METAPHORTRESS

# 2020 NETL FE R&D Annual Project Review Meeting

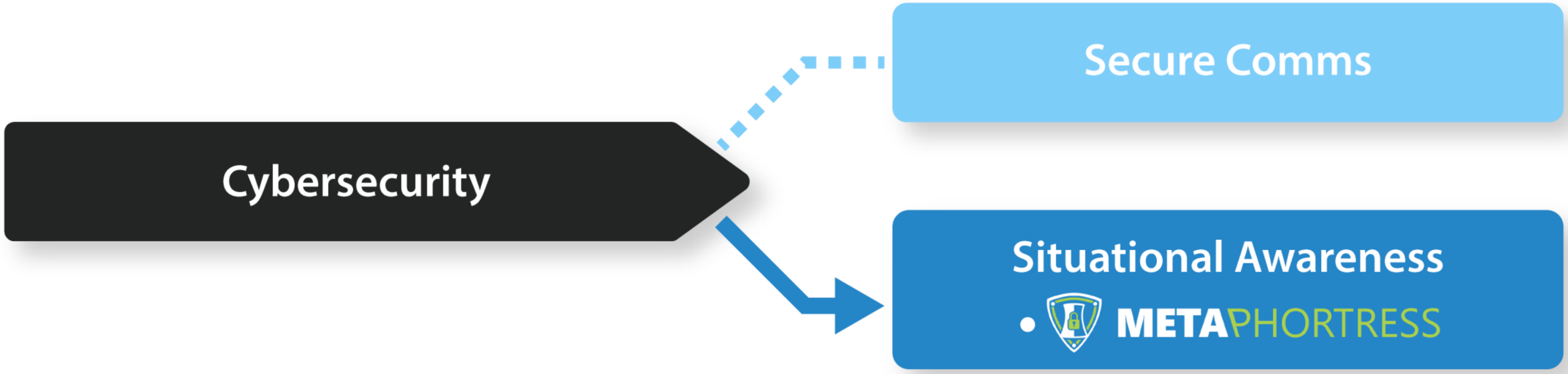
## Sensors and Controls

## MetaPhortress Project Status

**27 August 2020**

# Agenda

- Project Description & Objectives
  - System Concept and Features
  - Technology Stack
  - Lessons Learned
- Project Update
  - Situation Awareness Research
  - Energy Sector Stakeholder Interview Process
  - User Research Findings
  - User Interface Design
- Next Steps
- Conclusions



Cybersecurity

Secure Comms

Situational Awareness

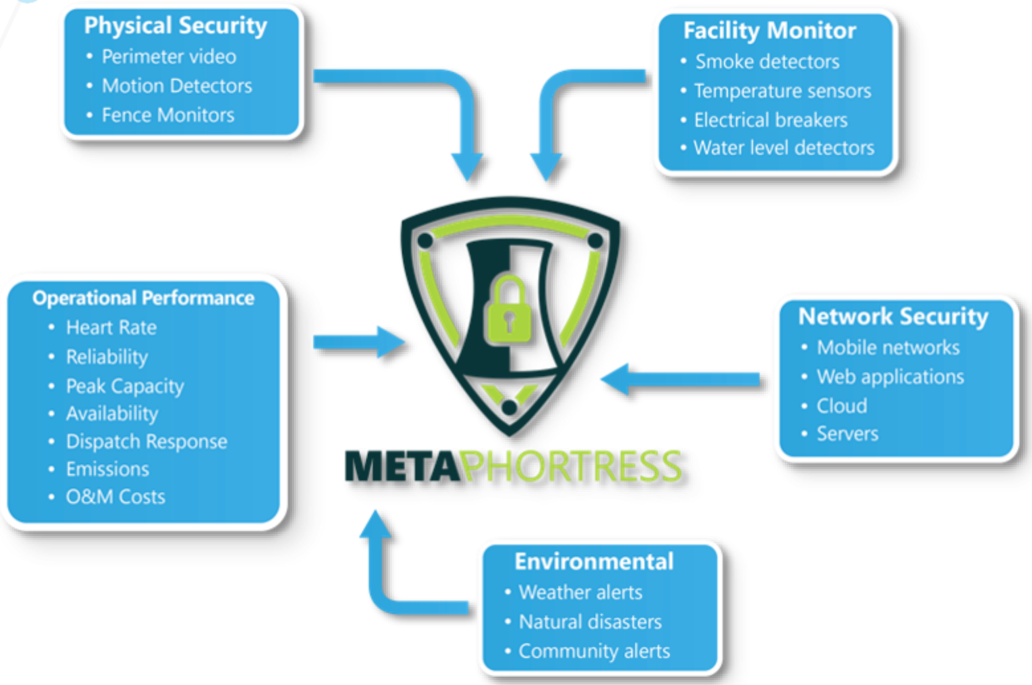
- METAPHORTRESS

# Project Description & Objectives

SBIR Data Rights Apply: Content subject to the restrictions on the title slide.

# Project Description and Objectives

DOE Office of Fossil Energy 2018-2020 Strategic Vision, Objective 2.2:
Advance technologies to improve the efficiency, reliability, emissions, and performance of existing fossil-based power generation



**Physical Security**
- Perimeter video
- Motion Detectors
- Fence Monitors

**Facility Monitor**
- Smoke detectors
- Temperature sensors
- Electrical breakers
- Water level detectors

**Operational Performance**
- Heart Rate
- Reliability
- Peak Capacity
- Availability
- Dispatch Response
- Emissions
- O&M Costs

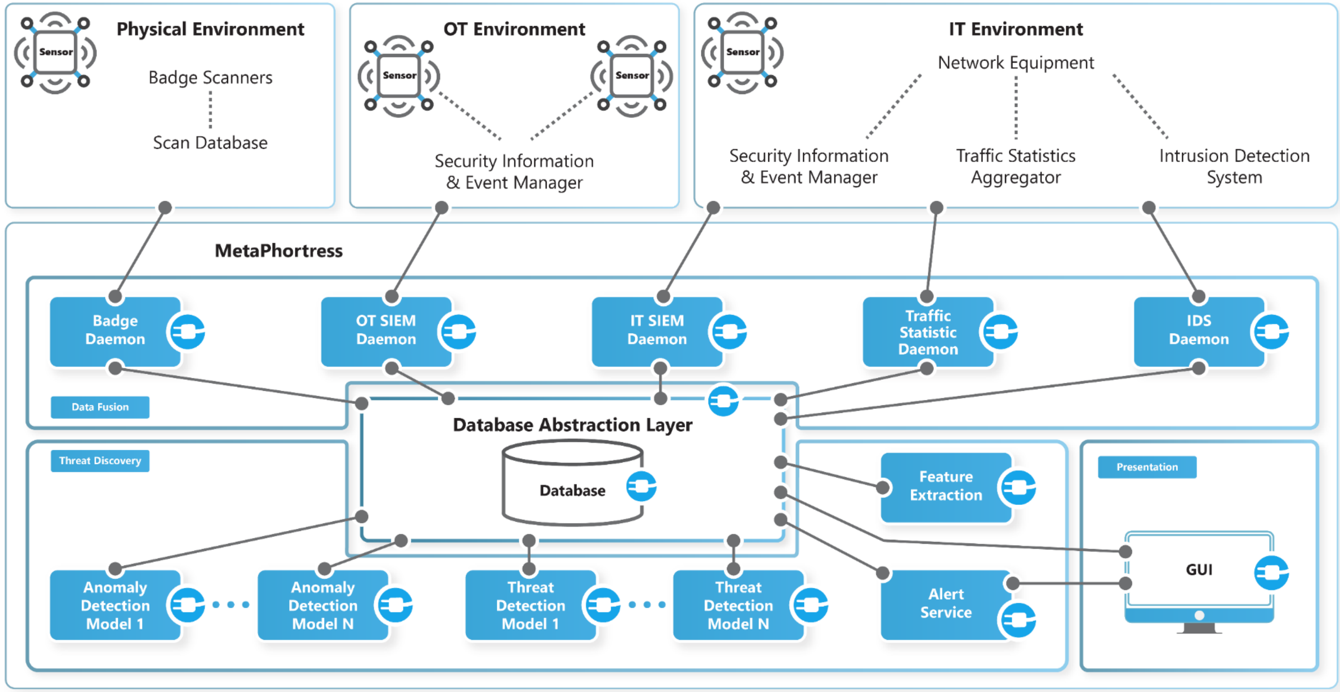
**Network Security**
- Mobile networks
- Web applications
- Cloud
- Servers

**Environmental**
- Weather alerts
- Natural disasters
- Community alerts

- To avoid service interruptions, fossil fuel power plants need effective situation awareness to detect and mitigate cyber threats.
- MetaPhortress is an automated cyber situation awareness tool that will enhance the resilience, safety, and reliability of these facilities.
- This question drives us: How do we provide accurate, timely, and actionable cyber situation awareness and threat detection to power plants?

# System Concept

- MetaPhortress adapts our patented cyber feature-extraction and behavior analysis platform to provide comprehensive, simultaneous coverage of fossil power plant operational technology (OT)/ICS, information technology networks (IT), and physical access control systems (PACS).
- Performs data fusion upon networked sensor outputs in all three domains to characterize nominal operational modes
- Uses machine learning and data analytics techniques extract features, detect deviations from nominal modes, determine which anomalous conditions correspond to malicious behavior, and alert system operators to potential cyber incidents.



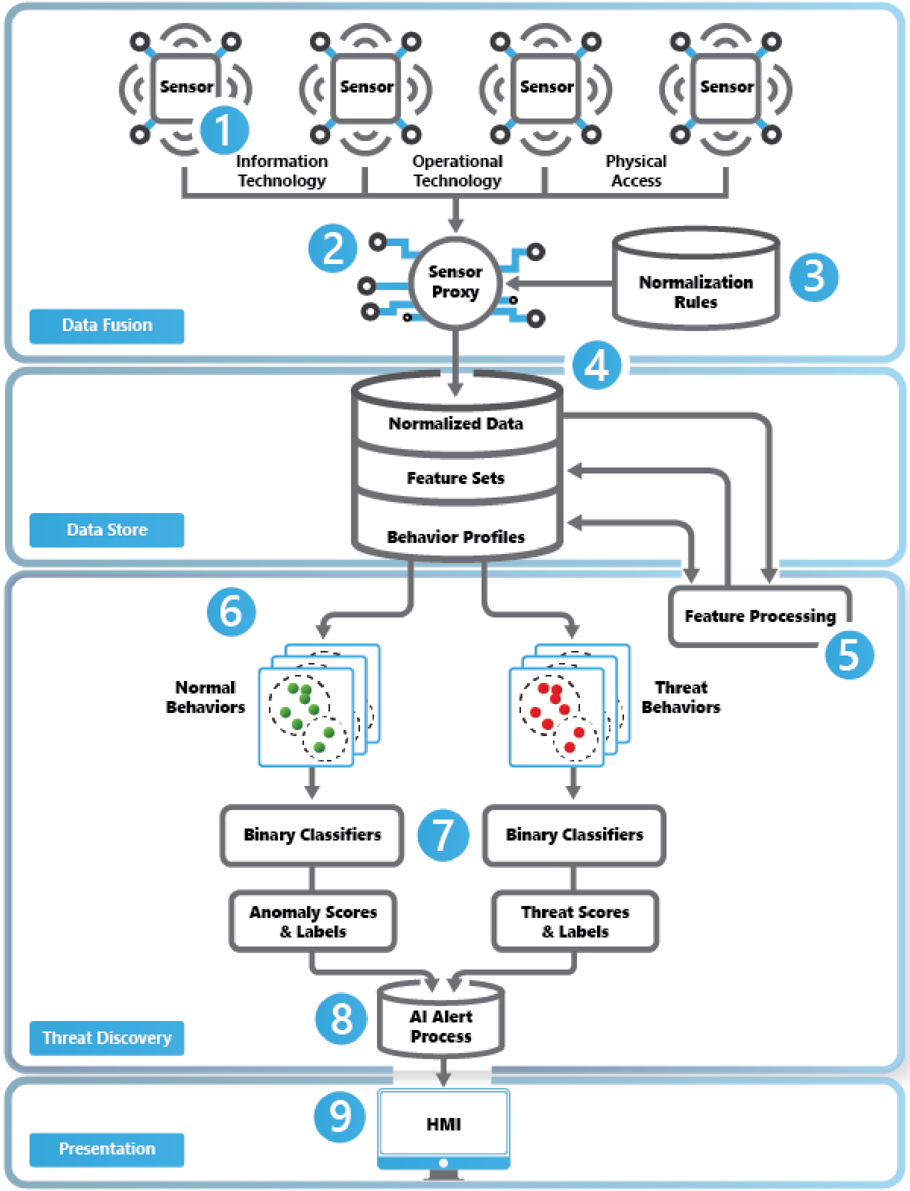
SBIR Data Rights Apply: Content subject to the restrictions on the title slide.

# System Features

METAPHORTRESS

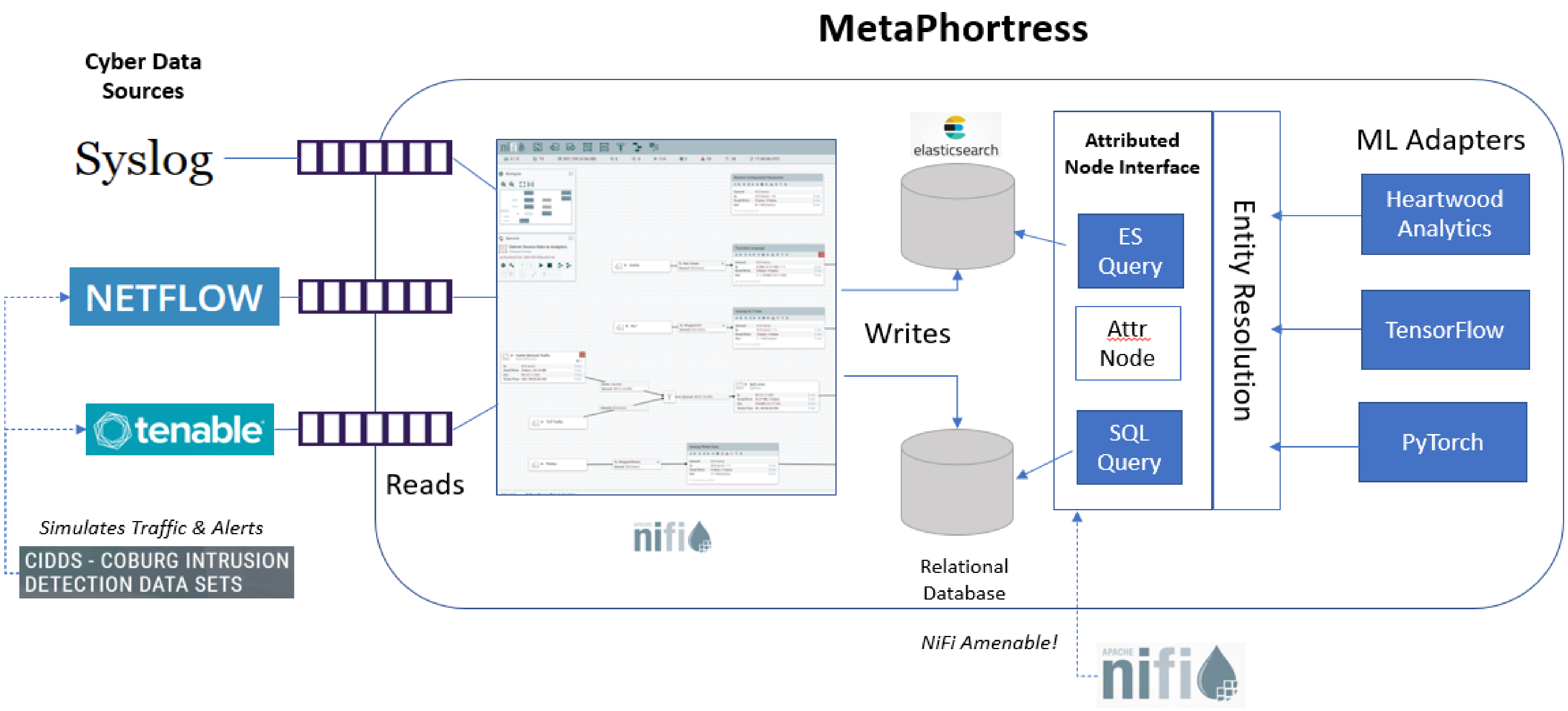
- Converged, simultaneous sensor data analysis of OT, IT, and PACS to discover cyber threats and resolve them against the time and system domains
- Aggregated behavior analysis to discover malicious entities that attempt multiple vectors across power plant attack surfaces
- Temporally aggregated analysis to detect attacks that unfold over varied timescales
- Rapid, clear, actionable presentation of threat alerts to power plant operators
- Improved defense of critical energy infrastructure to known and emerging cyber threats

- Collaboration Partners
  - **CUBRC** – data fusion and machine learning expertise
  - **TDi Technologies** – power generation domain knowledge, software integration requirements, and domain specific datasets



# Technology Stack

NIST guidance for cyber protection of power generation facilities recommends converged threat analysis of the OT/ICS, IT, and PACS domains. Individual, siloed analysis of those data areas is common; MetaPhortress, instead, automates this combined analysis with data fusion over all three areas.



# What We've Learned

- The MetaPhortress development team continues to meet with energy sector stakeholders in industry who provide valuable insights that guide needs assessment, requirements analysis, and system design.
- MetaPhortress team efforts have:
  - Researched and characterized the sensor types available in the domain
  - Obtained representative data sets
  - Determined attack surfaces over the range of fossil power plant types
  - Determined system integration requirements
  - Designed a prototype human-machine interface
  - Designed a system architecture
- By executing these efforts, and working with our stakeholders, we now realize that what we initially saw as an analytics challenge is actually also a human factors challenge – how do we convert machine learning outputs into clear and effective situation awareness cues that will help plant operators act on potential cyber threats?

METAPHORTRESS

# Project Update

# Situation Awareness (SA)

SA: Knowing what’s going on, so you can make good decisions

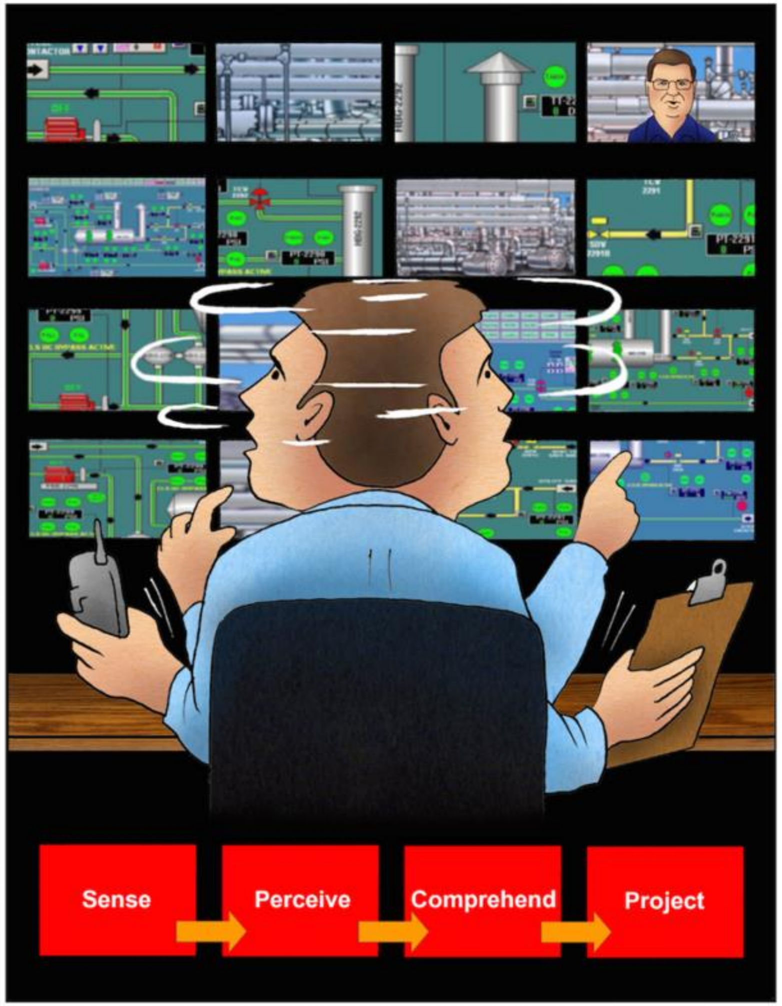
- Experimental psychology construct, theory, and model
- Describes how different factors… affect a human’s ability to acquire and interpret information for effective decision making (Endsley, 1995)
- SA Model is composed of three levels (Endsley, 1995, 2000):
  - $SA_1$: Perception of elements in the environment
  - $SA_2$: Comprehension of the current situation
  - $SA_3$: Projection of future status

M. R. Endsley, “Toward a theory of situation awareness in dynamic systems,” Human Factors: The Journal of the Human Factors and Ergonomics Society, 37(1), pp 32-64, 1995.

M. R. Endsley, “Theoretical underpinnings of situation awareness: A critical review,” In Situation Awareness Analysis and Measurement, M. R. Endsley and D. Garland, Eds., Mahwah: Lawrence Erlbaum, 2000, pp. 3-32.

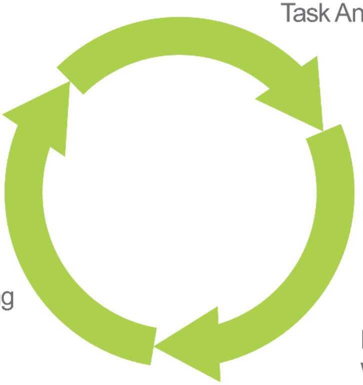
# Situation Awareness

## Situation Awareness and Sensemaking



- Sensemaking is a part of situation awareness (SA).
- SA is “the perception of the elements in the environment within a volume of time and space, the comprehension of their meaning, and the projection of their status in the near future“ (Endsley, 1995).
- Sensemaking is both retrospective and prospective and is a process (rather than a state).

# User Interaction – Feedback Cycle



**Plan**

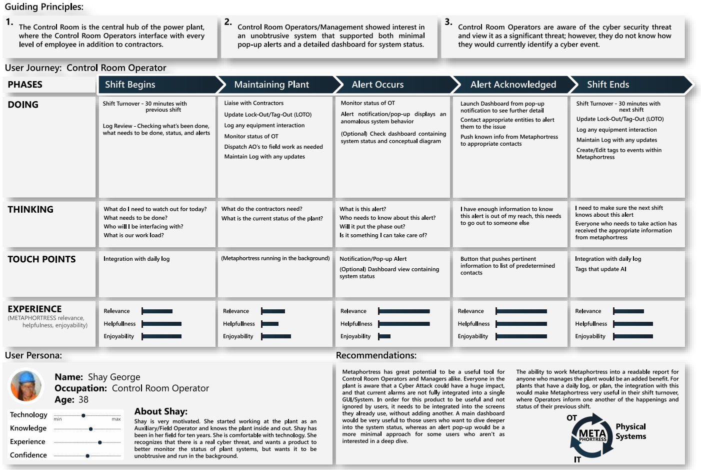
Research
User Interviews
Mental Models
Task Analysis

**Design**

Experience Mapping
Wireframe
Mockups
Interactive Prototype

**Test**

Usability Testing
Funnel Matrix
User Testing
Validating Design



Guiding Principles:

1. The Control Room is the central hub of the power plant, where the Control Room Operators interface with every level of employee in addition to contractors.

2. Control Room Operators/Management showed interest in an unobtrusive system that supported both minimal pop-up alerts and a detailed dashboard for system status.

3. Control Room Operators are aware of the cyber security threat and view it as a significant threat; however, they do not know how they would currently identify a cyber event.

User Journey: Control Room Operator

| PHASES | Shift Begins | Maintaining Plant | Alert Occurs | Alert Acknowledged | Shift Ends |
|---|---|---|---|---|---|
| DOING | Shift Turnover – 30 minutes with previous shift<br>Log Review – Checking what's been done, what needs to be done, status, and alerts | Liaise with Contractors<br>Update Lock-Out/Tag-Out (LOTO)<br>Log any equipment interaction<br>Monitor status of OT<br>Dispatch AO's to field work as needed<br>Maintain Log with any updates | Monitor status of OT<br>Alert notification/pop-up displays an anomalous system behavior<br>(Optional) Check dashboard containing system status and conceptual diagram | Launch Dashboard from pop-up notification to see further detail<br>Contact appropriate entities to alert them to the issue<br>Push known info from Metaphortress to appropriate contacts | Shift Turnover – 30 minutes with next shift<br>Update Lock-Out/Tag-Out (LOTO)<br>Log any equipment interaction<br>Maintain Log with any updates<br>Create/Edit tags to events within Metaphortress |
| THINKING | What do I need to watch out for today?<br>What needs to be done?<br>Who will I be interfacing with?<br>What is our work load? | What do the contractors need?<br>What is the current status of the plant? | What is this alert?<br>Who needs to know about this alert?<br>Will it put the phase out?<br>Is it something I can take care of? | I have enough information to know this alert is out of my reach, this needs to go out to someone else | I need to make sure the next shift knows about this alert<br>Everyone who needs to take action has received the appropriate information from metaphortress |
| TOUCH POINTS | Integration with daily log | (Metaphortress running in the background) | Notification/Pop-up Alert<br>(Optional) Dashboard view containing system status | Button that pushes pertinent information to list of predetermined contacts | Integration with daily log<br>Tags that update AI |
| EXPERIENCE (METAPHORTRESS relevance, helpfulness, enjoyability) | Relevance<br>Helpfullness<br>Enjoyability | Relevance<br>Helpfullness<br>Enjoyability | Relevance<br>Helpfullness<br>Enjoyability | Relevance<br>Helpfullness<br>Enjoyability | Relevance<br>Helpfullness<br>Enjoyability |

User Persona:

**Name:** Shay George
**Occupation:** Control Room Operator
**Age:** 38

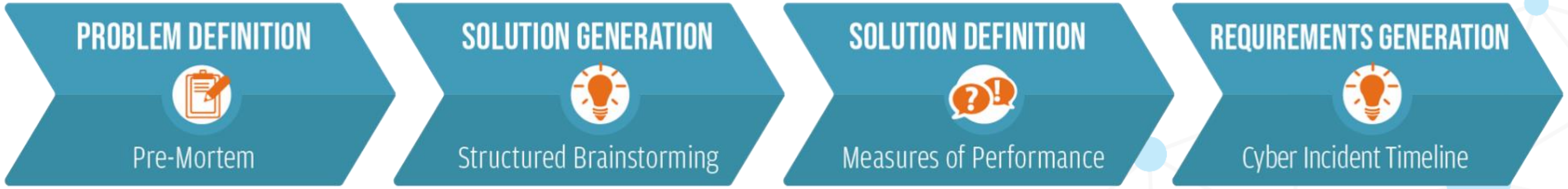
Technology min max
Knowledge
Experience
Confidence

**About Shay:**
Shay is very motivated. She started working at the plant as an Auxiliary/Field Operator and knows the plant inside and out. Shay has been in her field for ten years. She is comfortable with technology. She recognizes that there is a real cyber threat, and wants a product to better monitor the status of plant systems, but wants it to be unobtrusive and run in the background.

Recommendations:

Metaphortress has great potential to be a useful tool for Control Room Operators and Managers alike. Everyone in the plant is aware that a Cyber Attack could have a huge impact, and that current alarms are not fully integrated into a single GUI/System. In order for this product to be useful and not ignored by users, it needs to be integrated into the screens they already use, without adding another. A main dashboard would be very useful to those users who want to dive deeper into the system status, whereas an alert pop-up would be a more minimal approach for some users who aren't as interested in a deep dive.

The ability to work Metaphortress into a readable report for anyone who manages the plant would be an added benefit. For plants that have a daily log, or plan, the integration with this would make Metaphortress very useful in their shift turnover, where Operators inform one another of the happenings and status of their previous shift.



**PROBLEM DEFINITION** – Pre-Mortem

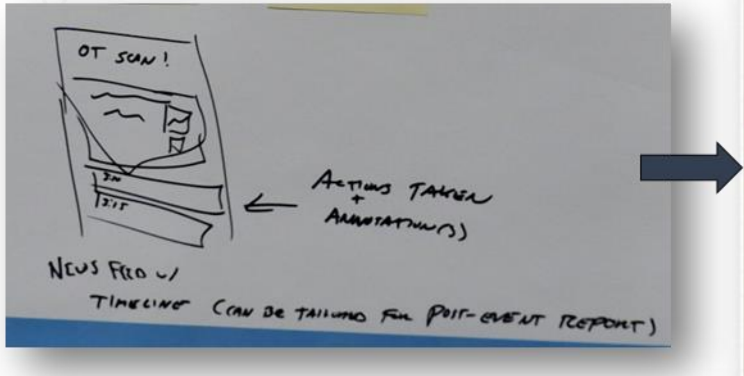
**SOLUTION GENERATION** – Structured Brainstorming

**SOLUTION DEFINITION** – Measures of Performance

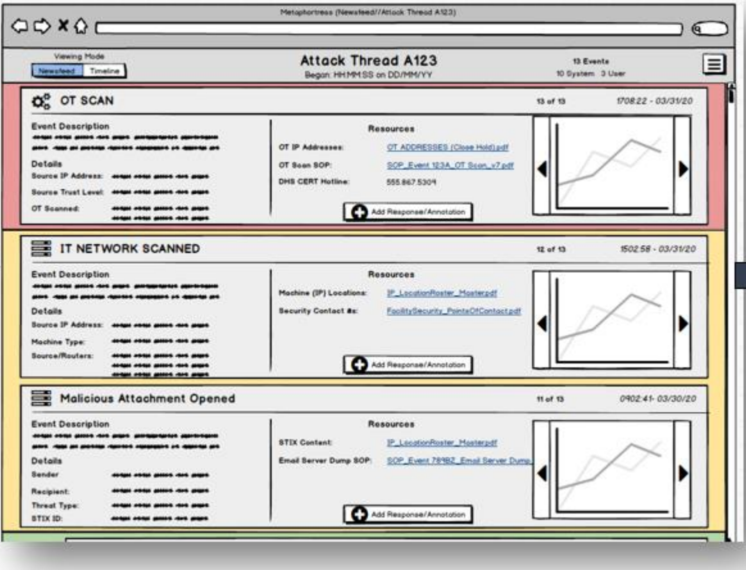
**REQUIREMENTS GENERATION** – Cyber Incident Timeline

# Findings and Recommendations

METAPHORTRESS


OT SCAN!
3:11
3:15
ACTIONS TAKEN + ANNOTATIONS)
NEWS FEED w/ TIMELINE (CAN BE TAILORED FOR POST-EVENT REPORT)

**Rough Sketch from TIDE**


Metaphortress (Newsfeed//Attack Thread A123)

Viewing Mode: Newsfeed | Timeline

**Attack Thread A123**

Began: HH:MM:SS on DD/MM/YY

13 Events
10 System 3 User

**OT SCAN** — 13 of 13 — 1708:22 - 03/31/20

Event Description

Details
Source IP Address:
Source Trust Level:
OT Scanned:

Resources
OT IP Addresses: OT ADDRESSES (Close Hold).pdf
OT Scan SOP: SOP_Event 123A_OT Scan_v7.pdf
DHS CERT Hotline: 555.867.5309

Add Response/Annotation

**IT NETWORK SCANNED** — 12 of 13 — 1502:58 - 03/31/20

Event Description

Details
Source IP Address:
Machine Type:
Source/Routers:

Resources
Machine (IP) Locations: IP_LocationRoster_Master.pdf
Security Contact #s: FacilitySecurity_PointsOfContact.pdf

Add Response/Annotation

**Malicious Attachment Opened** — 11 of 13 — 0902:41- 03/30/20

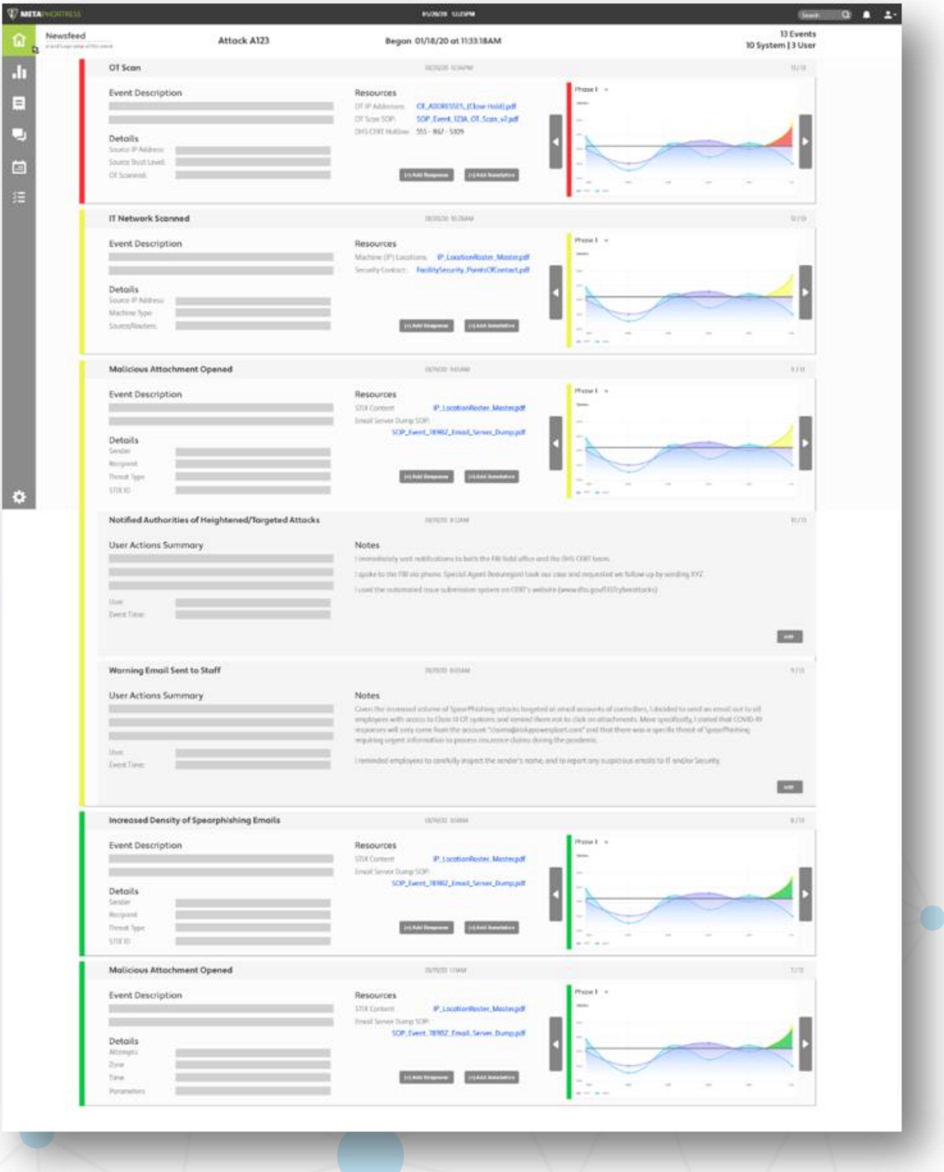
Event Description

Details
Sender
Recipient:
Threat Type:
STIX ID:

Resources
STIX Content: IP_LocationRoster_Master.pdf
Email Server Dump SOP: SOP_Event 7898Z_Email Server Dump

Add Response/Annotation

**Wireframe**


METAPHORTRESS

Newsfeed — Attack A123 — Began 01/18/20 at 11:33:18AM — 13 Events, 10 System | 3 User

**OT Scan**

Event Description

Details
Source IP Address:
Source Trust Level:
OT Scanned:

Resources
OT IP Addresses: OT_ADDRESSES_(Close Hold).pdf
OT Scan SOP: SOP_Event_123A_OT_Scan_v7.pdf
DHS CERT Hotline: 555 - 867 - 5309

(+) Add Response (+) Add Annotation

**IT Network Scanned**

Event Description

Details
Source IP Address:
Machine Type:
Source/Routers:

Resources
Machine (IP) Locations: IP_LocationRoster_Master.pdf
Security Contact: FacilitySecurity_PointsOfContact.pdf

(+) Add Response (+) Add Annotation

**Malicious Attachment Opened**

Event Description

Details
Sender
Recipient
Threat Type
STIX ID

Resources
STIX Content: IP_LocationRoster_Master.pdf
Email Server Dump SOP: SOP_Event_78982_Email_Server_Dump.pdf

(+) Add Response (+) Add Annotation

**Notified Authorities of Heightened/Targeted Attacks**

User Actions Summary
User
Event Time

Notes
I immediately sent notifications to both the FBI field office and the DHS CERT team.
I spoke to the FBI via phone. Special Agent [illegible] took our case and requested we follow up by sending XYZ
I used the automated issue submission system on CERT's website (www.dhs.gov/[illegible]cyberattacks)

Edit

**Warning Email Sent to Staff**

User Actions Summary
User
Event Time

Notes
Given the increased volume of SpearPhishing attacks targeted at email accounts of controllers, I decided to send an email out to all employees with access to Class III OT systems and remind them not to click on attachments. More specifically, I stated that COVID-19 responses will only come from the account "claims@[illegible].com" and that there was a specific threat of SpearPhishing requiring urgent information to process insurance claims during the pandemic.

I reminded employees to carefully inspect the sender's name, and to report any suspicious emails to IT and/or Security.

Edit

**Increased Density of Spearphishing Emails**

Event Description

Details
Sender
Recipient
Threat Type
STIX ID

Resources
STIX Content: IP_LocationRoster_Master.pdf
Email Server Dump SOP: SOP_Event_78982_Email_Server_Dump.pdf

(+) Add Response (+) Add Annotation

**Malicious Attachment Opened**

Event Description

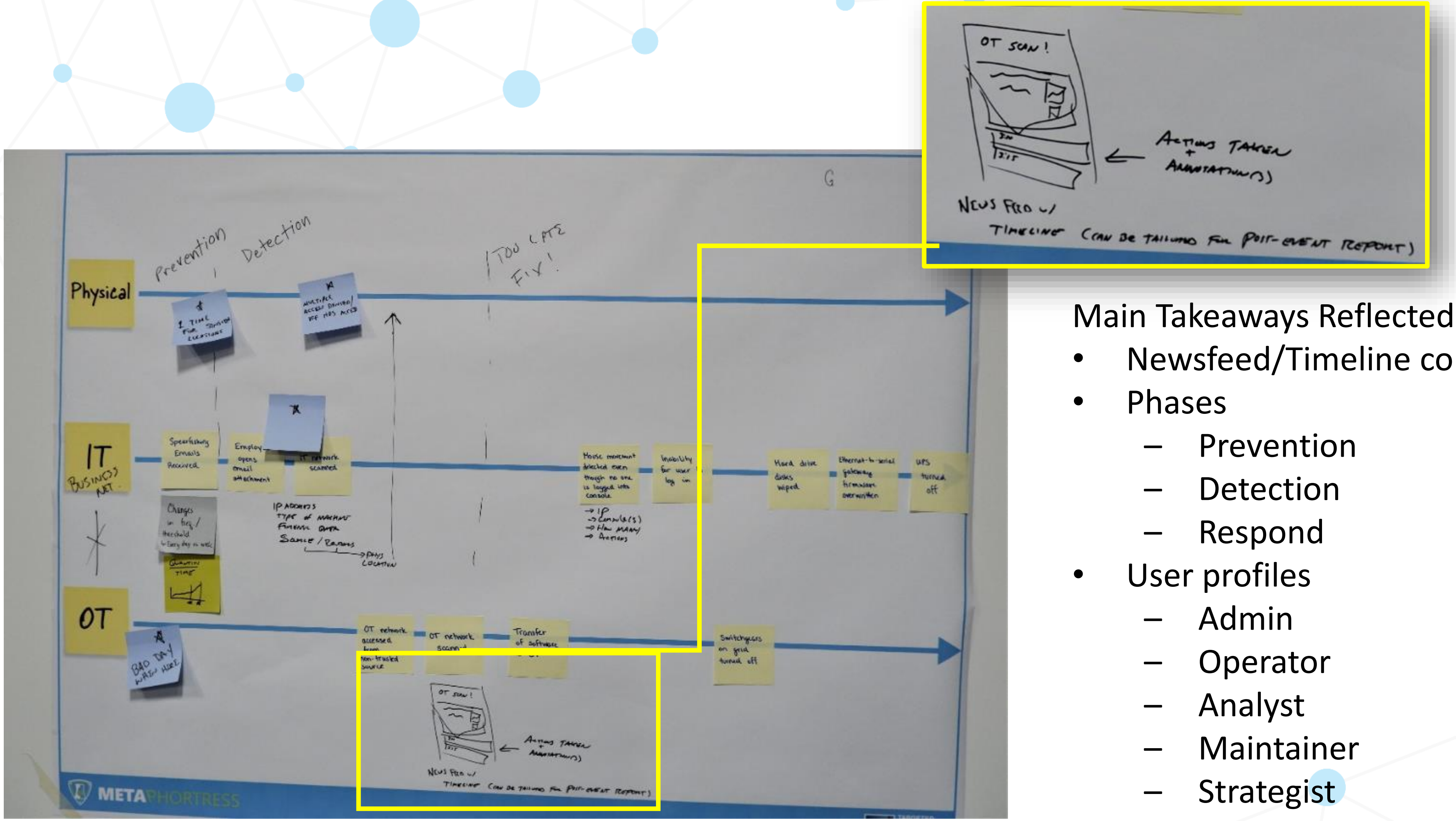
Details
Attempts
Zone
Time
Parameters

Resources
STIX Content: IP_LocationRoster_Master.pdf
Email Server Dump SOP: SOP_Event_78982_Email_Server_Dump.pdf

(+) Add Response (+) Add Annotation

**Formal Mock-up**

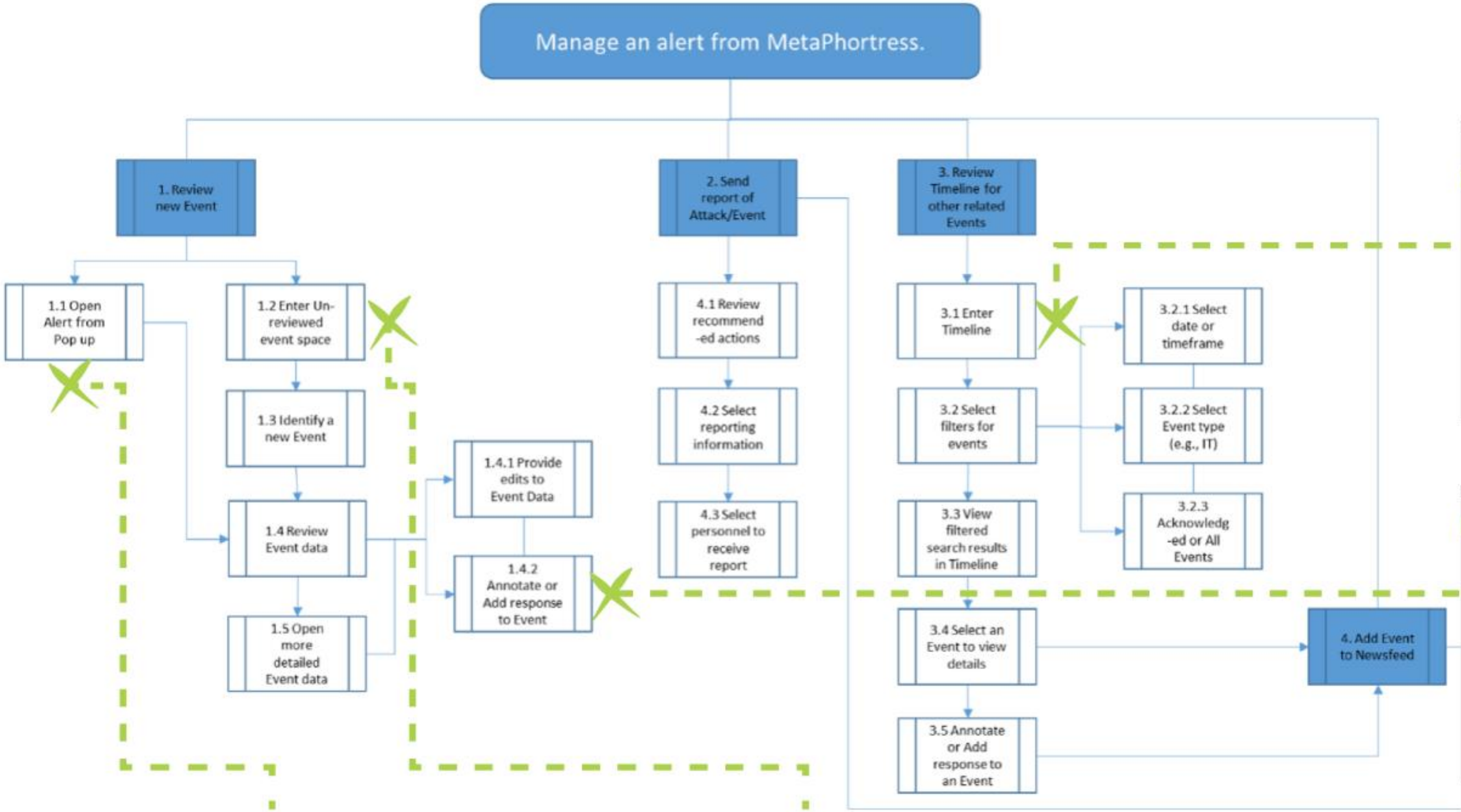
# Findings and Recommendations


Prevention
Detection
Too late
Fix!
G
Physical
1 time for sensitive locations
Multiple access denied/ FF has access
IT
Business net
Spearfishing Emails Received
Employ. opens email attachment
IT network scanned
Changes in freq./ threshold → Every day vs week
Quantity
Time
IP Address
type of machine
Forensic data
Source / Ratings
→ Phys location
Mouse movement detected even though no one is logged into console
→ IP
→ Console(s)
→ How many
→ Actions
Inability for user to log in
Hard drive disks wiped
Ethernet-to-serial gateway firmware overwritten
UPS turned off
OT
Bad day was here
OT network accessed from non-trusted source
OT network scanned
Transfer of software
Switchgears on grid turned off
OT scan!
Actions taken + annotation(s)
News feed w/ timeline (can be tailored for post-event report)
METAPHORTRESS

Main Takeaways Reflected in Designs:

- Newsfeed/Timeline concept
- Phases
  - Prevention
  - Detection
  - Respond
- User profiles
  - Admin
  - Operator
  - Analyst
  - Maintainer
  - Strategist

# Mock-ups



Manage an alert from MetaPhortress.

1. Review new Event

1.1 Open Alert from Pop up

1.2 Enter Un-reviewed event space

1.3 Identify a new Event

1.4 Review Event data

1.4.1 Provide edits to Event Data

1.4.2 Annotate or Add response to Event

1.5 Open more detailed Event data

2. Send report of Attack/Event

4.1 Review recommend-ed actions

4.2 Select reporting information

4.3 Select personnel to receive report

3. Review Timeline for other related Events

3.1 Enter Timeline

3.2 Select filters for events

3.2.1 Select date or timeframe

3.2.2 Select Event type (e.g., IT)

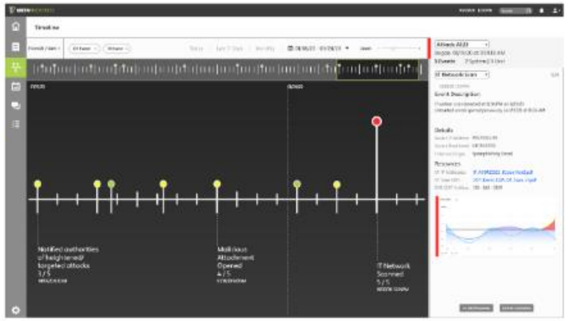
3.2.3 Acknowledg-ed or All Events

3.3 View filtered search results in Timeline

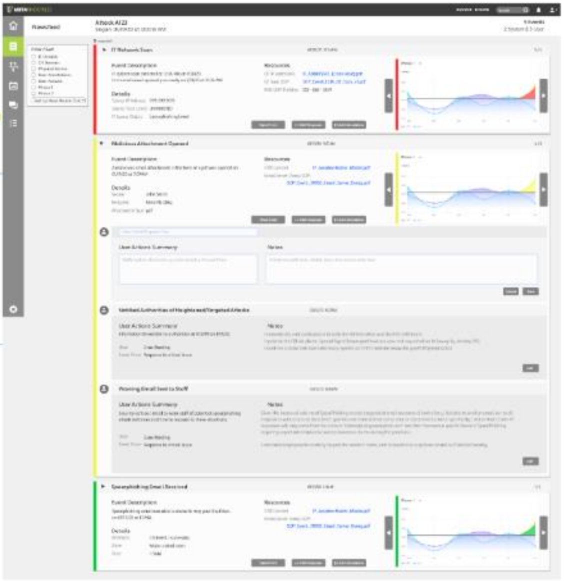
3.4 Select an Event to view details

3.5 Annotate or Add response to an Event

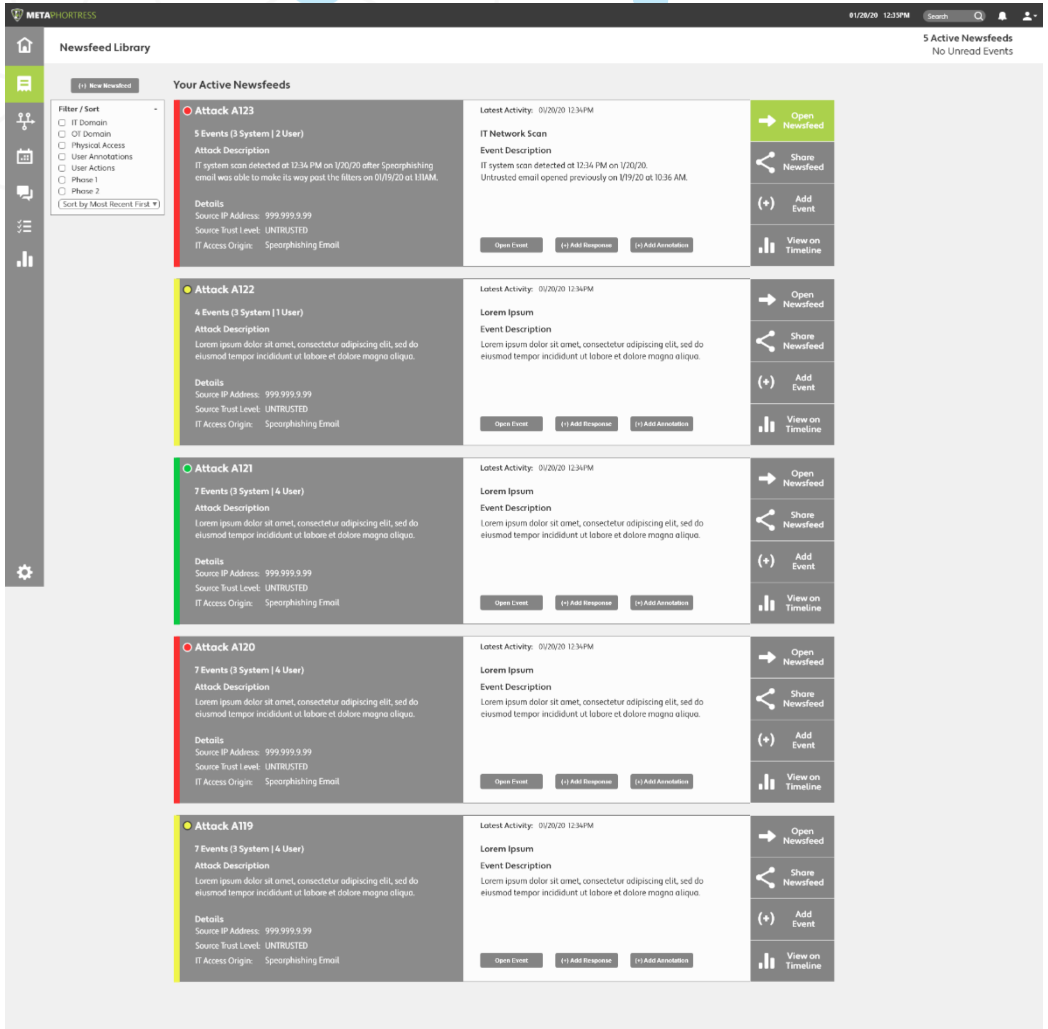
4. Add Event to Newsfeed



Timeline
Notified authorities of heightened/ targeted attacks
3 / 5
Malicious Attachment Opened
4 / 5
IT Network Scanned
5 / 5
Details
Resources



# Newsfeed



Newsfeed Library

5 Active Newsfeeds
No Unread Events

Filter / Sort

- ☐ IT Domain
- ☐ OT Domain
- ☐ Physical Access
- ☐ User Annotations
- ☐ User Actions
- ☐ Phase 1
- ☐ Phase 2

Sort by Most Recent First ▾

Your Active Newsfeeds

● Attack A123

5 Events (3 System | 2 User)

Attack Description

IT system scan detected at 12:34 PM on 1/20/20 after Spearphishing email was able to make its way past the filters on 01/19/20 at 1:11AM.

Details

Source IP Address: 999.999.9.99

Source Trust Level: UNTRUSTED

IT Access Origin: Spearphishing Email

Latest Activity: 01/20/20 12:34PM

IT Network Scan

Event Description

IT system scan detected at 12:34 PM on 1/20/20.
Untrusted email opened previously on 1/19/20 at 10:36 AM.

● Attack A122

4 Events (3 System | 1 User)

Attack Description

Lorem ipsum dolor sit amet, consectetur adipiscing elit, sed do eiusmod tempor incididunt ut labore et dolore magna aliqua.

Details

Source IP Address: 999.999.9.99

Source Trust Level: UNTRUSTED

IT Access Origin: Spearphishing Email

Latest Activity: 01/20/20 12:34PM

Lorem Ipsum

Event Description

Lorem ipsum dolor sit amet, consectetur adipiscing elit, sed do eiusmod tempor incididunt ut labore et dolore magna aliqua.

● Attack A121

7 Events (3 System | 4 User)

Attack Description

Lorem ipsum dolor sit amet, consectetur adipiscing elit, sed do eiusmod tempor incididunt ut labore et dolore magna aliqua.

Details

Source IP Address: 999.999.9.99

Source Trust Level: UNTRUSTED

IT Access Origin: Spearphishing Email

Latest Activity: 01/20/20 12:34PM

Lorem Ipsum

Event Description

Lorem ipsum dolor sit amet, consectetur adipiscing elit, sed do eiusmod tempor incididunt ut labore et dolore magna aliqua.

● Attack A120

7 Events (3 System | 4 User)

Attack Description

Lorem ipsum dolor sit amet, consectetur adipiscing elit, sed do eiusmod tempor incididunt ut labore et dolore magna aliqua.

Details

Source IP Address: 999.999.9.99

Source Trust Level: UNTRUSTED

IT Access Origin: Spearphishing Email

Latest Activity: 01/20/20 12:34PM

Lorem Ipsum

Event Description

Lorem ipsum dolor sit amet, consectetur adipiscing elit, sed do eiusmod tempor incididunt ut labore et dolore magna aliqua.

● Attack A119

7 Events (3 System | 4 User)

Attack Description

Lorem ipsum dolor sit amet, consectetur adipiscing elit, sed do eiusmod tempor incididunt ut labore et dolore magna aliqua.

Details

Source IP Address: 999.999.9.99

Source Trust Level: UNTRUSTED

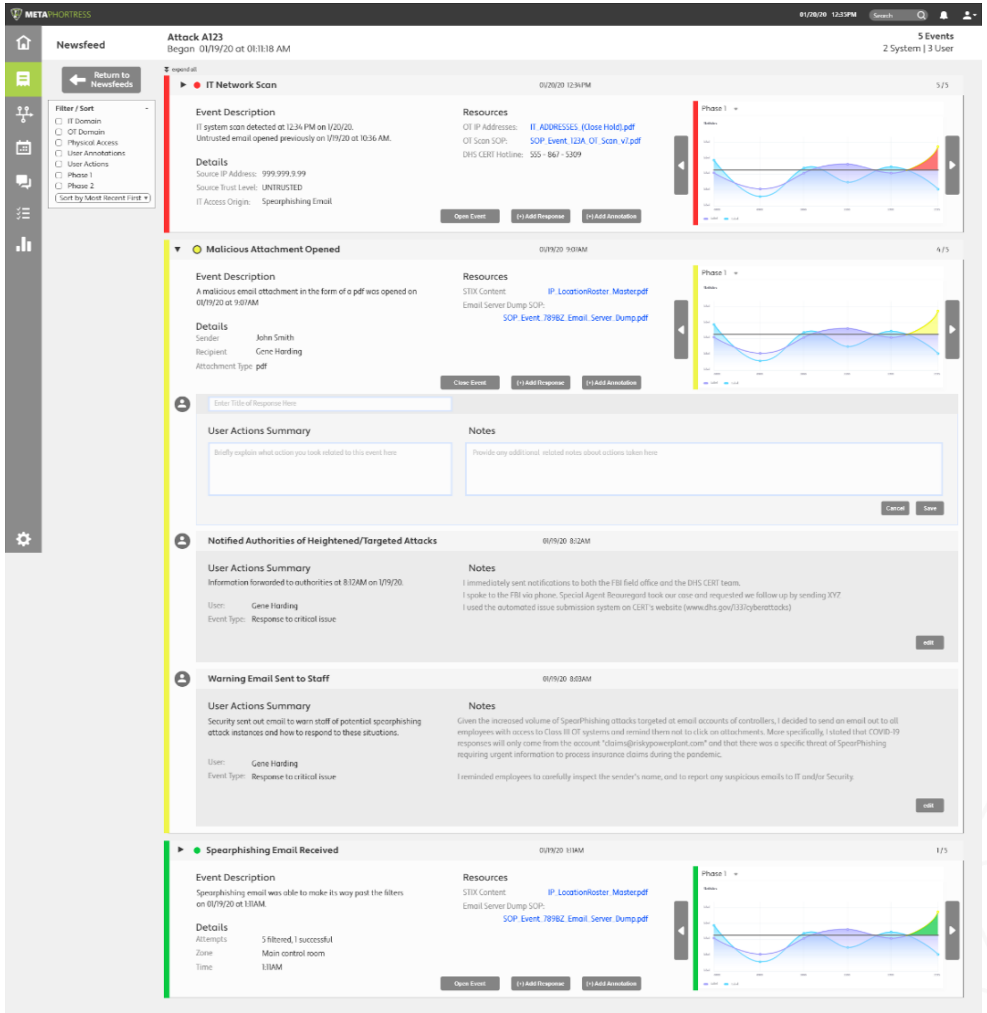
IT Access Origin: Spearphishing Email

Latest Activity: 01/20/20 12:34PM

Lorem Ipsum

Event Description

Lorem ipsum dolor sit amet, consectetur adipiscing elit, sed do eiusmod tempor incididunt ut labore et dolore magna aliqua.



Newsfeed

Attack A123
Began 01/19/20 at 01:11:18 AM

5 Events
2 System | 3 User

Filter / Sort

- ☐ IT Domain
- ☐ OT Domain
- ☐ Physical Access
- ☐ User Annotations
- ☐ User Actions
- ☐ Phase 1
- ☐ Phase 2

Sort by Most Recent First ▾

▶ ● IT Network Scan 01/20/20 12:34PM 5/5

Event Description

IT system scan detected at 12:34 PM on 1/20/20.
Untrusted email opened previously on 1/19/20 at 10:36 AM.

Details

Source IP Address: 999.999.9.99

Source Trust Level: UNTRUSTED

IT Access Origin: Spearphishing Email

Resources

OT IP Addresses: IT_ADDRESSES_(Close Hold).pdf

OT Scan SOP: SOP_Event_123A_OT_Scan_v7.pdf

DHS CERT Hotline: 555 - 867 - 5309

▼ ○ Malicious Attachment Opened 01/19/20 9:07AM 4/5

Event Description

A malicious email attachment in the form of a pdf was opened on 01/19/20 at 9:07AM

Details

Sender John Smith

Recipient Gene Harding

Attachment Type pdf

Resources

STIX Content IP_LocationRoster_Master.pdf

Email Server Dump SOP: SOP_Event_789BZ_Email_Server_Dump.pdf

Enter Title of Response Here

User Actions Summary

Briefly explain what action you took related to this event here

Notes

Provide any additional related notes about actions taken here

Notified Authorities of Heightened/Targeted Attacks 01/19/20 8:12AM

User Actions Summary

Information forwarded to authorities at 8:12AM on 1/19/20.

User: Gene Harding

Event Type: Response to critical issue

Notes

I immediately sent notifications to both the FBI field office and the DHS CERT team.
I spoke to the FBI via phone. Special Agent Beauregard took our case and requested we follow up by sending XYZ
I used the automated issue submission system on CERT's website (www.dhs.gov/1337cyberattacks)

Warning Email Sent to Staff 01/19/20 8:03AM

User Actions Summary

Security sent out email to warn staff of potential spearphishing attack instances and how to respond to these situations.

User: Gene Harding

Event Type: Response to critical issue

Notes

Given the increased volume of SpearPhishing attacks targeted at email accounts of controllers, I decided to send an email out to all employees with access to Class III OT systems and remind them not to click on attachments. More specifically, I stated that COVID-19 responses will only come from the account "claims@riskypowerplant.com" and that there was a specific threat of SpearPhishing requiring urgent information to process insurance claims during the pandemic.

I reminded employees to carefully inspect the sender's name, and to report any suspicious emails to IT and/or Security.

▶ ● Spearphishing Email Received 01/19/20 1:11AM 1/5

Event Description

Spearphishing email was able to make its way past the filters on 01/19/20 at 1:11AM.

Details

Attempts 5 filtered, 1 successful

Zone Main control room

Time 1:11AM

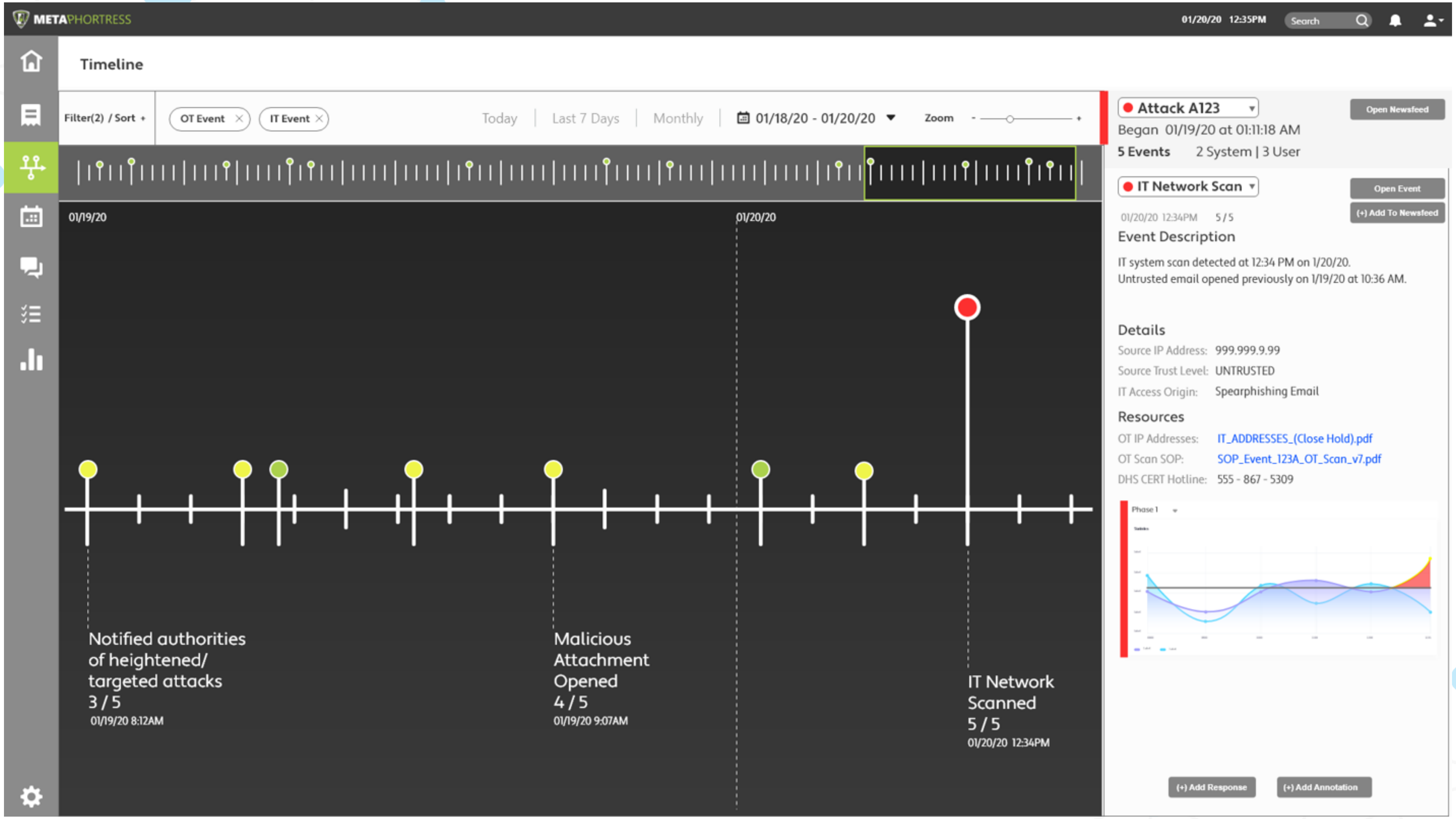
Resources

STIX Content IP_LocationRoster_Master.pdf

Email Server Dump SOP: SOP_Event_789BZ_Email_Server_Dump.pdf

SBIR Data Rights Apply: Content subject to the restrictions on the title slide.

# Timeline



Notified authorities of heightened/ targeted attacks
3 / 5
01/19/20 8:12AM

Malicious Attachment Opened
4 / 5
01/19/20 9:07AM

IT Network Scanned
5 / 5
01/20/20 12:34PM

● Attack A123

Open Newsfeed

Began 01/19/20 at 01:11:18 AM

5 Events 2 System | 3 User

● IT Network Scan

Open Event

(+) Add To Newsfeed

01/20/20 12:34PM 5 / 5

Event Description

IT system scan detected at 12:34 PM on 1/20/20.
Untrusted email opened previously on 1/19/20 at 10:36 AM.

Details

Source IP Address: 999.999.9.99
Source Trust Level: UNTRUSTED
IT Access Origin: Spearphishing Email

Resources

OT IP Addresses: IT_ADDRESSES_(Close Hold).pdf
OT Scan SOP: SOP_Event_123A_OT_Scan_v7.pdf
DHS CERT Hotline: 555 - 867 - 5309

SBIR Data Rights Apply: Content subject to the restrictions on the title slide.

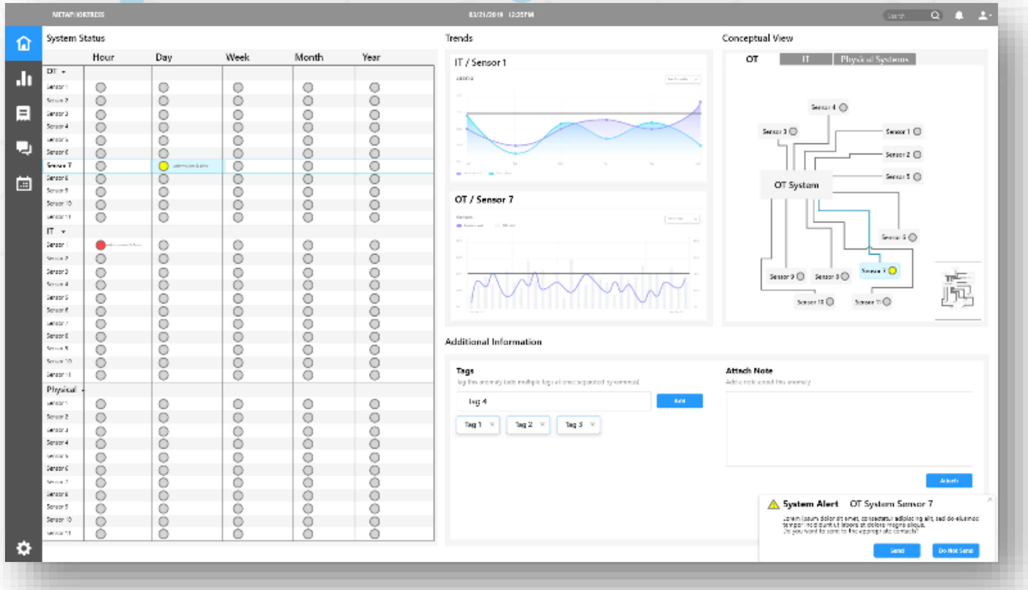
# Technology & Collaborative Challenges

- **Technology Challenges**
  - Training datasets with coherent IT, OT, and PACS are difficult to obtain
    - Align disparate datasets to produce coherent datasets
    - Continued outreach to industry development partners to improve quantity and quality of data we integrate
  - Numerous upstream sensors to integrate with and create UIs for
    - Integrate with data aggregation elements in each information domain, as opposed to individual sensors
  - Ability to integrate with a wide range of sensors
    - Architecture design that promotes loose coupling with in-situ power plant sensor elements
    - Transforming site specific data characteristics into MetaPhortress internal format at data ingest
- **Collaborative Challenges**
  - Ongoing recruitment and retention of participants for user research
    - Reaching out to all municipal utilities in Connecticut
    - Continuing inputs from existing contacts at Eversource and other CT power generators
  - COVID-19 requires new methods for conducting user research
    - Performed literature review and developed remote user research methods

METAPHORTRESS

# Next Steps

# Continued Refinement of Designs



Additional Information

**Tags**

Tag 4 Add

Tag 1 × Tag 2 × Tag 3 ×

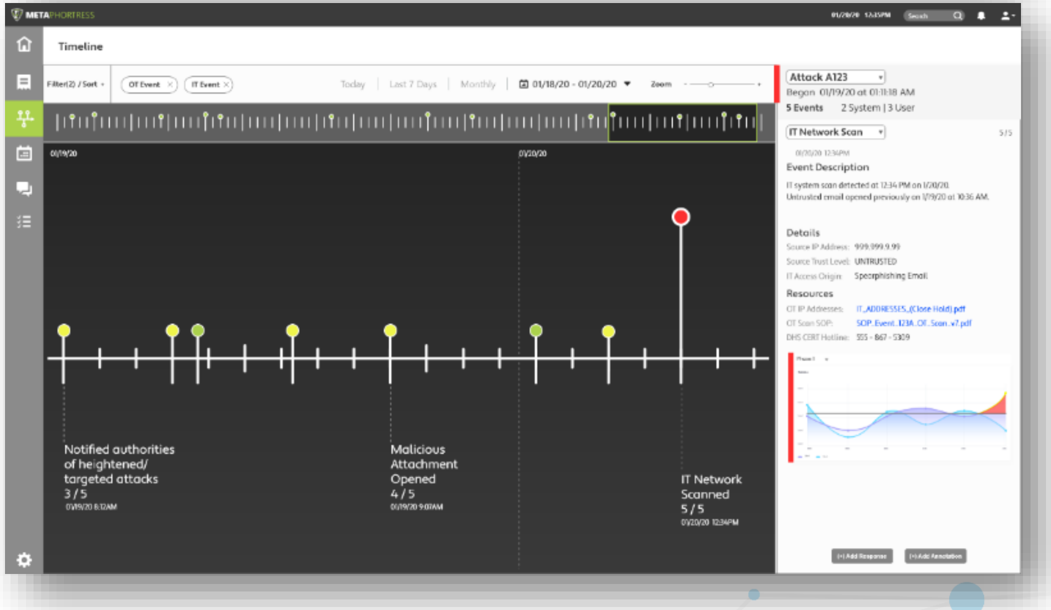
**Attach Note**

Attach

⚠ **System Alert** OT System Sensor 7

Lorem ipsum dolor sit amet, consectetur adipiscing elit, sed do eiusmod tempor incididunt ut labore et dolore magna aliqua. Do you want to send to the appropriate contacts?

Send Do Not Send



Notified authorities of heightened/ targeted attacks
3 / 5
01/19/20 8:12AM

Malicious Attachment Opened
4 / 5
01/19/20 9:07AM

IT Network Scanned
5 / 5
01/20/20 12:34PM

Attack A123
Begon 01/19/20 at 01:11:18 AM
5 Events 2 System | 3 User

IT Network Scan 5/5

01/20/20 12:34PM

Event Description

IT system scan detected at 12:34 PM on 1/20/20.
Untrusted email opened previously on 1/19/20 at 10:36 AM.

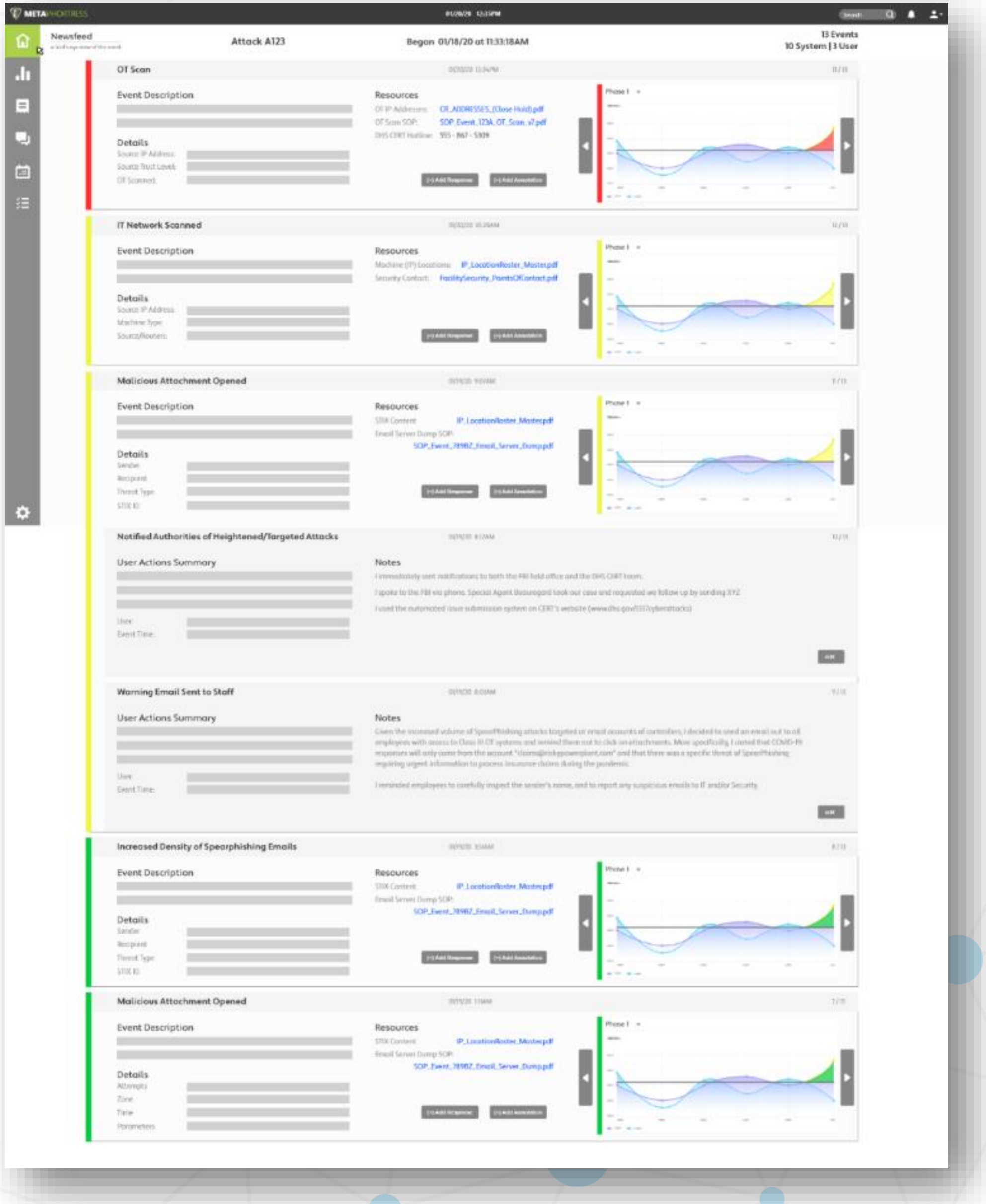
Details

Source IP Address: 999.999.9.99
Source Trust Level: UNTRUSTED
IT Access Origin: Spearphishing Email

Resources

OT IP Addresses: IT_ADDRESSES_(Close Hold).pdf
OT Scan SOP: SOP_Event_123A_OT_Scan_v7.pdf
DHS CERT Hotline: 555 - 867 - 5309

(+) Add Response (+) Add Annotation



Newsfeed

Attack A123 Begon 01/18/20 at 11:33:18AM 13 Events 10 System | 3 User

**OT Scan**

Event Description

Details
Source IP Address:
Source Trust Level:
OT Scanned:

Resources
OT IP Addresses: OT_ADDRESSES_(Close Hold).pdf
OT Scan SOP: SOP_Event_123A_OT_Scan_v7.pdf
DHS CERT Hotline: 555 - 867 - 5309

(+) Add Response (+) Add Annotation

**IT Network Scanned**

Event Description

Details
Source IP Address:
Machine Type:
Source/Routers:

Resources
Machine (IP) Locations: IP_LocationRoster_Master.pdf
Security Contact: FacilitySecurity_PointsOfContact.pdf

**Malicious Attachment Opened**

Event Description

Details
Sender:
Recipient:
Threat Type:
STIX ID:

Resources
STIX Content: IP_LocationRoster_Master.pdf
Email Server Dump SOP: SOP_Event_78987_Email_Server_Dump.pdf

**Notified Authorities of Heightened/Targeted Attacks**

User Actions Summary

User:
Event Time:

Notes

I immediately sent notifications to both the FBI field office and the DHS CERT team.

I spoke to the FBI via phone. Special Agent Beauregard took our case and requested we follow up by sending XYZ.

I used the automated issue submission system on CERT's website (www.dhs.gov/[illegible]/cyberattacks)

**Warning Email Sent to Staff**

User Actions Summary

User:
Event Time:

Notes

Given the increased volume of SpearPhishing attacks targeted at email accounts of controllers, I decided to send an email out to all employees with access to Class III OT systems and remind them not to click on attachments. More specifically, I stated that COVID-19 responses will only come from the account "claims@[illegible].com" and that there was a specific threat of SpearPhishing requiring urgent information to process insurance claims during the pandemic.

I reminded employees to carefully inspect the sender's name, and to report any suspicious emails to IT and/or Security.

**Increased Density of Spearphishing Emails**

Event Description

Details
Sender:
Recipient:
Threat Type:
STIX ID:

Resources
STIX Content: IP_LocationRoster_Master.pdf
Email Server Dump SOP: SOP_Event_78987_Email_Server_Dump.pdf

**Malicious Attachment Opened**

Event Description

Details
Attempts:
Zone:
Time:
Parameters:

Resources
STIX Content: IP_LocationRoster_Master.pdf
Email Server Dump SOP: SOP_Event_78987_Email_Server_Dump.pdf

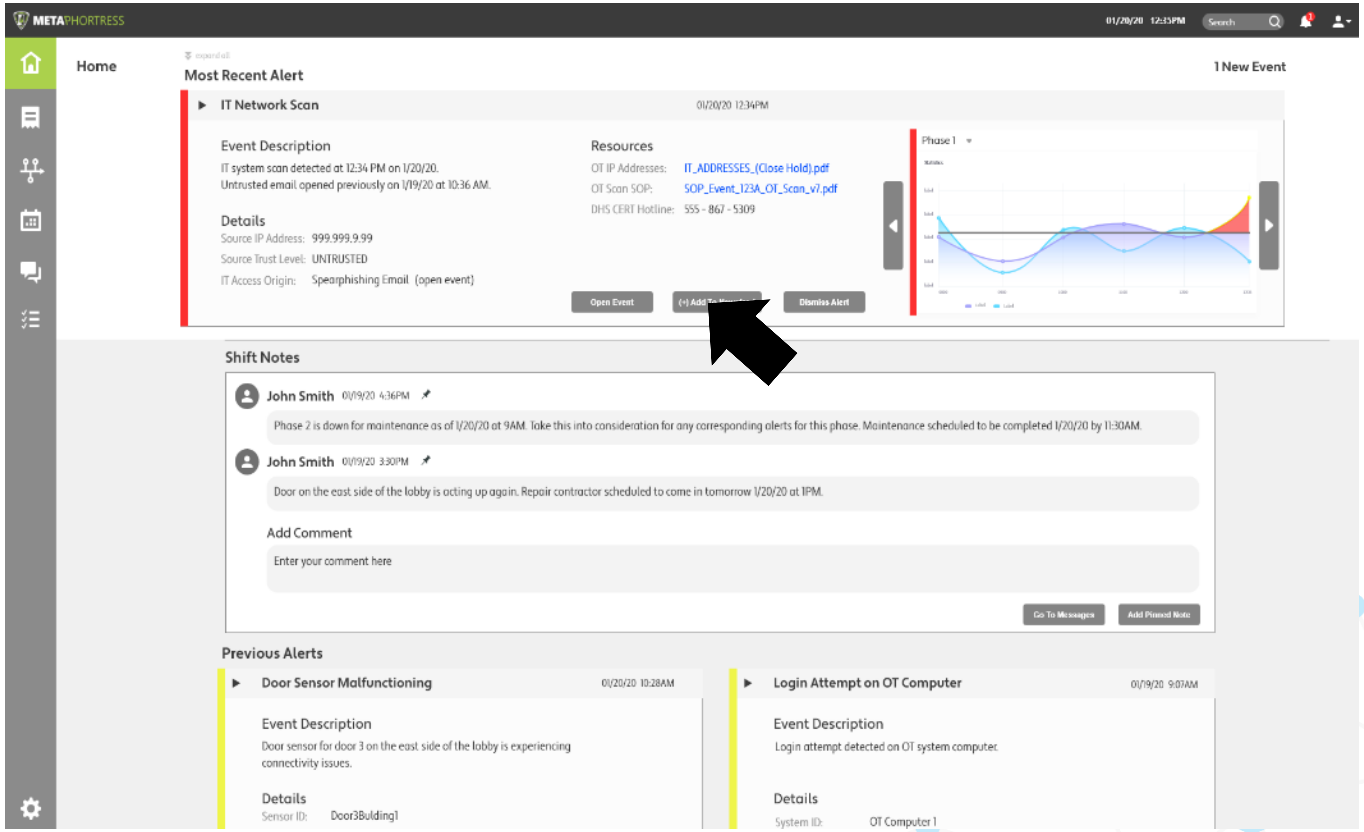
# Concept of Operations (CONOPS) Development

We are developing a CONOPS document that will provide a framework for assessing the strategy and path to market:

- Identify the who/what/where/when/why of:
  - System installation
  - System maintenance/updates
  - AI/ML model maintenance
  - User training
- Proactively provide inputs to:
  - User requirements
  - Performance specifications
  - System designs (beyond the user interface)

# User Research/Testing

- In order to continue our human factors research with power plant stakeholders, while obeying COVID-19 isolation requirements, we have developed remote methods.
- Remote knowledge elicitation (KE) activities include:
  - First Click Testing
  - Tree Testing
  - Verbal Protocol Analysis
  - Interviews



Most Recent Alert

1 New Event

IT Network Scan 01/20/20 12:34PM

Event Description

IT system scan detected at 12:34 PM on 1/20/20.
Untrusted email opened previously on 1/19/20 at 10:36 AM.

Details

Source IP Address: 999.999.9.99
Source Trust Level: UNTRUSTED
IT Access Origin: Spearphishing Email (open event)

Resources

OT IP Addresses: IT_ADDRESSES_(Close Hold).pdf
OT Scan SOP: SOP_Event_123A_OT_Scan_v7.pdf
DHS CERT Hotline: 555 - 867 - 5309

Shift Notes

John Smith 01/19/20 4:36PM

Phase 2 is down for maintenance as of 1/20/20 at 9AM. Take this into consideration for any corresponding alerts for this phase. Maintenance scheduled to be completed 1/20/20 by 11:30AM.

John Smith 01/19/20 3:30PM

Door on the east side of the lobby is acting up again. Repair contractor scheduled to come in tomorrow 1/20/20 at 1PM.

Add Comment

Enter your comment here

Previous Alerts

Door Sensor Malfunctioning 01/20/20 10:28AM

Event Description

Door sensor for door 3 on the east side of the lobby is experiencing connectivity issues.

Details

Sensor ID: Door3Bulding1

Login Attempt on OT Computer 01/19/20 9:07AM

Event Description

Login attempt detected on OT system computer.

Details

System ID: OT Computer 1

METAPHORTRESS

# Conclusions

# Conclusions

METAPHORTRESS

- MetaPhortress will increase SA and cybersecurity at fossil energy generation plants by:
  - Fusing information from classically disparate domains (IT, OT, PACS)
  - Using Machine Learning (ML) to detect potential cyber threats
  - Provide operators with an intuitive interface that encourages sensemaking of voluminous and highly uncertain data
- Challenges include:
  - Developing an initial capability and a robust training dataset
  - Continued recruitment and retention of participants for user research
- Next steps:
  - Iterative user research and testing
  - Iterative refinement and development of system capabilities
  - Development of CONOPS to guide transition to market

# References

- Goyal, N., Leshed, G., & Fussell, S. R. (2013). Effects of visualization and note-taking on sensemaking and analysis. CHI '13: Proceedings of the SIGCHI Conference on Human Factors in Computing Systems April 2013 Pages 2721–2724. https://doi.org/10.1145/2470654.2481376
- Hackos, J. T. & Redish, J. C. (1998). User and Task Analysis for Interface Design. New York: John Wiley & Sons.
- McCarthy, J., et al (2019). SP 1800-7 Situational Awareness for Electric Utilities. National Institute of Standards and Technology.
- Pirolli, P. & Russell, D. M. (2011). Introduction to this Special Issue on Sensemaking. Human–Computer Interaction, 26, 1-8.
- Wong, B. L. W. (2014). How Analysts Think (?): Early Observations, 2014 IEEE Joint Intelligence and Security Informatics Conference, The Hague, 2014, pp. 296-299.