A Testbed for Operations in the Information Environment

CSET 2024, August 13, 2024

Presented by: Adam Tse

Authors: Adam Tse, Swaroop Vattam, Vincent Ercolani, Douglas Stetson, and Mary Ellen Zurko

LINCOLN LABORATORY
MASSACHUSETTS INSTITUTE OF TECHNOLOGY

The Need for Enhanced Execution of Operations in the Information Environment (OIE)

U.S. Department *of* Defense

2022

National Defense Strategy

of

The United States of America

Including the 2022 Nuclear Posture Review and the 2022 Missile Defense Review

“To strengthen deterrence while managing escalation risks, the Department will enhance its ability to operate in the information domain – for example, by working to ensure its messages are conveyed effectively.”

“Emerging technologies and applications are making [competitors’ gray zone] activities more effective at building their military and non-military advantages which, if left unaddressed, could endanger U.S. military effectiveness now and in the future.”

DoD strategy emphasizes the importance of ensuring effective execution of OIE with emerging technologies

Cyber Security vs Information Environment Testbeds

[1]

NICE | community coordinating council

THE CYBER RANGE

A GUIDE

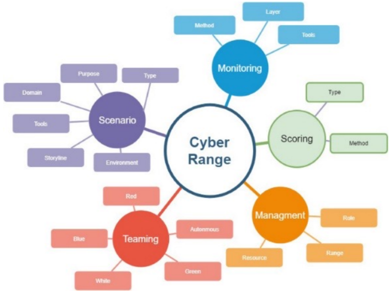
Guidance Document for the Use Cases, Features, and Types of Cyber Ranges in Cybersecurity Education, Certification, and Training

Prepared by the Cyber Range Project Team and the NICE Community Coordinating Council, Cybersecurity Skills Competitions Community of Interest

September 2023

NIST: Cyber Range Guidance

[2]



Cyber Security Range Components

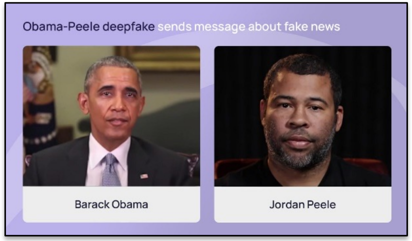
Cyber Security

- Mature, proven field with guidance from NIST and underlying standards for the technology being simulated
- Different degrees in emulation for networks, servers, storage, traffic, and attacks
- Ability to redeploy environments quickly and enable rigorous/repeated testing

Task Force 46 / C2CRE-B
CYBER IMPACT 2022
Multi-domain Operations Cyber Effects on Homeland Defense DSCA/CBRN Response

Table-Top Exercises (TTX)

[3]



Obama-Peele deepfake sends message about fake news

Barack Obama

Jordan Peele

ML Models Applied to OIE

Information Environment

- Exercises are tailored to strategic decision makers, not individual operators
- Little focus on monitoring IE technology performance
- Evaluation limited to general, qualitative observation
- Limited capabilities at simulating IE operators experience in operations

Lessons learned from cyber security testbeds can be applied to testbeds in the information environment

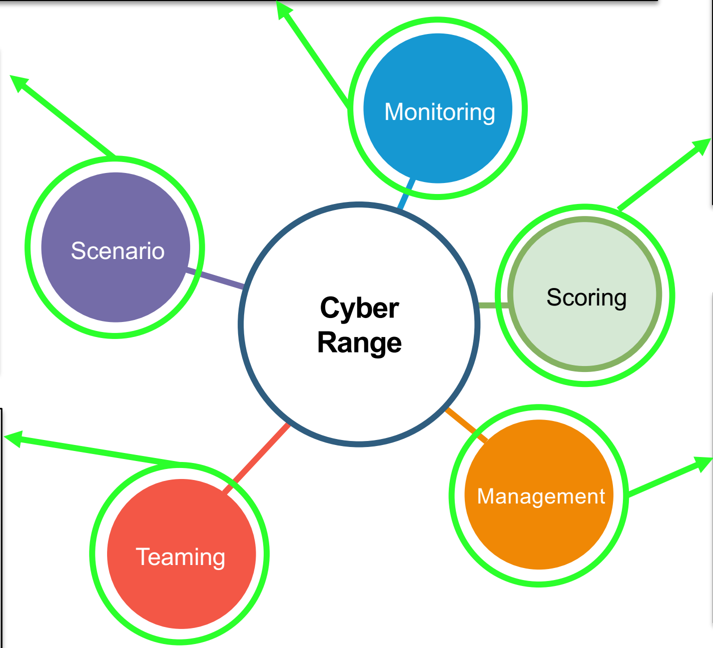
[1] https://www.nist.gov/system/files/documents/2023/09/29/The%20Cyber%20Range_A%20Guide.pdf
[2] Yamin, Muhammad Mudassar, Basel Katt, and Vasileios Gkioulos. "Cyber ranges and security testbeds: Scenarios, functions, tools and architecture." Computers & Security 88 (2020): 101636.
[3] https://sosafe-awareness.com/blog/how-to-spot-a-deepfake/

NIST: National Institute of Standards and Technology
IE: Information Environment

Components of an Information Environment Testbed

Monitoring
- Observer live monitoring and note taking
- Automated recording of operator actions
- Intermediate metrics summarizing user actions

Scenario
- Storylines
- Networks
- Hosts
- Servers
- Data feeds
- Threats



Scoring
- Completion of objectives
- Qualitative feedback on participant workflow and understanding
- Progress metrics for operators reaching objectives
- Technical metrics for how efficiently objectives are reached

Teaming
- Offense
- Defense
- Observers
- Management

Management
- Running and testing of exercise provided participant tools
- Tools for diagnosing status of monitoring capabilities
- Tools for diagnosing status of exercise provided computer resources provided to participants

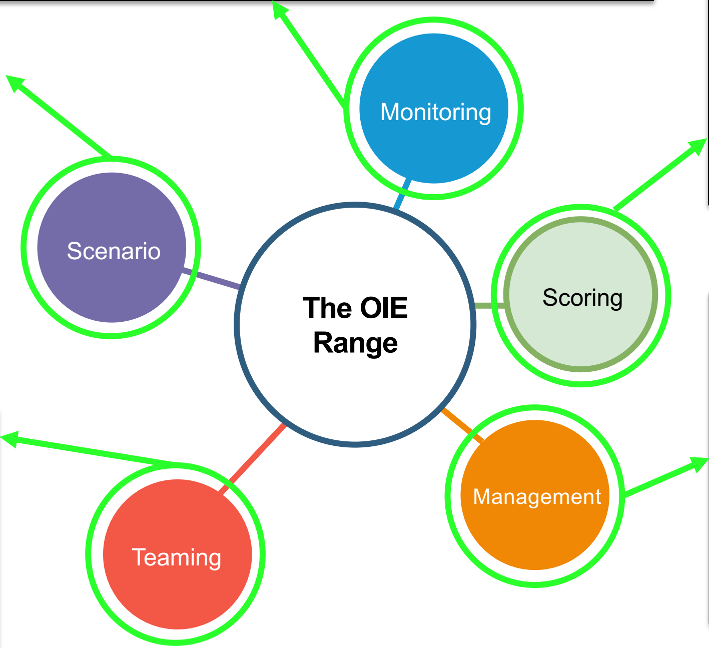
Yamin, Muhammad Mudassar, Basel Katt, and Vasileios Gkioulos. "Cyber ranges and security testbeds: Scenarios, functions, tools and architecture." *Computers & Security* 88 (2020): 101636.

Components of an Information Environment Testbed

Monitoring
- Observer live monitoring and note taking
- Automated recording of operator actions
- Intermediate metrics summarizing user actions

Scenario
- Narratives
- Social media platforms
- News outlets
- Algorithms for recommending content
- Civilian behavior
- Adversary content

Teaming
- Participants
- Observers
- Management
- Adversary
- Simulated Civilians



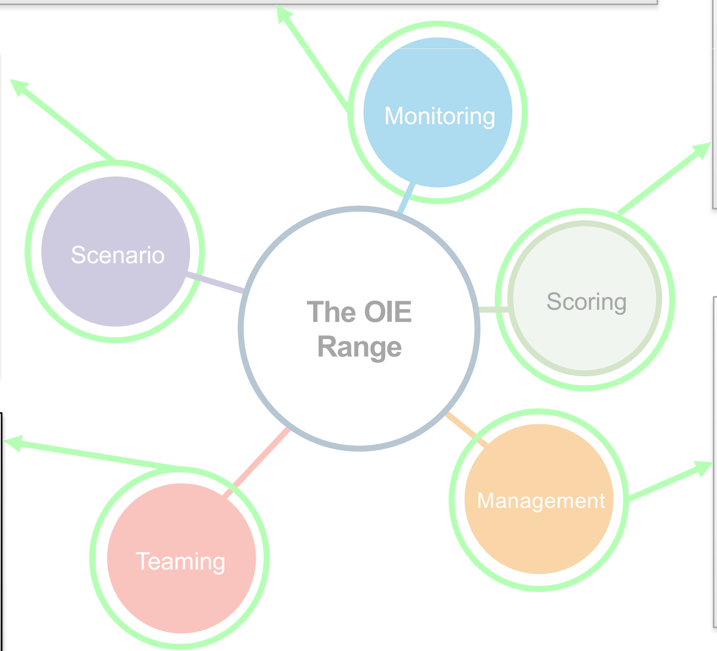
Scoring
- Completion of objectives
- Qualitative feedback on participant workflow and understanding
- Progress metrics for operators reaching objectives
- Technical metrics for how efficiently objectives are reached

Management
- Running and testing of exercise provided participant tools
- Tools for diagnosing status of monitoring capabilities
- Tools for diagnosing status of exercise provided computer resources provided to participants

Yamin, Muhammad Mudassar, Basel Katt, and Vasileios Gkioulos. "Cyber ranges and security testbeds: Scenarios, functions, tools and architecture." *Computers & Security* 88 (2020): 101636.

OIE: Operations in the Information Envrionment

Components of an Information Environment Testbed



Monitoring
- Observer live monitoring and note taking
- Automated recording of operator actions
- Intermediate metrics summarizing user actions

Scenario
- Narratives
- Social media platforms
- News outlets
- Algorithms for recommending content
- Civilian behavior
- Adversary content

Teaming
- Participants
- Observers
- Management
- Adversary
- Simulated Civilians

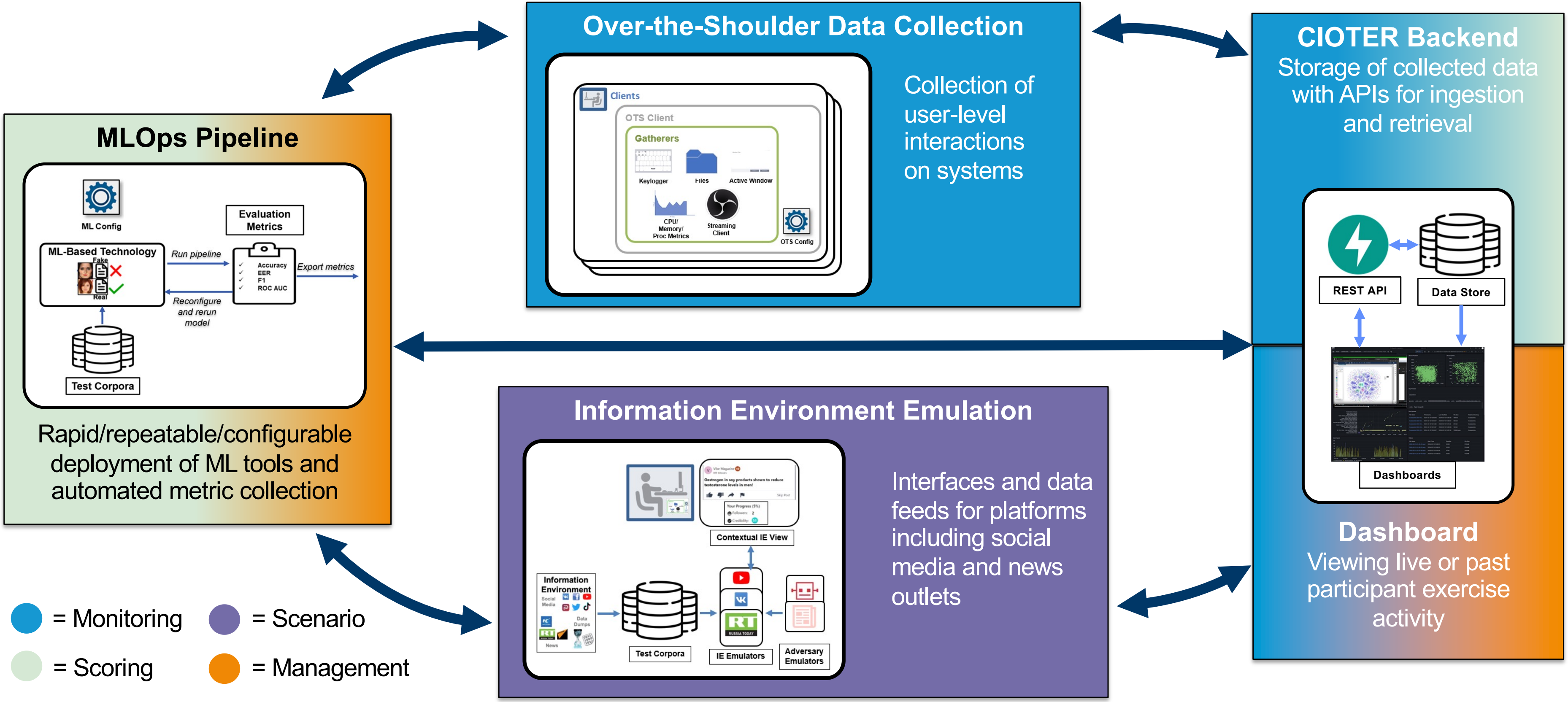
Scoring
- Completion of objectives
- Qualitative feedback on participant workflow and understanding
- Progress metrics for operators reaching objectives
- Technical metrics for how efficiently objectives are reached

Management
- Running and testing of exercise provided participant tools
- Tools for diagnosing status of monitoring capabilities
- Tools for diagnosing status of exercise provided computer resources provided to participants

Yamin, Muhammad Mudassar, Basel Katt, and Vasileios Gkioulos. "Cyber ranges and security testbeds: Scenarios, functions, tools and architecture." *Computers & Security* 88 (2020): 101636.

OIE: Operations in the Information Envrionment

Counter Influence Operations Test and Evaluation Range (CIOTER)



Over-the-Shoulder Data Collection

Collection of user-level interactions on systems

CIOTER Backend

Storage of collected data with APIs for ingestion and retrieval

Dashboard

Viewing live or past participant exercise activity

MLOps Pipeline

Rapid/repeatable/configurable deployment of ML tools and automated metric collection

Information Environment Emulation

Interfaces and data feeds for platforms including social media and news outlets

● = Monitoring

● = Scenario

● = Scoring

● = Management

MLOps: Machine Learning Operations
API: Application Program Interface

Machine Learning Operations Pipeline

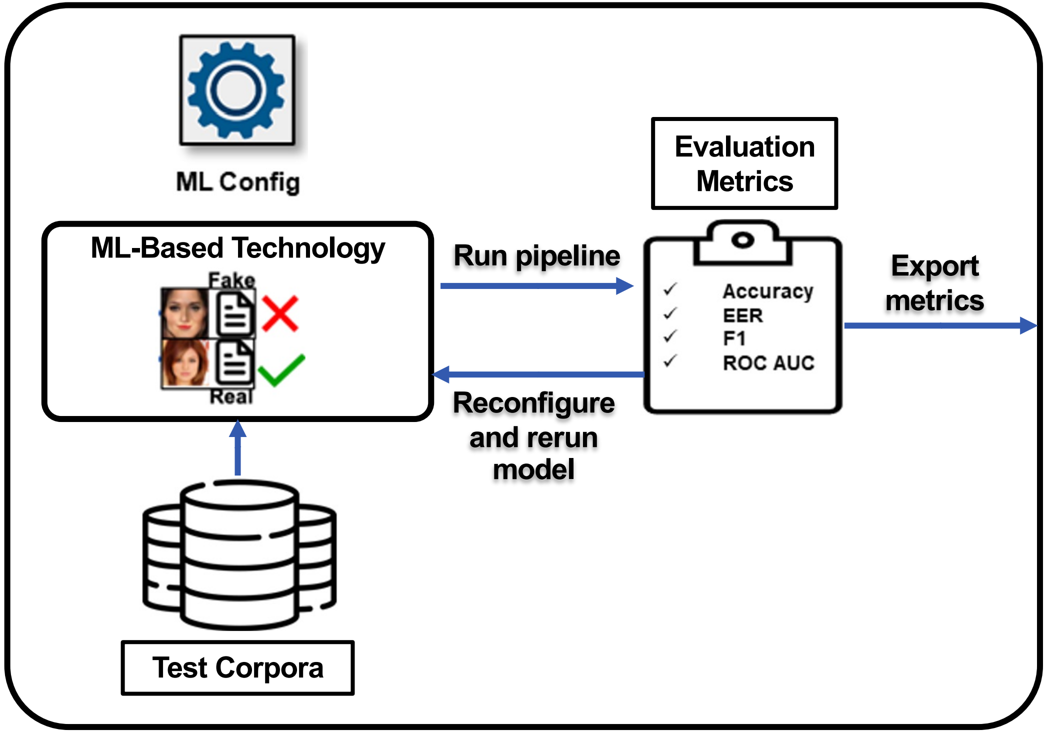
Scoring/Management

- **Enables rapid deployment, configuration, assessment of ML based tools**
- **Includes implementations of suite of common ML processes/metrics**
- **Easily extensible using well-defined interfaces**

MLOps Pipeline Steps

1. Package ML Tool into containerized SUT
2. Configure ML pipeline parameters, test corpora, jobs to run
3. Run the ML pipeline
4. Generate metrics into output
5. Write to CIOTER backend

MLOps Pipeline



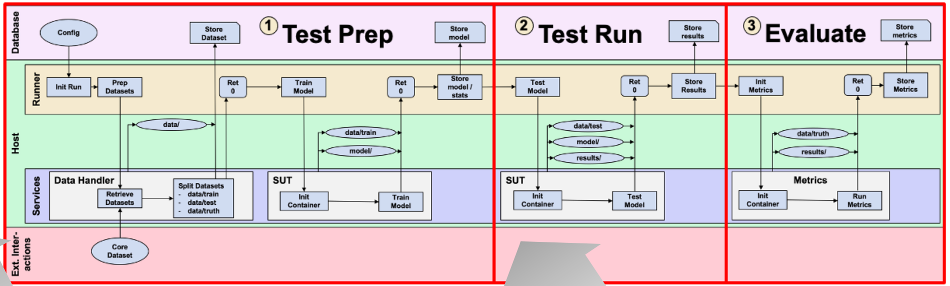
SUT: System under test
ML: Machine learning

EER: Equal error rate
ROC AUC: Area under the receiver operating characteristic curve

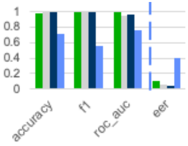
MLOps Demonstration

Scoring/Management

Dataset Storage



24 Metrics



Test Plan

- ✓ Accuracy
- ✓ EER
- ✓ F1
- ✓ ROC AUC

12 Datasets

17 Test Runs

	Smoke Test	Evaluation
Same Author?	PAN Challenge Amazon reviews Twitter 1 Twitter 2	Reddit dataset Mastodon dataset Yelp dataset
Deepfake Detection	Faceforensics++ GoogleDFD CelebDF	Real Fake Face Diverse Fake Face

Two Tasks, Three SUTs

Same Author?

Transformer cross-encoder model

Deepfake Detection

Xception-Net
Meso-Net

Automated testing of AI OIE tools, enabling rapid iteration of tests with varied data and parameters allows rapid convergence to effective solutions

SUT: System under test
AI: Artificial Intelligence
OIE: Operations in the Information Environment

EER: Equal error rate
ROC AUC: Area under the receiver operating characteristic curve

MLOps Lessons Learned

Scoring/Management

Standardized APIs and Containers

- Containerizing SUTs enable rapid deployment and running of tools
- Can be integrated into early development of ML systems to improve models quicker

Configuration and Automation

- Varied execution modes enabled by centralization
- Large suite of configuration options
- Enables rapid “plug-and-play” assessment of ML systems

Altered Adversarial Model

- Allows ability to detect if models can keep up with evolving attack techniques
- Proven on testing models’ performance on deep fake data vs manually generated fake data

Edge Case Finding

- Rapid deployments detect issues early with new datasets
- Enabled discovery of unverified test cases with new data sets
- Ensures models are well-tested

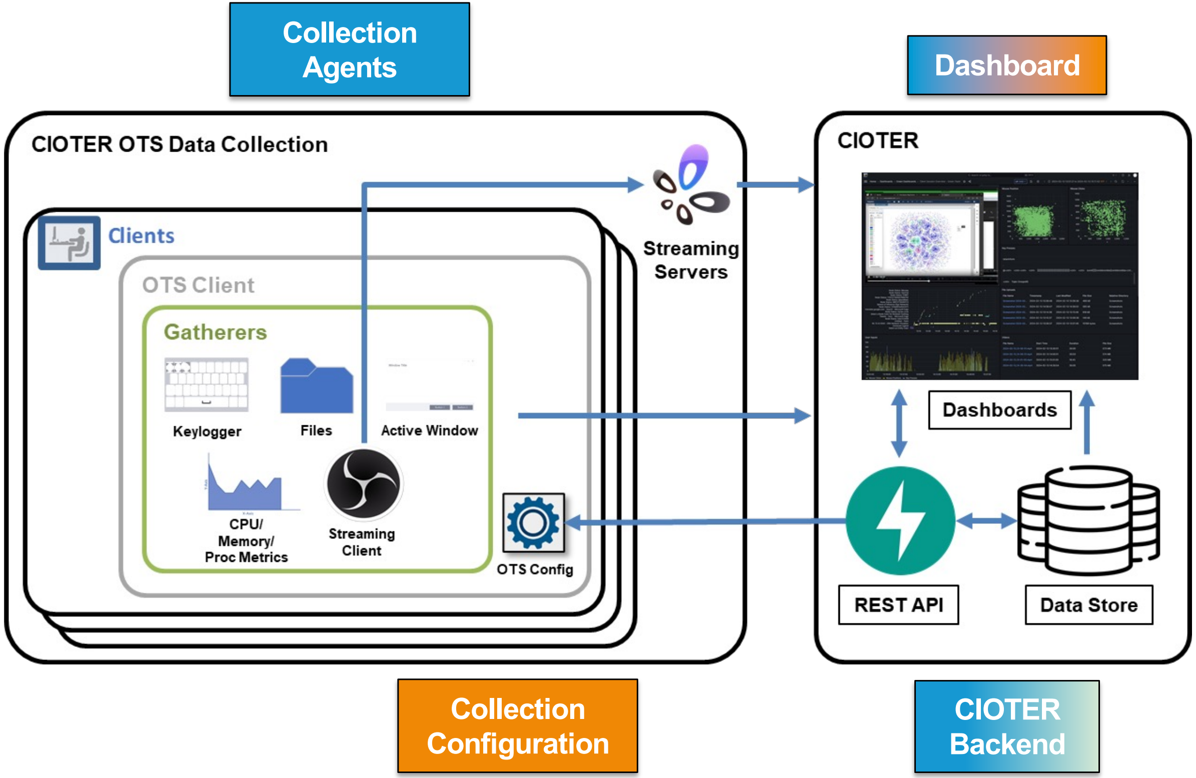
Data Storage and Reuse

- Storage of metrics, logs, and model artifacts
- Allow troubleshooting model
- Reuse of model artifacts save time in subsequent runs

ML: Machine Learning
SUT: System Under Test

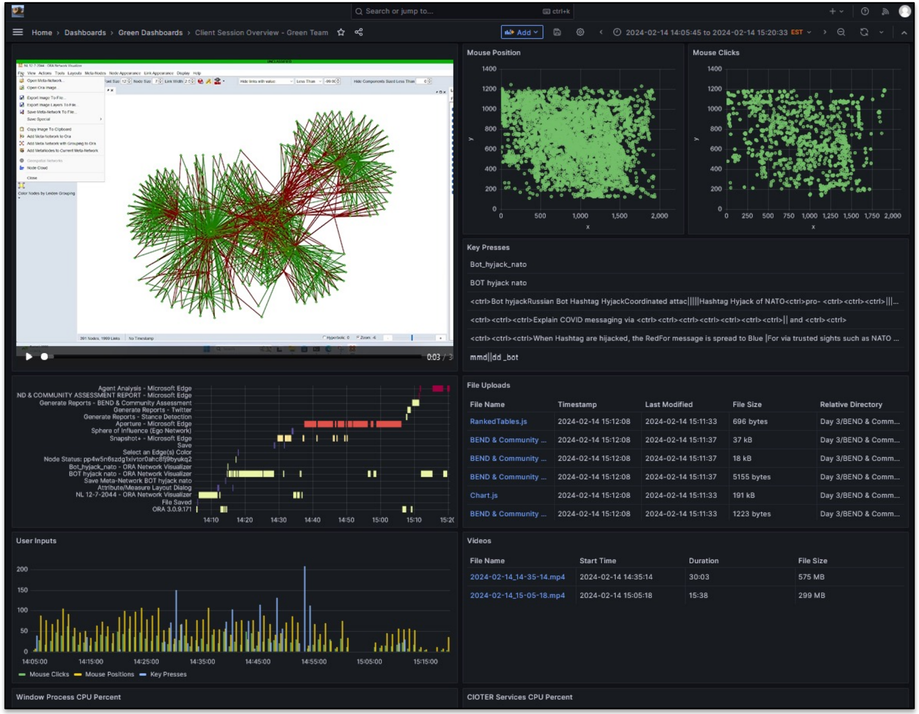
Over-the-Shoulder Monitoring

- Installed on participant machines
- Configurable parameters
- Gatherers for
  - Keylogging
  - Mouse Interactions
  - Files
  - Active Windows
  - CPU/Memory/Proc specs
  - Streaming/Video Recording



CIOTER: Counter Influence Operations Test and Evaluation Range
OTS: Over-the-shoulder
API: Application Program Interface

Over-the-Shoulder Monitoring Metrics


Search or jump to...
ctrl+k
Home › Dashboards › Green Dashboards › Client Session Overview - Green Team
Add
2024-02-14 14:05:45 to 2024-02-14 15:20:33 EST
Mouse Position
Mouse Clicks
1400
1200
1000
800
600
400
200
0
y
x
0
250
500
750
1,000
1,250
1,500
1,750
2,000
391 Nodes, 1999 Links
No Timestamp
Hyperbolic: 0
Zoom: -6
0:03 / 3
Agent Analysis - Microsoft Edge
ND & COMMUNITY ASSESSMENT REPORT - Microsoft Edge
Generate Reports - BEND & Community Assessment
Generate Reports - Twitter
Generate Reports - Stance Detection
Aperture - Microsoft Edge
Sphere of Influence (Ego Network)
Snapshot+ - Microsoft Edge
Save
Select an Edge(s) Color
Node Status: pp4w5n6szdg1xivtor0ahc8fj9byukq2
Bot_hyjack_nato - ORA Network Visualizer
BOT hyjack nato - ORA Network Visualizer
Save Meta-Network BOT hyjack nato
Attribute/Measure Layout Dialog
NL 12-7-2044 - ORA Network Visualizer
File Saved
ORA 3.0.9.171
14:10
14:20
14:30
14:40
14:50
15:00
15:10
15:20
User Inputs
200
150
100
50
0
14:05:00
14:15:00
14:25:00
14:35:00
14:45:00
14:55:00
15:05:00
15:15:00
Mouse Clicks
Mouse Positions
Key Presses
Window Process CPU Percent
CIOTER Services CPU Percent

Key Presses

```
Bot_hyjack_nato
BOT hyjack nato
<ctrl>Bot hyjackRussian Bot Hashtag HyjackCoordinated attac|||||Hashtag Hyjack of NATO<ctrl>pro- <ctrl><ctrl><ctrl>|||...
<ctrl><ctrl><ctrl>Explain COVID messaging via <ctrl><ctrl><ctrl><ctrl><ctrl><ctrl><ctrl>|| and <ctrl><ctrl>
<ctrl><ctrl><ctrl>When Hashtag are hijacked, the RedFor message is spread to Blue |For via trusted sights such as NATO ...
mmd||dd _bot
```

File Uploads

File Name	Timestamp	Last Modified	File Size	Relative Directory
RankedTables.js	2024-02-14 15:12:08	2024-02-14 15:11:33	696 bytes	Day 3/BEND & Comm...
BEND & Community ...	2024-02-14 15:12:08	2024-02-14 15:11:37	37 kB	Day 3/BEND & Comm...
BEND & Community ...	2024-02-14 15:12:08	2024-02-14 15:11:37	18 kB	Day 3/BEND & Comm...
BEND & Community ...	2024-02-14 15:12:08	2024-02-14 15:11:37	5155 bytes	Day 3/BEND & Comm...
Chart.js	2024-02-14 15:12:08	2024-02-14 15:11:33	191 kB	Day 3/BEND & Comm...
BEND & Community ...	2024-02-14 15:12:08	2024-02-14 15:11:33	1223 bytes	Day 3/BEND & Comm...

Videos

File Name	Start Time	Duration	File Size
2024-02-14_14-35-14.mp4	2024-02-14 14:35:14	30:03	575 MB
2024-02-14_15-05-18.mp4	2024-02-14 15:05:18	15:38	299 MB

Low-Level Actions

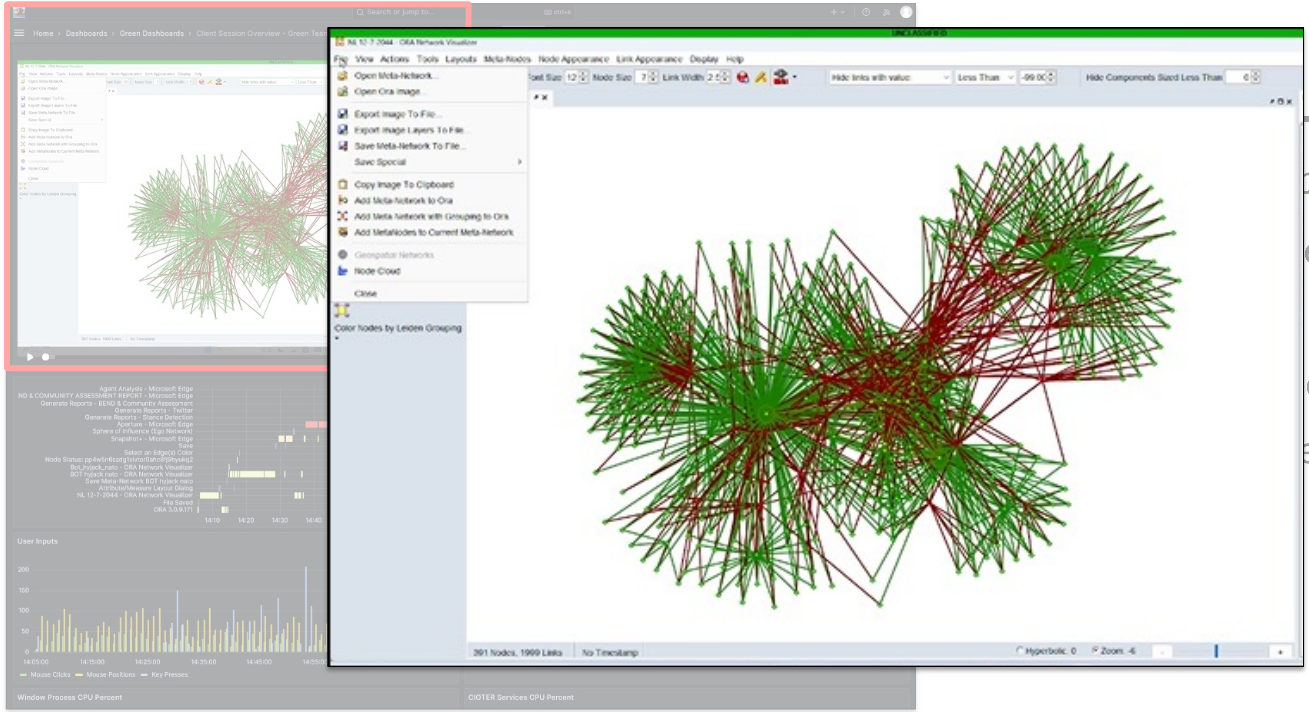
*What are participants **doing**?*

- Mouse Clicks/Movement
- Keypresses
- Active Window Titles
- Livestreaming/Video

Collection of low level actions reveals participant workflows that can be evaluated

Over-the-Shoulder Monitoring Metrics

MGMT/Monitoring/Scoring


Home › Dashboards › Green Dashboards › Client Session Overview - Green Team
NL 12-7-2044 - ORA Network Visualizer
UNCLASSIFIED
File View Actions Tools Layouts Meta-Nodes Node Appearance Link Appearance Display Help
Open Meta-Network...
Open Ora image
Export Image To File...
Export Image Layers To File...
Save Meta-Network To File...
Save Special
Copy Image To Clipboard
Add Meta-Network to Ora
Add Meta Network with Grouping to Ora
Add MetaNodes to Current Meta-Network
Geospatial Networks
Node Cloud
Close
Color Nodes by Leiden Grouping
Font Size 12 Node Size 7 Link Width 2.5
Hide links with value Less Than -99.00
Hide Components Sized Less Than 0
391 Nodes, 1999 Links
No Timestamp
Hyperbolic 0
Zoom -6
Agent Analysis - Microsoft Edge
ND & COMMUNITY ASSESSMENT REPORT - Microsoft Edge
Generate Reports - BEND & Community Assessment
Generate Reports - Twitter
Generate Reports - Stance Detection
Aperture - Microsoft Edge
Sphere of Influence (Ego Network)
Snapshot+ - Microsoft Edge
Save
Select an Edge(s) Color
Bot_hyjack_nato - ORA Network Visualizer
BOT hyjack nato - ORA Network Visualizer
Save Meta-Network BOT hyjack nato
Attribute/Measure Layout Dialog
NL 12-7-2044 - ORA Network Visualizer
File Saved
ORA 3.0.9.171
14:10
14:20
14:30
14:40
User Inputs
200
150
100
50
0
14:05:00
14:15:00
14:25:00
14:35:00
14:45:00
14:55:00
Mouse Clicks
Mouse Positions
Key Presses
Window Process CPU Percent
CIOTER Services CPU Percent

Level Actions

participants **doing**?

ement

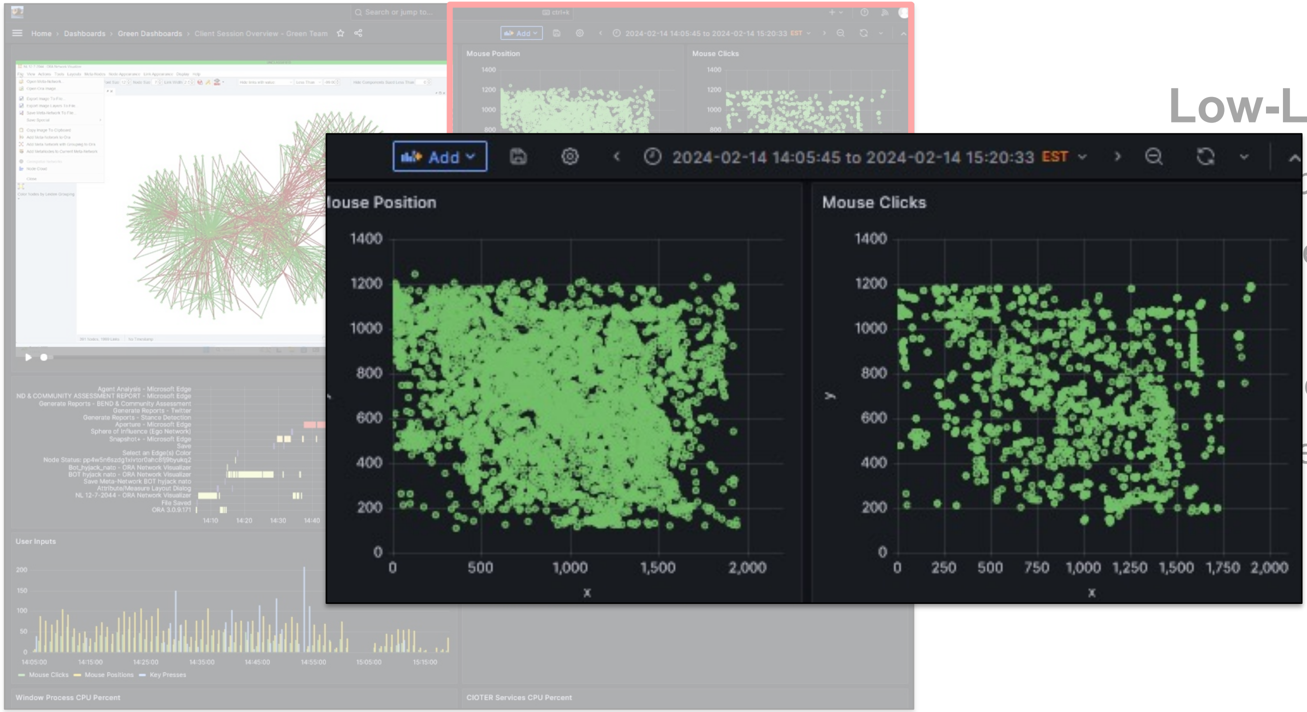
es

eo

Collection of low level actions reveals participant workflows that can be evaluated

Over-the-Shoulder Monitoring Metrics

MGMT/Monitoring/Scoring



Home › Dashboards › Green Dashboards › Client Session Overview - Green Team
Search or jump to...
Add
2024-02-14 14:05:45 to 2024-02-14 15:20:33 EST
Mouse Position
Mouse Clicks
1400
1200
1000
800
600
400
200
0
500
1,000
1,500
2,000
250
750
1,250
1,750
x
y
Agent Analysis - Microsoft Edge
ND & COMMUNITY ASSESSMENT REPORT - Microsoft Edge
Generate Reports - BEND & Community Assessment
Generate Reports - Twitter
Generate Reports - Stance Detection
Aperture - Microsoft Edge
Sphere of Influence (Ego Network)
Snapshot+ - Microsoft Edge
Save
Select an Edge(s) Color
Node Status: pp4w5n6szdg1xivtor0ahc8fj9byukq2
Bot_hyjack_nato - ORA Network Visualizer
BOT hyjack nato - ORA Network Visualizer
Save Meta-Network BOT hyjack nato
Attribute/Measure Layout Dialog
NL 12-7-2044 - ORA Network Visualizer
File Saved
ORA 3.0.9.171
14:10
14:20
14:30
14:40
User Inputs
200
150
100
50
0
14:05:00
14:15:00
14:25:00
14:35:00
14:45:00
14:55:00
15:05:00
15:15:00
Mouse Clicks
Mouse Positions
Key Presses
Window Process CPU Percent
CIOTER Services CPU Percent

Low-Level Actions

participants *doing*?

ement

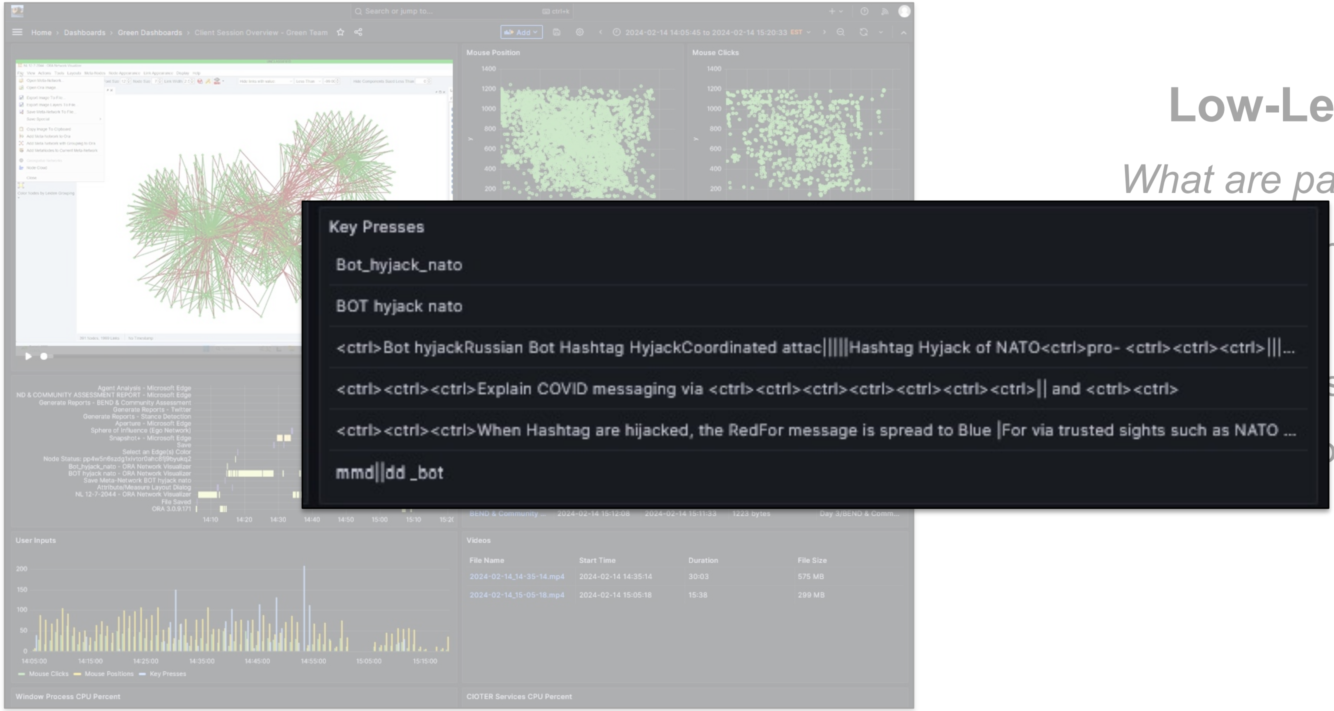
es

eo

Collection of low level actions reveals participant workflows that can be evaluated

Over-the-Shoulder Monitoring Metrics

MGMT/Monitoring/Scoring


Home › Dashboards › Green Dashboards › Client Session Overview - Green Team
2024-02-14 14:05:45 to 2024-02-14 15:20:33 EST
Mouse Position
Mouse Clicks
1400
1200
1000
800
600
400
200
Agent Analysis - Microsoft Edge
ND & COMMUNITY ASSESSMENT REPORT - Microsoft Edge
Generate Reports - BEND & Community Assessment
Generate Reports - Twitter
Generate Reports - Stance Detection
Aperture - Microsoft Edge
Sphere of Influence (Ego Network)
Snapshot+ - Microsoft Edge
Save
Select an Edge(s) Color
Node Status: pp4w5n6szdg1xivtor0ahc8fj9byukq2
Bot_hyjack_nato - ORA Network Visualizer
BOT hyjack nato - ORA Network Visualizer
Save Meta-Network BOT hyjack nato
Attribute/Measure Layout Dialog
NL 12-7-2044 - ORA Network Visualizer
File Saved
ORA 3.0.9.171
14:10
14:20
14:30
14:40
14:50
15:00
15:10
15:2(
User Inputs
200
150
100
50
0
14:05:00
14:15:00
14:25:00
14:35:00
14:45:00
14:55:00
15:05:00
15:15:00
Mouse Clicks
Mouse Positions
Key Presses
Window Process CPU Percent
CIOTER Services CPU Percent

Key Presses

Bot_hyjack_nato

BOT hyjack nato

<ctrl>Bot hyjackRussian Bot Hashtag HyjackCoordinated attac||||||Hashtag Hyjack of NATO<ctrl>pro- <ctrl><ctrl><ctrl>|||...

<ctrl><ctrl><ctrl>Explain COVID messaging via <ctrl><ctrl><ctrl><ctrl><ctrl><ctrl><ctrl>|| and <ctrl><ctrl>

<ctrl><ctrl><ctrl>When Hashtag are hijacked, the RedFor message is spread to Blue |For via trusted sights such as NATO ...

mmd||dd _bot

BEND & Community ...	2024-02-14 15:12:08	2024-02-14 15:11:33	1223 bytes	Day 3/BEND & Comm...

Videos

File Name	Start Time	Duration	File Size
2024-02-14_14-35-14.mp4	2024-02-14 14:35:14	30:03	575 MB
2024-02-14_15-05-18.mp4	2024-02-14 15:05:18	15:38	299 MB

Low-Level Actions

*What are participants **doing**?*

ment

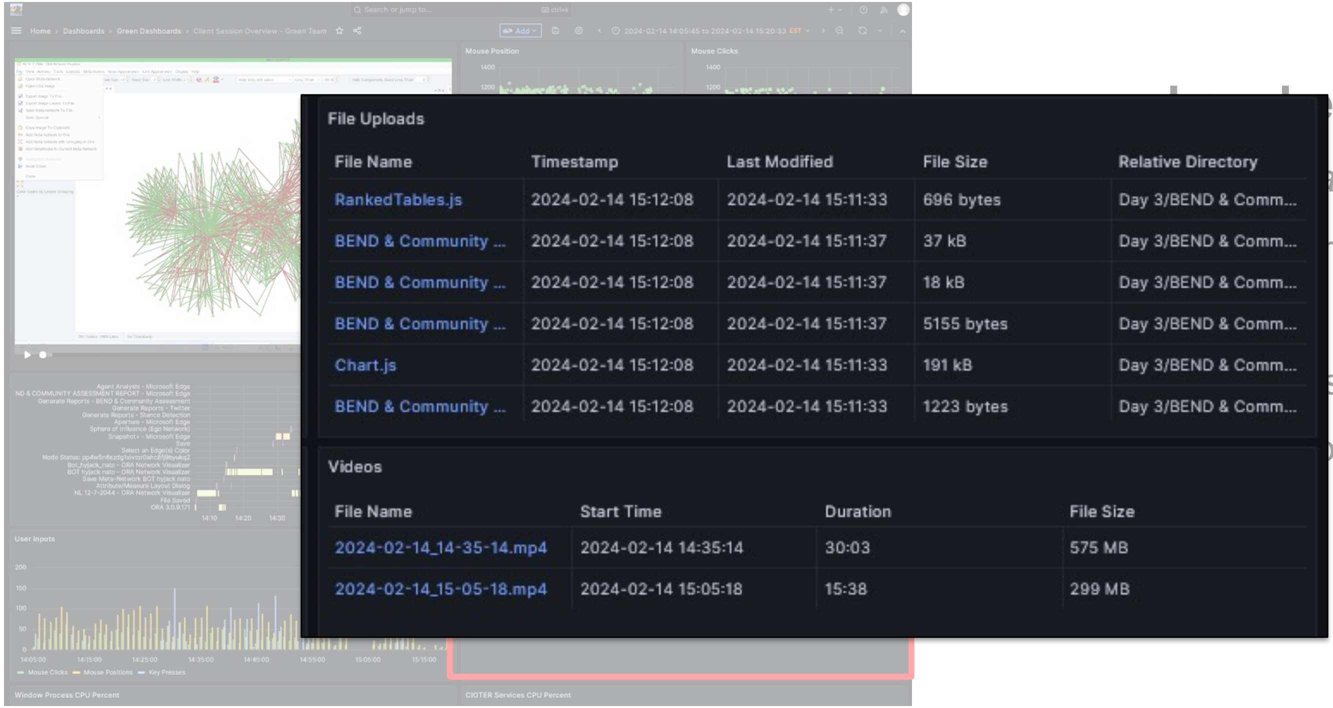
s

o

Collection of low level actions reveals participant workflows that can be evaluated

Over-the-Shoulder Monitoring Metrics

MGMT/Monitoring/Scoring


Home › Dashboards › Green Dashboards › Client Session Overview - Green Team
2024-02-14 14:05:45 to 2024-02-14 15:20:33 EST
Mouse Position
Mouse Clicks
User Inputs
Mouse Clicks
Mouse Positions
Key Presses
Window Process CPU Percent
CIOTER Services CPU Percent

File Uploads

File Name	Timestamp	Last Modified	File Size	Relative Directory
RankedTables.js	2024-02-14 15:12:08	2024-02-14 15:11:33	696 bytes	Day 3/BEND & Comm...
BEND & Community ...	2024-02-14 15:12:08	2024-02-14 15:11:37	37 kB	Day 3/BEND & Comm...
BEND & Community ...	2024-02-14 15:12:08	2024-02-14 15:11:37	18 kB	Day 3/BEND & Comm...
BEND & Community ...	2024-02-14 15:12:08	2024-02-14 15:11:37	5155 bytes	Day 3/BEND & Comm...
Chart.js	2024-02-14 15:12:08	2024-02-14 15:11:33	191 kB	Day 3/BEND & Comm...
BEND & Community ...	2024-02-14 15:12:08	2024-02-14 15:11:33	1223 bytes	Day 3/BEND & Comm...

Videos

File Name	Start Time	Duration	File Size
2024-02-14_14-35-14.mp4	2024-02-14 14:35:14	30:03	575 MB
2024-02-14_15-05-18.mp4	2024-02-14 15:05:18	15:38	299 MB

evel Actions

*articipants **doing**?*

ment

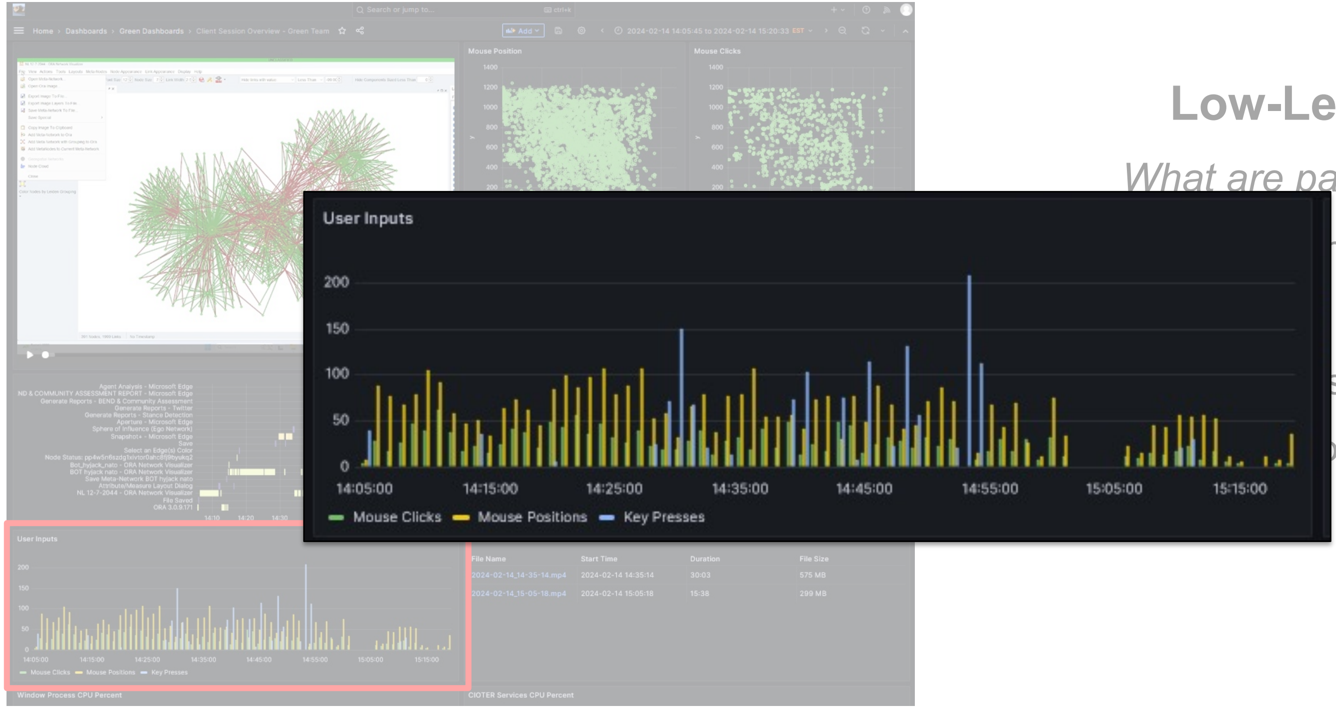
s

)

Collection of low level actions reveals participant workflows that can be evaluated

Over-the-Shoulder Monitoring Metrics

MGMT/Monitoring/Scoring


Search or jump to...
ctrl+k
Home › Dashboards › Green Dashboards › Client Session Overview - Green Team
Add
2024-02-14 14:05:45 to 2024-02-14 15:20:33 EST
Mouse Position
Mouse Clicks
1400
1200
1000
800
600
400
200
391 Nodes, 1999 Links
No Timestamp
Agent Analysis - Microsoft Edge
ND & COMMUNITY ASSESSMENT REPORT - Microsoft Edge
Generate Reports - BEND & Community Assessment
Generate Reports - Twitter
Generate Reports - Stance Detection
Aperture - Microsoft Edge
Sphere of Influence (Ego Network)
Snapshot+ - Microsoft Edge
Save
Select an Edge(s) Color
Node Status: pp4w5n6szdg1xivtor0ahc8fj9byukq2
Bot_hyjack_nato - ORA Network Visualizer
BOT hyjack nato - ORA Network Visualizer
Save Meta-Network BOT hyjack nato
Attribute/Measure Layout Dialog
NL 12-7-2044 - ORA Network Visualizer
File Saved
ORA 3.0.9.171
14:10
14:20
14:30
User Inputs
200
150
100
50
0
14:05:00
14:15:00
14:25:00
14:35:00
14:45:00
14:55:00
15:05:00
15:15:00
Mouse Clicks
Mouse Positions
Key Presses
Window Process CPU Percent
CIOTER Services CPU Percent

File Name	Start Time	Duration	File Size
2024-02-14_14-35-14.mp4	2024-02-14 14:35:14	30:03	575 MB
2024-02-14_15-05-18.mp4	2024-02-14 15:05:18	15:38	299 MB

Low-Level Actions

*What are participants **doing**?*

ment

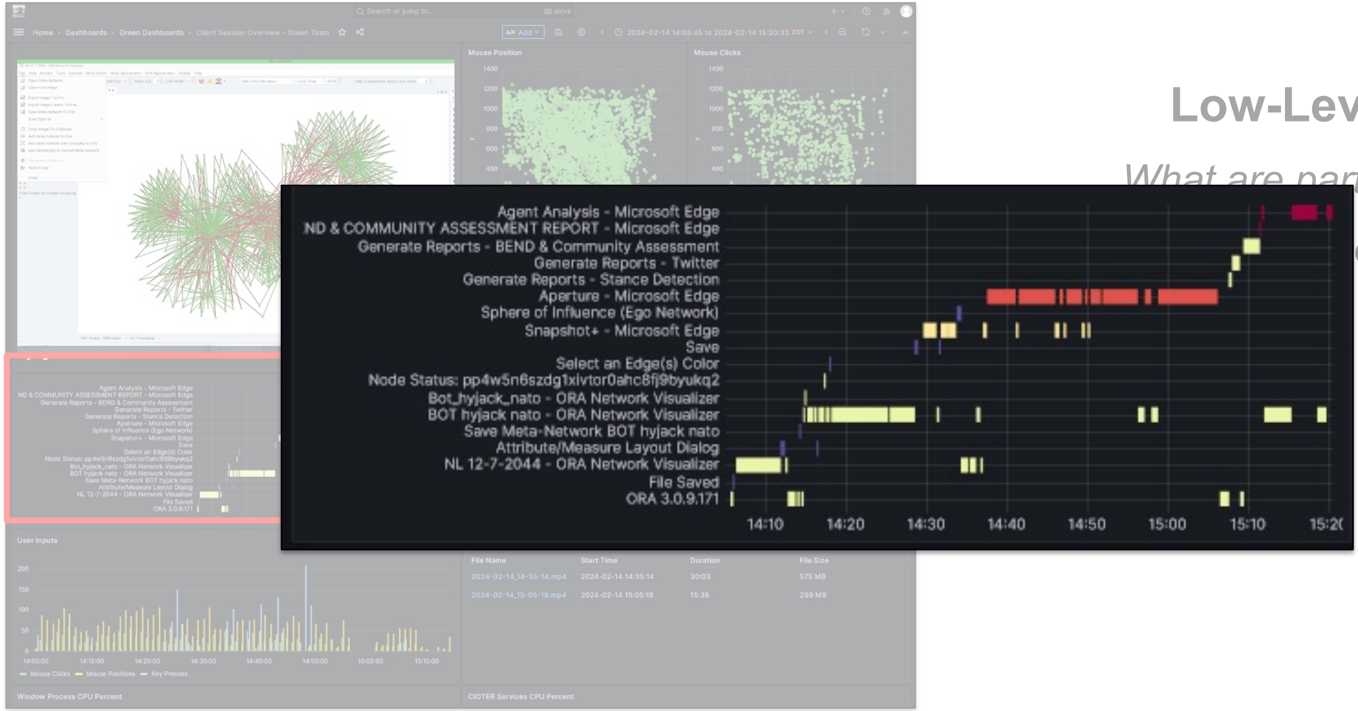
s

o

Collection of low level actions reveals participant workflows that can be evaluated

Over-the-Shoulder Monitoring Metrics

MGMT/Monitoring/Scoring


Search or jump to...
ctrl+k
Home › Dashboards › Green Dashboards › Client Session Overview - Green Team
Add
2024-02-14 14:05:45 to 2024-02-14 15:20:33 EST
Mouse Position
Mouse Clicks
1400
1200
1000
800
600
400
Agent Analysis - Microsoft Edge
ND & COMMUNITY ASSESSMENT REPORT - Microsoft Edge
Generate Reports - BEND & Community Assessment
Generate Reports - Twitter
Generate Reports - Stance Detection
Aperture - Microsoft Edge
Sphere of Influence (Ego Network)
Snapshot+ - Microsoft Edge
Save
Select an Edge(s) Color
Node Status: pp4w5n6szdg1xlvtor0ahc8fj9byukq2
Bot_hyjack_nato - ORA Network Visualizer
BOT hyjack nato - ORA Network Visualizer
Save Meta-Network BOT hyjack nato
Attribute/Measure Layout Dialog
NL 12-7-2044 - ORA Network Visualizer
File Saved
ORA 3.0.9.171
14:10
14:20
14:30
14:40
14:50
15:00
15:10
15:20
User Inputs
200
150
100
50
0
14:05:00
14:15:00
14:25:00
14:35:00
14:45:00
14:55:00
15:05:00
15:15:00
Mouse Clicks
Mouse Positions
Key Presses
Window Process CPU Percent
CIOTER Services CPU Percent

File Name	Start Time	Duration	File Size
2024-02-14_14-35-14.mp4	2024-02-14 14:35:14	30:03	575 MB
2024-02-14_15-05-18.mp4	2024-02-14 15:05:18	15:38	299 MB

Low-Level Actions

*What are participants **doing**?*

ent

Collection of low level actions reveals participant workflows that can be evaluated

Over-the-Shoulder Monitoring Metrics

MGMT/Monitoring/Scoring

Abstracting from Low-Level Actions

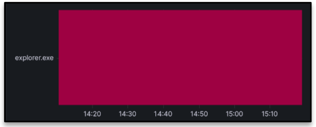
*What are participants **thinking**?*

Workflow Complexity Metrics

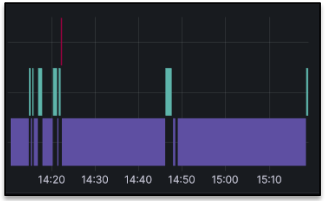
- **How complex is the distribution of active window switching during the workflow?**
- **Current metrics**
  - Workflow compression ratio (WCR)
  - Auto-correlation
  - Entropy

Workflow Distance Metrics

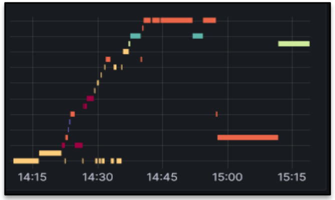
- **How do workflows of multiple participants differ?**
- **Current metrics**
  - Normalized Levenshtein distance
  - Jarowinkler distance
  - etc



Workflow Complexity Inactive User



Workflow Complexity of Scribe



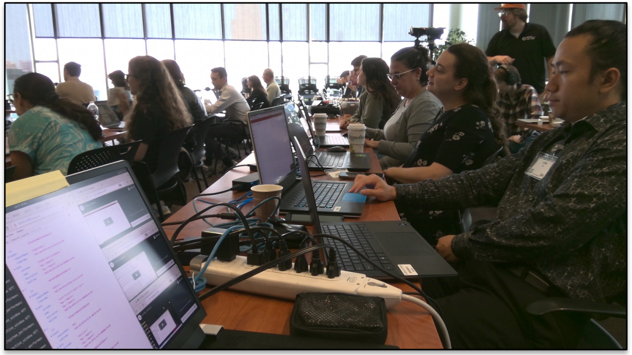
Workflow Complexity of Analyst

Extracting characteristics of workflows is the first step to analyzing workflows automatically

Over-the-Shoulder Demonstrations

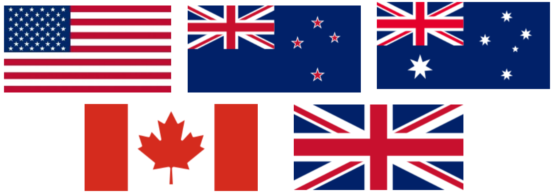
MGMT/Monitoring/Scoring

Tool Training Event



Piloted at training event for tool used at the OZ information warfare exercise

OZ Information Warfare Exercise



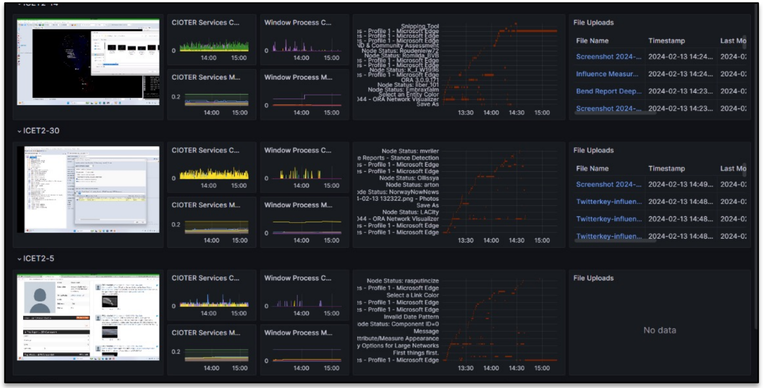
- Demonstration of new ways of working, with potential applicability to tactics, techniques and procedures
- 22 exercise participants in 4 teams across 5 countries
- Exercise roles included commander, public affairs office (PAO), and information analyst

OZ Information Warfare Exercise

MGMT/Monitoring/Scoring

Scenario — **Semi-synthetic dataset provided by exercise planners created from language generation technologies**

- **Participant goal to analyze data, brief findings, and recommend courses of action**
- **Participants were provided tools and taught workflows to analyze data**
- **CIOTER monitored all 22 participant machines through OTS Situational Awareness Dashboard**



File Uploads

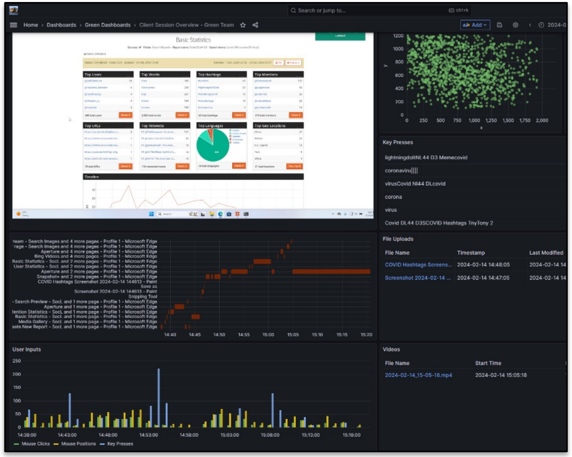
File Name	Timestamp	Last Mo
Screenshot 2024-...	2024-02-13 14:24...	2024-0:
Influence Measur...	2024-02-13 14:24...	2024-0:
Bend Report Deep...	2024-02-13 14:23...	2024-0:
Screenshot 2024-...	2024-02-13 14:23...	2024-0:

File Uploads

File Name	Timestamp	Last Mo
Screenshot 2024-...	2024-02-13 14:49...	2024-0:
Twitterkey-influen...	2024-02-13 14:48...	2024-0:
Twitterkey-influen...	2024-02-13 14:48...	2024-0:
Twitterkey-influen...	2024-02-13 14:48...	2024-0:

File Uploads

No data



Key Presses

lightningdoltNl.44 D3 Memecovid
coronaviru||||
virusCovid Nl44 DLcovid
corona
virus
Covid DL44 D3SCOVID Hashtags TnyTony 2

File Uploads

File Name	Timestamp	Last Modified
COVID Hashtags Screens...	2024-02-14 14:48:05	2024-02-14 14
Screenshot 2024-02-14 ...	2024-02-14 14:47:05	2024-02-14 14

Videos

File Name	Start Time
2024-02-14_15-05-18.mp4	2024-02-14 15:05:18

CIOTER: Counter Influence Operations Test and Evaluation Range
OTS: Over-the-shoulder

Over-the-Shoulder Lessons Learned

Monitoring/Scoring/MGMT

Flexible Deployment

- Containerized backend and packaged client collectors allowed rapid deployment on to exercise environment
- Minor network configurations for REST APIs, database, dashboard, client collector, and streaming

Distributed Architecture

- Video streaming requires a large amount of CPU and memory for the backend servers
- Scales by distributing video streaming processing to other servers

Live Configurations

- Architecture allowed live building of dashboards
- Histogram of mouse/keyboard activity added mid-event
- Reduced collection and live streaming for bandwidth constraints

System Level Monitoring

- Enabled collection of participant actions on client and web-based services
- System/application/OTS processes health for each participant’s system

Timestamped OTS Data

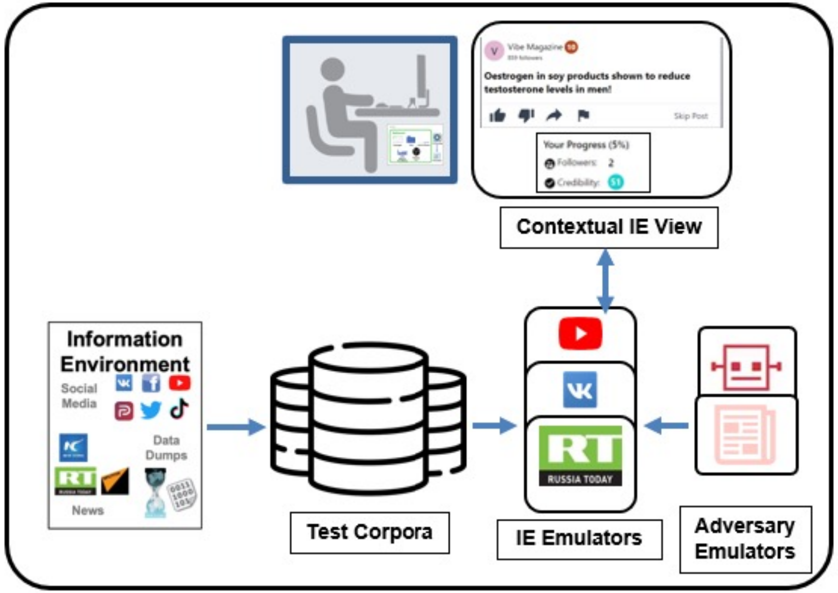
- Allows ability to replay past exercises and sessions
- Enables drill-downs on time windows of interest
- Spikes in metrics or active windows of interest highlight time periods

Current Work: Information Environment Emulatio

Scenario

- Emulates news and social media sites
- Data generated from real data
- Frontend configurable to emulate any platform
- Recreating recommendation algorithms
- Emulating injection of pink slime news, red personas, and bots

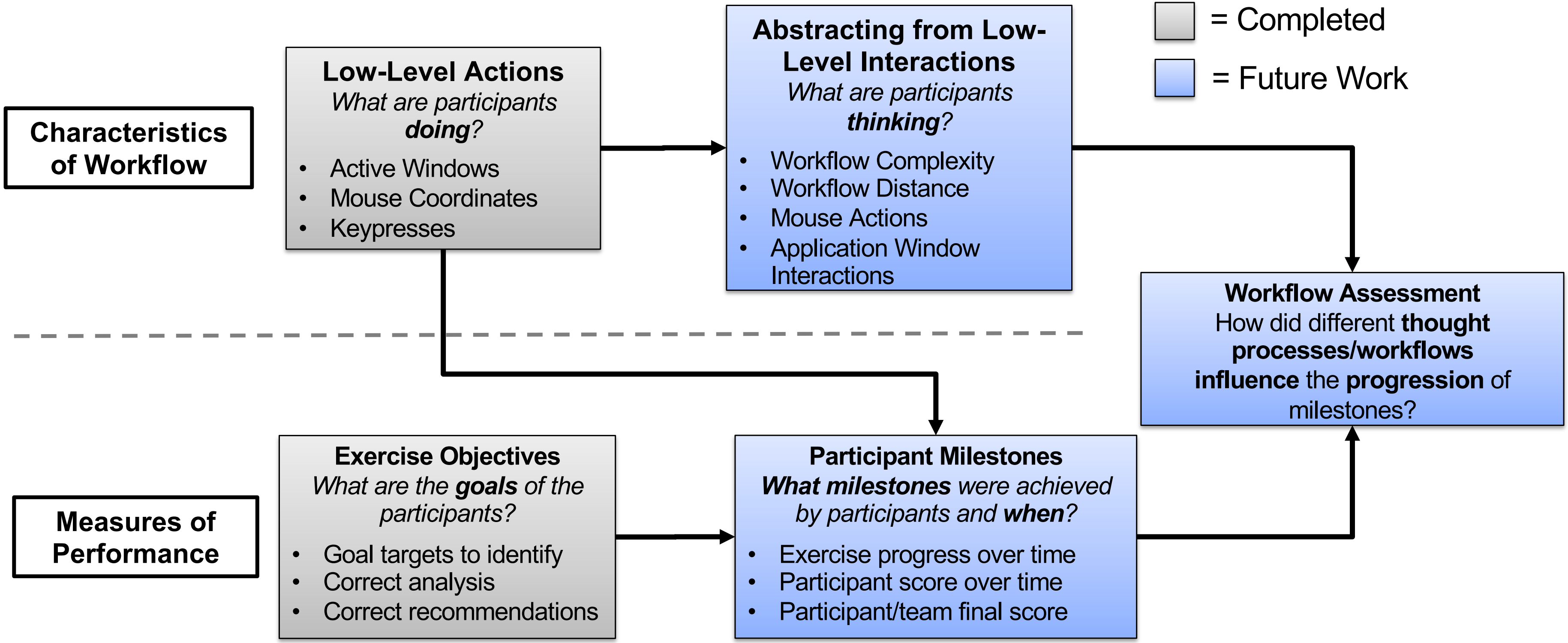
IE Emulation



Configurable gray cell platform framework supporting emulation of full range of social media and web platforms, enabling tool and operator integration

Future Work: Actions to Measures of Performance

Scoring



▢ = Completed

🟦 = Future Work

Characteristics of Workflow

Low-Level Actions
What are participants ***doing****?*

- Active Windows
- Mouse Coordinates
- Keypresses

Abstracting from Low-Level Interactions
What are participants ***thinking****?*

- Workflow Complexity
- Workflow Distance
- Mouse Actions
- Application Window Interactions

Workflow Assessment
How did different **thought processes/workflows influence** the **progression** of milestones?

Measures of Performance

Exercise Objectives
What are the ***goals*** *of the participants?*

- Goal targets to identify
- Correct analysis
- Correct recommendations

Participant Milestones
What milestones *were achieved by participants and* ***when****?*

- Exercise progress over time
- Participant score over time
- Participant/team final score

Summary

- Lessons learned on the successful implementation of cyber security testbeds can be applied to OIE testbeds to hasten the maturation of OIE tools and workflows
- CIOTER was developed as a composable, open architecture testbed with 2 current capabilities, MLOPs and OTS Situational Awareness, that were fielded in demonstrations
- CIOTER aims to pave the way as an exemplar for future OIE testbeds which would evolve resiliency for defense strategies
- Questions