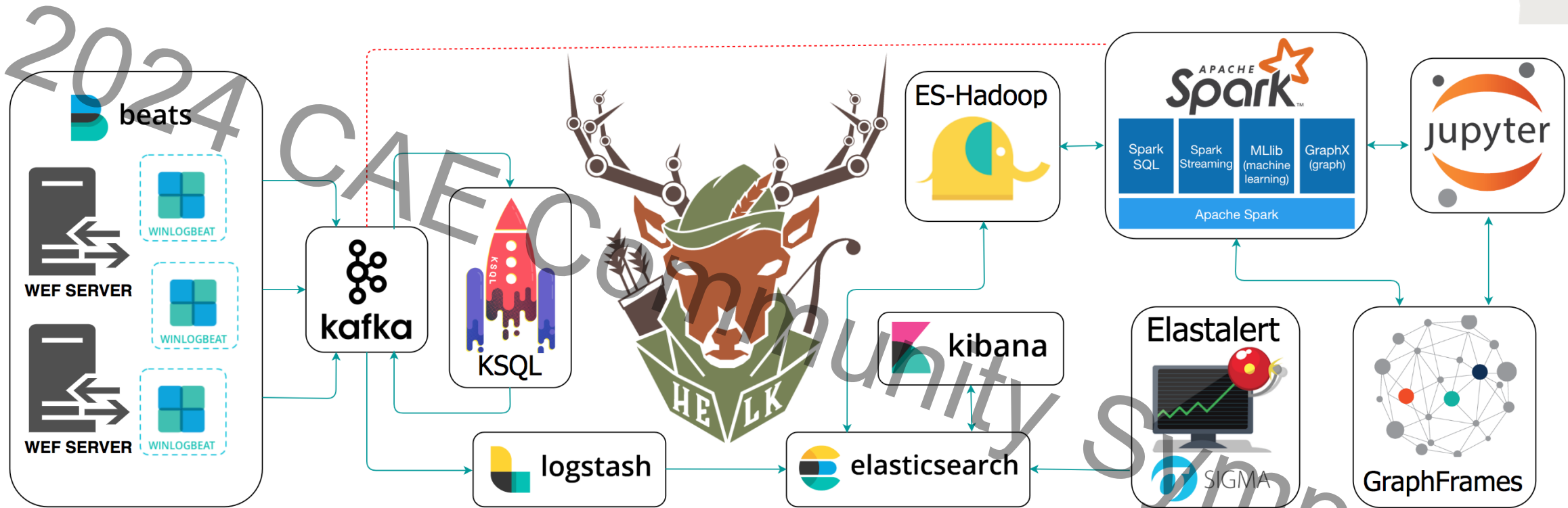
Practice Zeek and Suricata command line analysis  
Explore ZUI for advanced threat hunting techniques

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>