INL/CON-21-63826-Revision-0

HP in Cybersecurity: CyOTE

August 2021

Samuel Douglas Chanoski, Julio G Rodriguez

DISCLAIMER

This information was prepared as an account of work sponsored by an agency of the U.S. Government. Neither the U.S. Government nor any agency thereof, nor any of their employees, makes any warranty, expressed or implied, or assumes any legal liability or responsibility for the accuracy, completeness, or usefulness, of any information, apparatus, product, or process disclosed, or represents that its use would not infringe privately owned rights. References herein to any specific commercial product, process, or service by trade name, trade mark, manufacturer, or otherwise, does not necessarily constitute or imply its endorsement, recommendation, or favoring by the U.S. Government or any agency thereof. The views and opinions of authors expressed herein do not necessarily state or reflect those of the U.S. Government or any agency thereof.

INL/CON-21-63826-Revision-0

HP in Cybersecurity: CyOTE

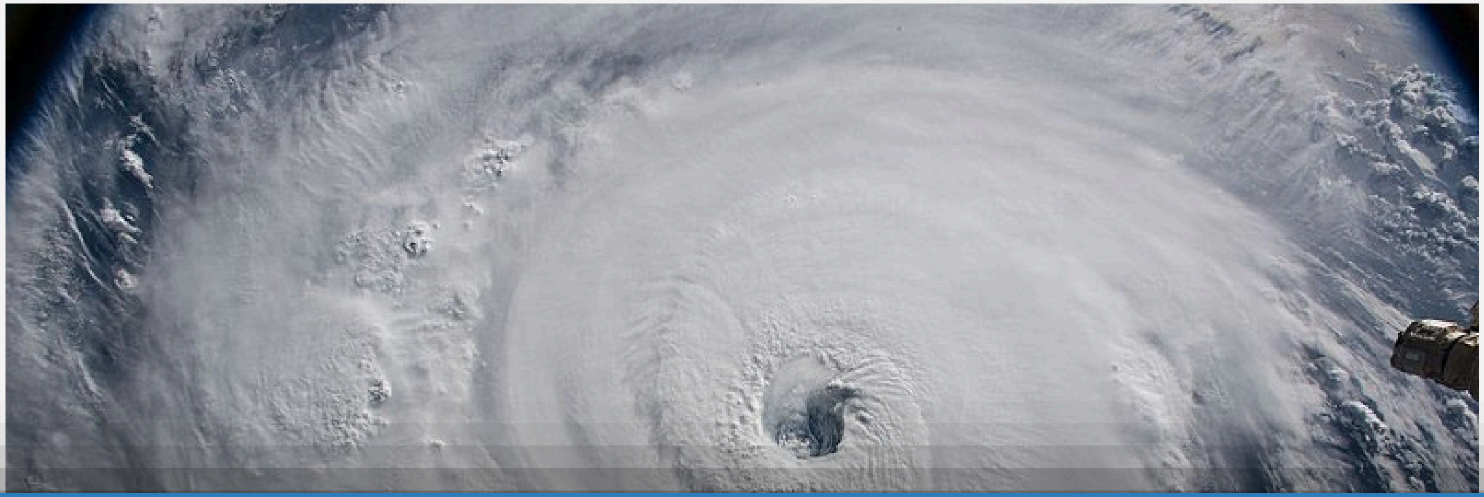
Samuel Douglas Chanoski, Julio G Rodriguez

August 2021

Idaho National Laboratory
Idaho Falls, Idaho 83415

http://www.inl.gov

Prepared for the
U.S. Department of Energy
Under DOE Idaho Operations Office
Contract DE-AC07-05ID14517



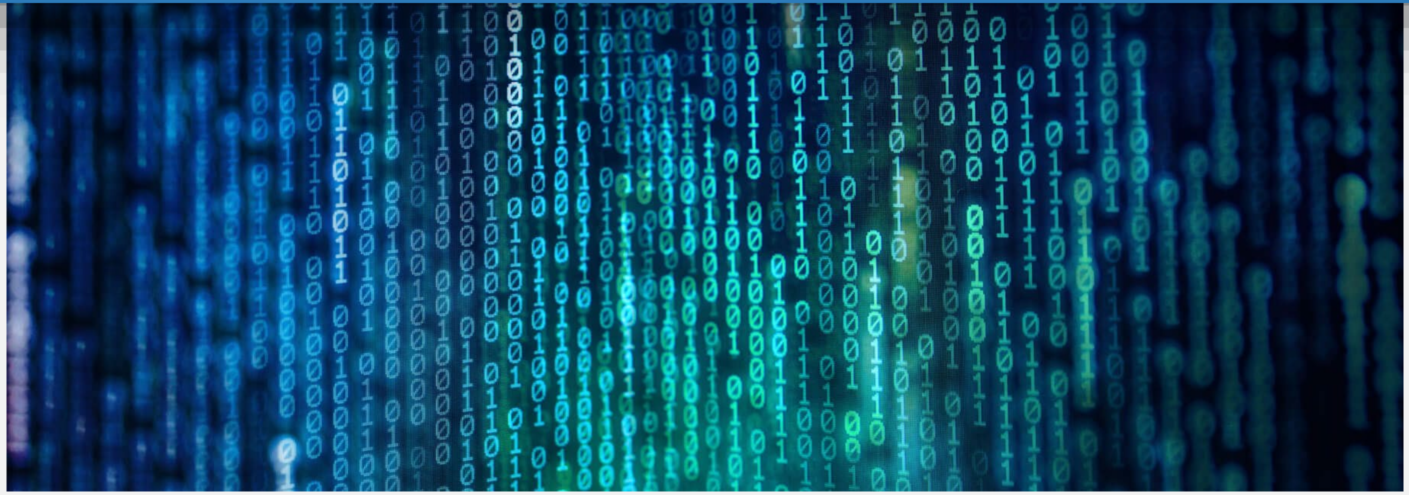
U.S. DEPARTMENT OF ENERGY

OFFICE OF
Cybersecurity, Energy Security,
and Emergency Response

CyOTE
Cybersecurity for the
Operational Technology
Environment

HP in Cybersecurity: CyOTE™

ReliabilityFirst Human Performance Workshop – August 12, 2021 – Sam Chanoski, Idaho National Laboratory



CyOTE Purpose and Goals

CyOTE Cybersecurity for the Operational Technology Environment

U.S. DEPARTMENT OF ENERGY | OFFICE OF Cybersecurity, Energy Security, and Emergency Response

What Need is CyOTE Targeting?

Today's energy sector IT and OT systems are **complex and interconnected**.

Sophisticated adversaries have the knowledge to target OT environments that result in **physical disruptions** to energy flows or damaged equipment.

Industry visibility, monitoring, and analysis capabilities in the OT space are still relatively new and immature—leaving asset owners and operators (AOOs) struggling to **determine** whether **anomalous operational events** potentially have a malicious cyber cause.

We need to **change the paradigm** for security and begin thinking of security as a holistic analysis of business operations to **identify anomalies** from unalterable data sources and investigate further from those sources.

What is the Problem CyOTE is Trying to Address?

Most AOOs lack the capability to analyze data from their OT networks effectively and consistently identify attacks, much less in real time – in significant contrast to their IT networks.

Even those who have some capabilities still want and need to improve their level of OT understanding.

Improving understanding of OT data enables AOOs to make better risk-informed decisions to secure their OT environments.

Challenges

Regulations limit the information that can be shared.

Geographic dispersion of assets in the field.

Communications channels may be limited.

No common lexicon for data fields and threat information.

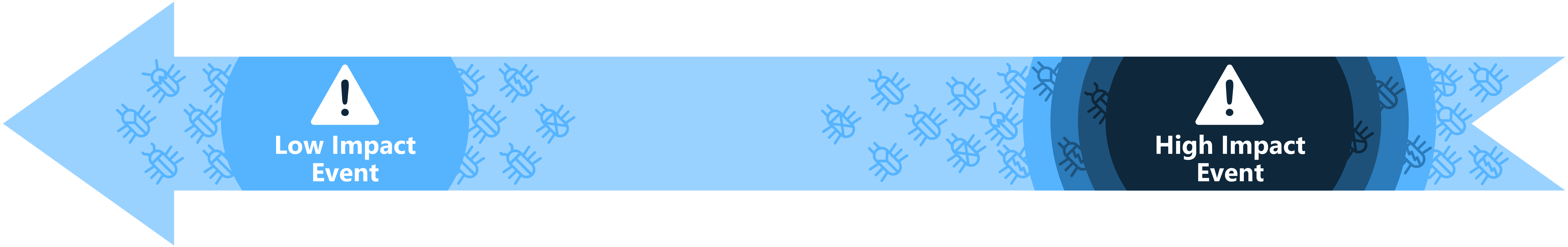
Understanding anomalies in operations.

CyOTE Vision

Develop a threat identification capability for energy sector asset owners and operators to independently identify indicators of attack within their operational technology (OT) networks.

Solution

CyOTE aims to move the energy sector AOO’s threat detection capability **earlier into an attack campaign**. The better understanding an asset owner has into their OT environment, the less obvious anomalies they may be able to confidently identify as either an attack technique or a non-malicious operational failure. This shifts the AOO’s threat detection capability **earlier into an attack campaign** to **identify attacks with ever-decreasing impacts**.



Leveraging HOP Principles

CyOTE Cybersecurity for the Operational Technology Environment

U.S. DEPARTMENT OF ENERGY | OFFICE OF Cybersecurity, Energy Security, and Emergency Response

Central Concept

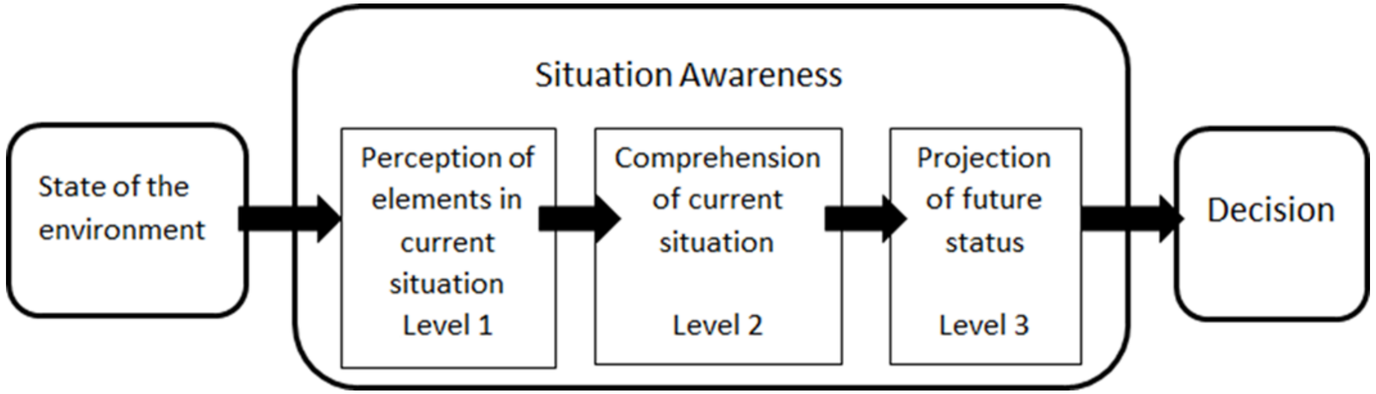
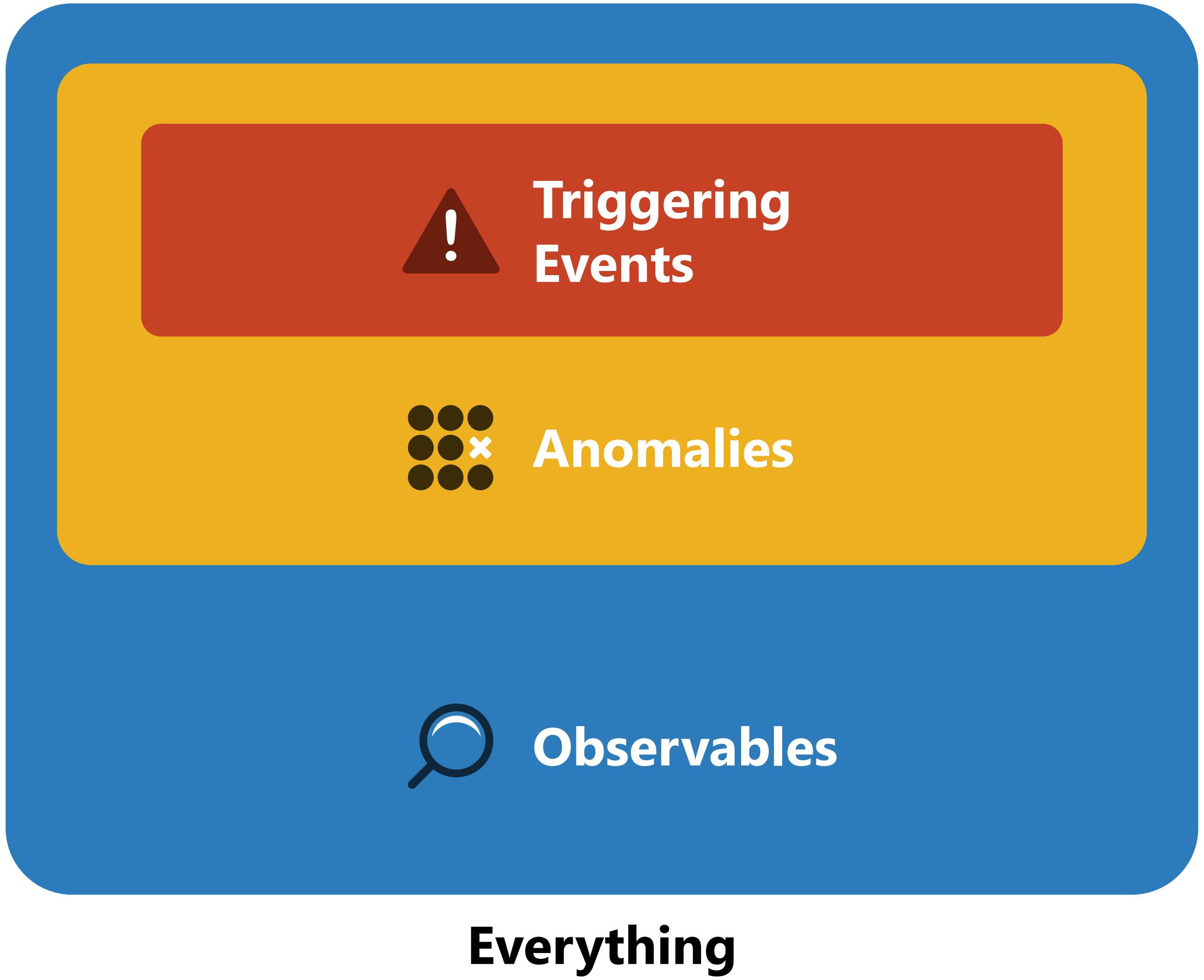

State of the environment
Situation Awareness
Perception of elements in current situation
Level 1
Comprehension of current situation
Level 2
Projection of future status
Level 3
Decision

Image: https://www.nerc.com/comm/RSTC_Reliability_Guidelines/SA_for_System_Operators.pdf

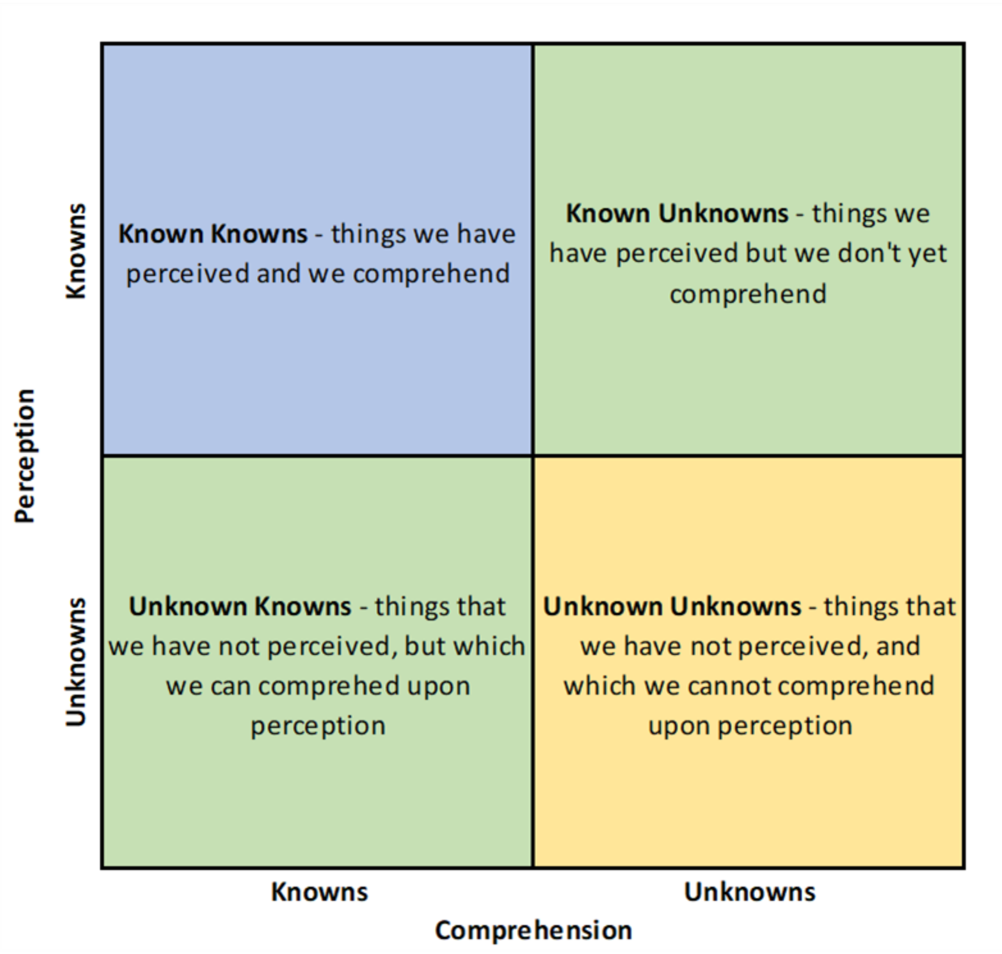
- Adapted from Endsley's 1995 Model of Situation Awareness
- Perception: individual human ability to detect an observable
- Comprehension: organizational human ability to understand an observable

Nested Mental Model of Occurrences



- **Observable:** an occurrence that can be perceived
- **Anomaly:** an observable different from what is expected or “normal”
- **Triggering event:** an anomaly that merits investigation

Knowns and Unknowns



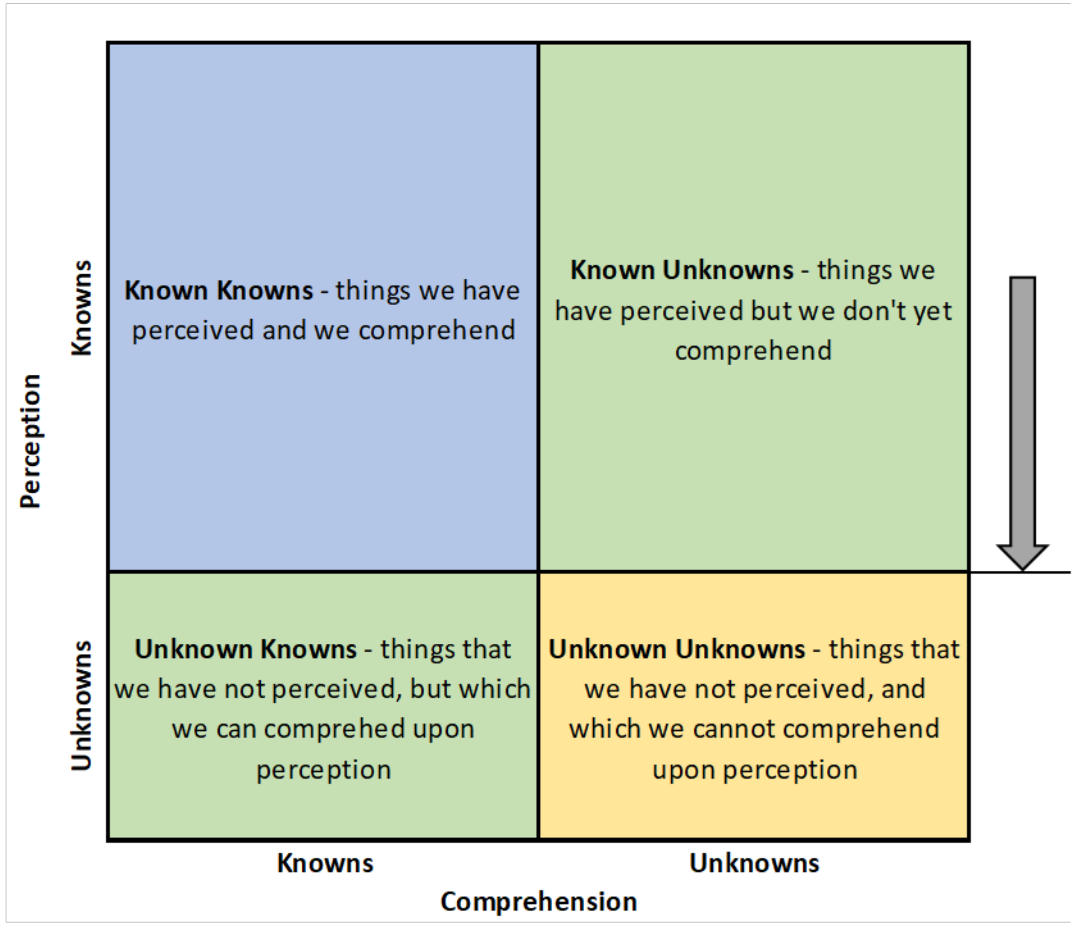
Perception

	Knowns	Unknowns
Knowns	**Known Knowns** - things we have perceived and we comprehend	**Known Unknowns** - things we have perceived but we don't yet comprehend
Unknowns	**Unknown Knowns** - things that we have not perceived, but which we can comprehed upon perception	**Unknown Unknowns** - things that we have not perceived, and which we cannot comprehend upon perception

Comprehension

- The world is divided into Knowns and Unknowns
- Division applies to perception and to comprehension

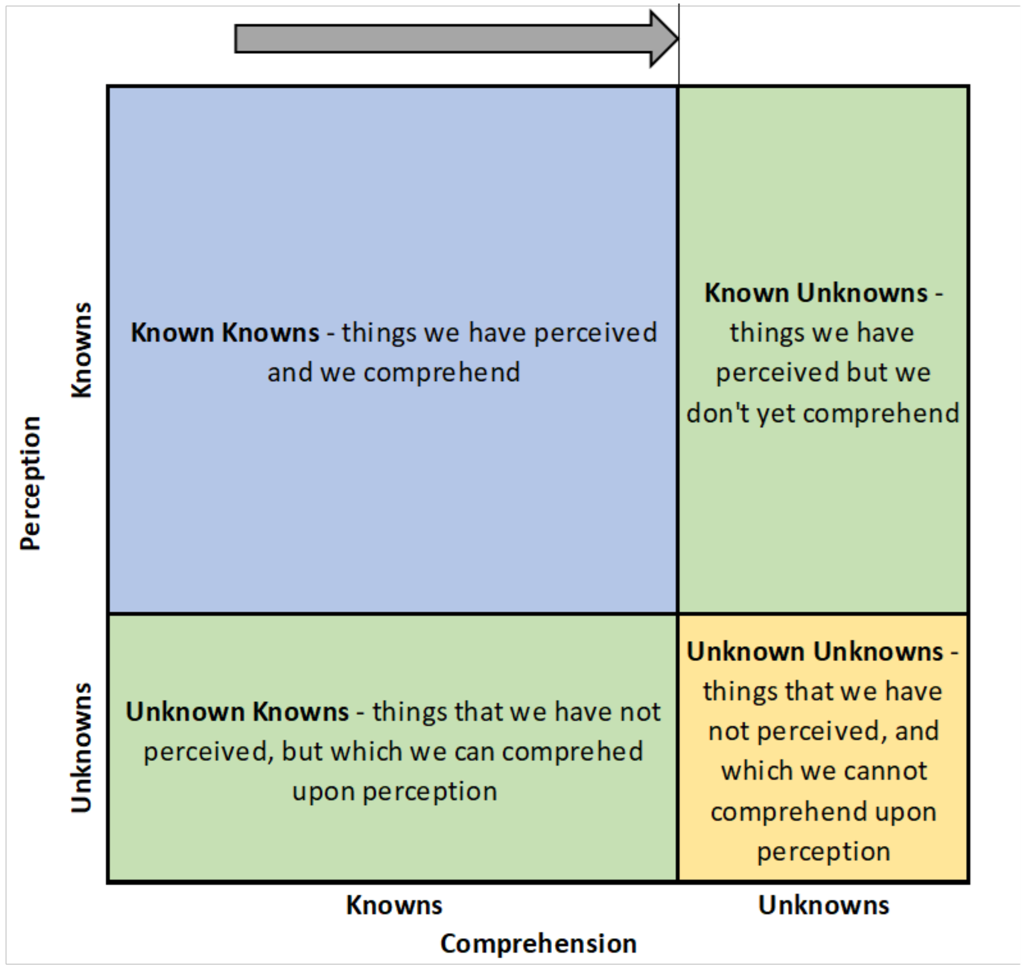
Improving Perception



Perception		Comprehension: Knowns	Comprehension: Unknowns
	Knowns	**Known Knowns** - things we have perceived and we comprehend	**Known Unknowns** - things we have perceived but we don't yet comprehend
	Unknowns	**Unknown Knowns** - things that we have not perceived, but which we can comprehed upon perception	**Unknown Unknowns** - things that we have not perceived, and which we cannot comprehend upon perception

- Improving our perception shrinks the Unknown world
- Conscious visibility
- Still need to understand the newly perceived observables

Improving Comprehension



Perception \ Comprehension	Knowns	Unknowns
Knowns	**Known Knowns** - things we have perceived and we comprehend	**Known Unknowns** - things we have perceived but we don't yet comprehend
Unknowns	**Unknown Knowns** - things that we have not perceived, but which we can comprehed upon perception	**Unknown Unknowns** - things that we have not perceived, and which we cannot comprehend upon perception

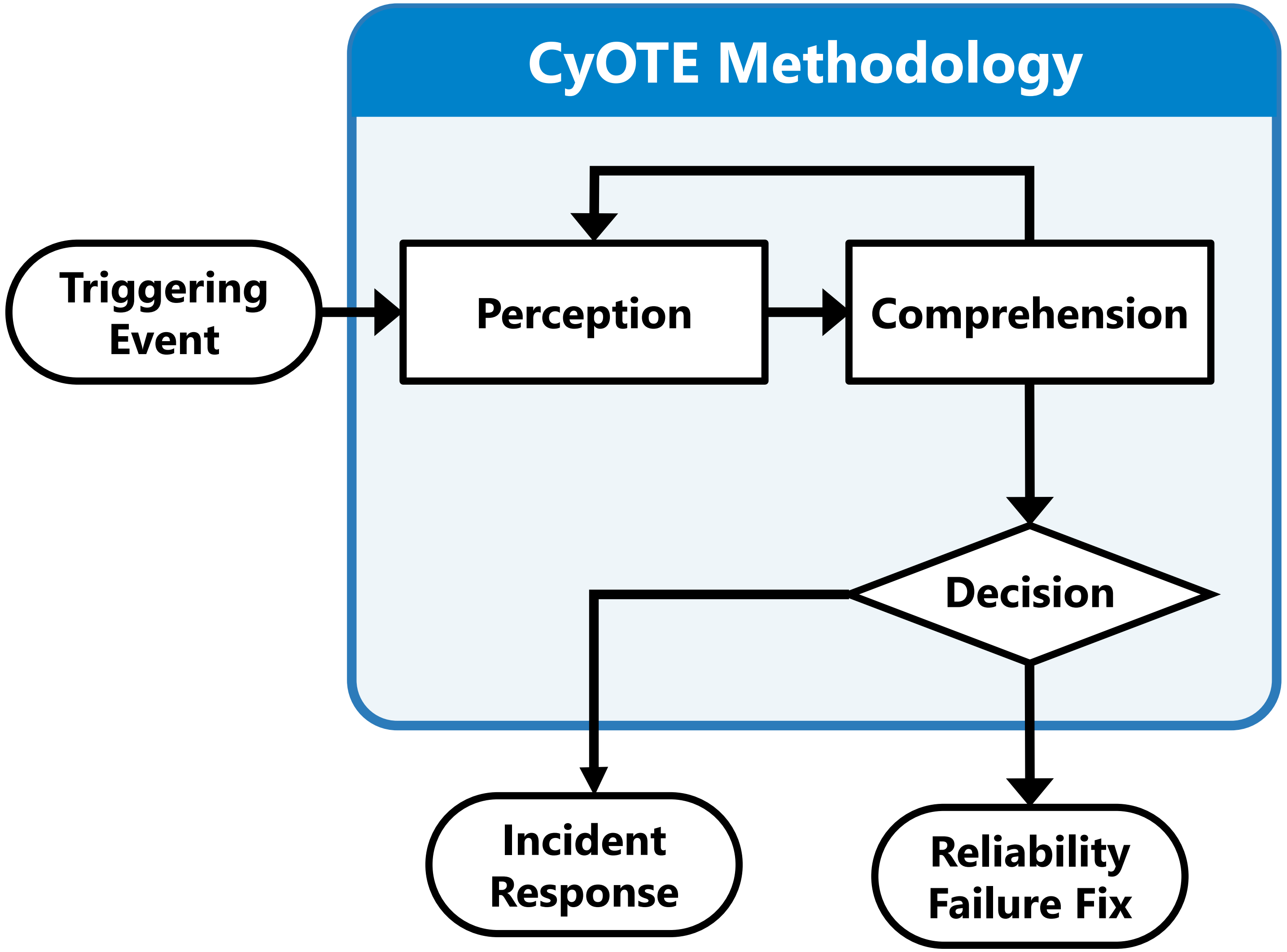
- Improving our comprehension further shrinks the unknown world
- Better idea of what not-yet-perceived observables look like (Fact Sheets and Recipes)

Organizational Capabilities

- Relationships between departments
- Energy monitoring capabilities and practices
- Capability to respond to and resolve reliability failures
- Capability to respond to and resolve cybersecurity incidents*
- Understanding of organizational risk appetite*
- Capability for organizational learning and continuous improvement
- OT instrumented visibility*

* Relates to a Cybersecurity Capability Maturity Model (C2M2) domain

CyOTE Methodology Overview



- How to understand the information you have, not get more data
- Applies concepts of perception and comprehension to a world of Knowns and Unknowns
- MITRE ATT&CK® Framework for ICS is a central part of our common lexicon
- Endpoint is making a risk-informed decision to conduct incident response or to treat as a reliability failure
- Over time, detect fainter signals sooner

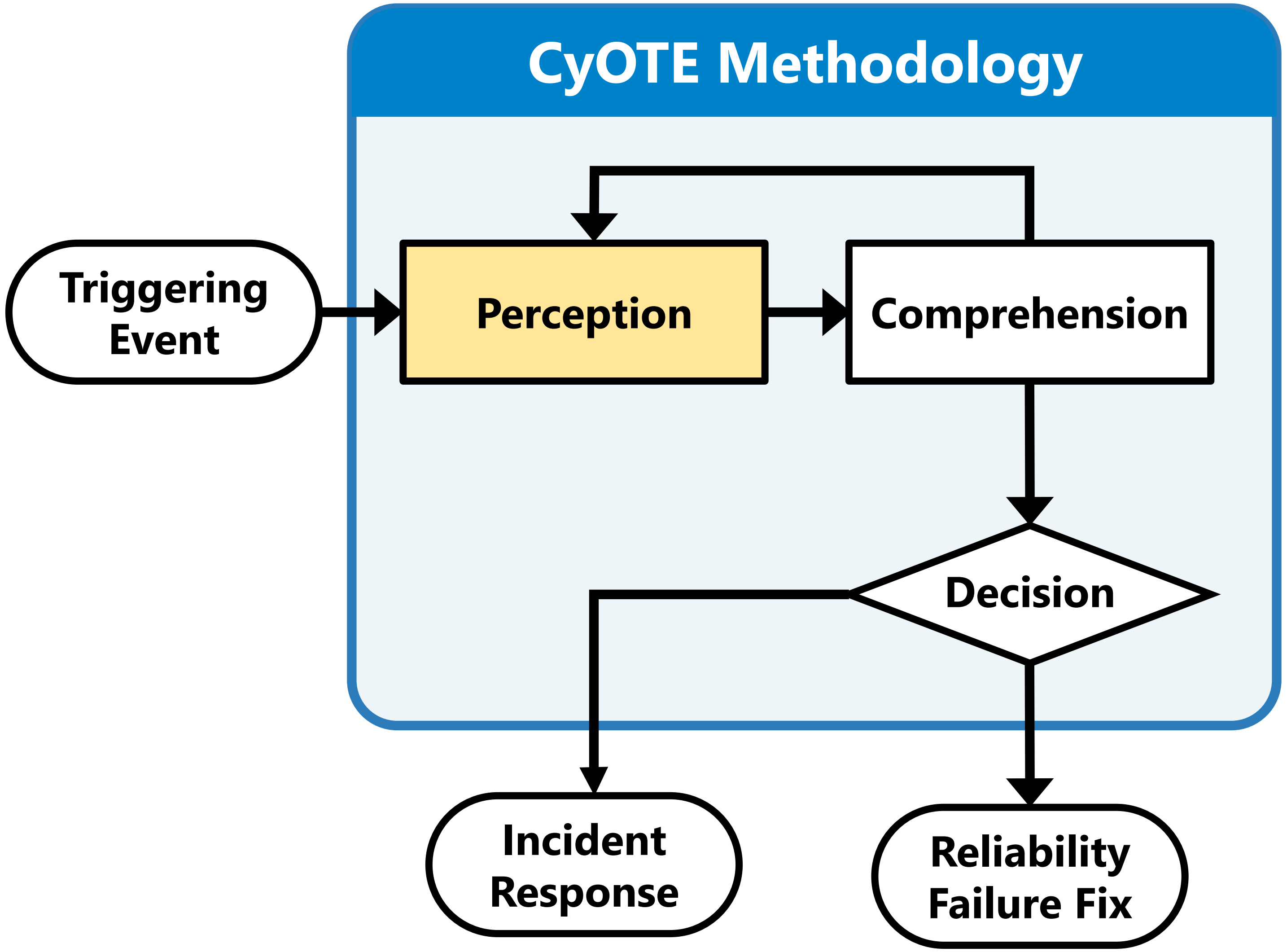
Initial Access	Execution	Persistence	Evasion	Discovery	Lateral Movement	Collection	Command and Control	Inhibit Response Function	Impair Process Control	Impact
Data Historian Compromise 🟩🟦🟧	✓ Change Program State 🟩🟦🟧	Hooking	Exploitation for Evasion	✓ Control Device Identification 🟩🟦	✓ Default Credentials 🟦	Automated Collection 🟩	Commonly Used Port 🟩	Activate Firmware Update Mode 🟩	✓ Brute Force I/O 🟦🟧	Damage to Property 🟩🟦🟧
Drive-by Compromise	Command-Line Interface	✓ Module Firmware 🟧	✓ Indicator Removal on Host 🟩🟦🟧	✓ I/O Module Discovery	Exploitation of Remote Services 🟩🟦	✓ Data from Information Repositories 🟩🟦🟧	✓ Connection Proxy 🟦	Alarm Suppression 🟧	✓ Change Program State 🟩🟦🟧	Denial of Control 🟩🟦🟧
Engineering Workstation Compromise 🟩🟦🟧	Execution through API 🟩	✓ Program Download 🟩🟦🟧	Masquerading 🟧	Network Connection Enumeration	External Remote Services 🟦	✓ Detect Operating Mode 🟩🟦	Standard Application Layer Protocol 🟩🟦	Block Command Message 🟩🟧	Masquerading 🟧	Denial of View 🟩🟦🟧
Exploit Public-Facing Application 🟦	Graphical User Interface 🟩	Project File Infection 🟩🟦	Rogue Master Device 🟦🟧	Network Service Scanning	Program Organization Units 🟩🟦	Detect Program State 🟩🟦		✓ Block Reporting Message 🟩🟧	✓ Modify Control Logic 🟩🟧	Loss of Availability 🟩🟦🟧
External Remote Services 🟦	Man-in-the-middle	System Firmware 🟧	Rootkit 🟩🟦	Network Sniffing	✓ Remote File Copy 🟩🟦	I/O Image		Block Serial COM 🟧	✓ Modify Parameter 🟩🟧	Loss of Control 🟩🟦🟧
Internet Accessible Devices 🟦	Program Organization Units 🟩🟦	Valid Accounts 🟩🟦	✓ Spoof Reporting Message 🟩🟧	Remote System Discovery 🟩🟦	Valid Accounts 🟩🟦	Location Identification		✓ Data Destruction 🟩🟦	✓ Module Firmware 🟧	Loss of Productivity and Revenue
Replication Through Removable Media 🟩	Project File Infection 🟩🟦		✓ Utilize/Change Operating Mode 🟩🟦🟧	Serial Connection Enumeration		Monitor Process State 🟩🟦		✓ Denial of Service 🟩🟦🟧	✓ Program Download 🟩🟦🟧	Loss of Safety 🟩🟧
Spearphishing Attachment	Scripting					✓ Point & Tag Identification 🟩🟦		✓ Device Restart/ Shutdown 🟧	Rogue Master Device 🟦🟧	Loss of View 🟩🟦🟧
Supply Chain Compromise 🟩🟦	User Execution 🟩🟦					✓ Program Upload 🟩🟦		Manipulate I/O Image 🟦	✓ Service Stop 🟩🟦🟧	Manipulation of Control 🟩🟦🟧
Wireless Compromise 🟦						Role Identification 🟦		✓ Modify Alarm Settings 🟩🟦🟧	✓ Spoof Reporting Message 🟩🟧	Manipulation of View 🟦🟧
						Screen Capture 🟩		✓ Modify Control Logic 🟩🟧	✓ Unauthorized Command Message 🟩🟧	Theft of Operational Information 🟩🟦
								✓ Program Download 🟩🟦🟧		
								Rootkit 🟩🟦		
								System Firmware 🟧		
								✓ Utilize/Change Operating Mode 🟩🟦🟧		

Legend

Tactics | Techniques | Use Cases: HMI 🟩 Remote Login 🟦 Alarm Logs 🟧 | ✓ Fact Sheet

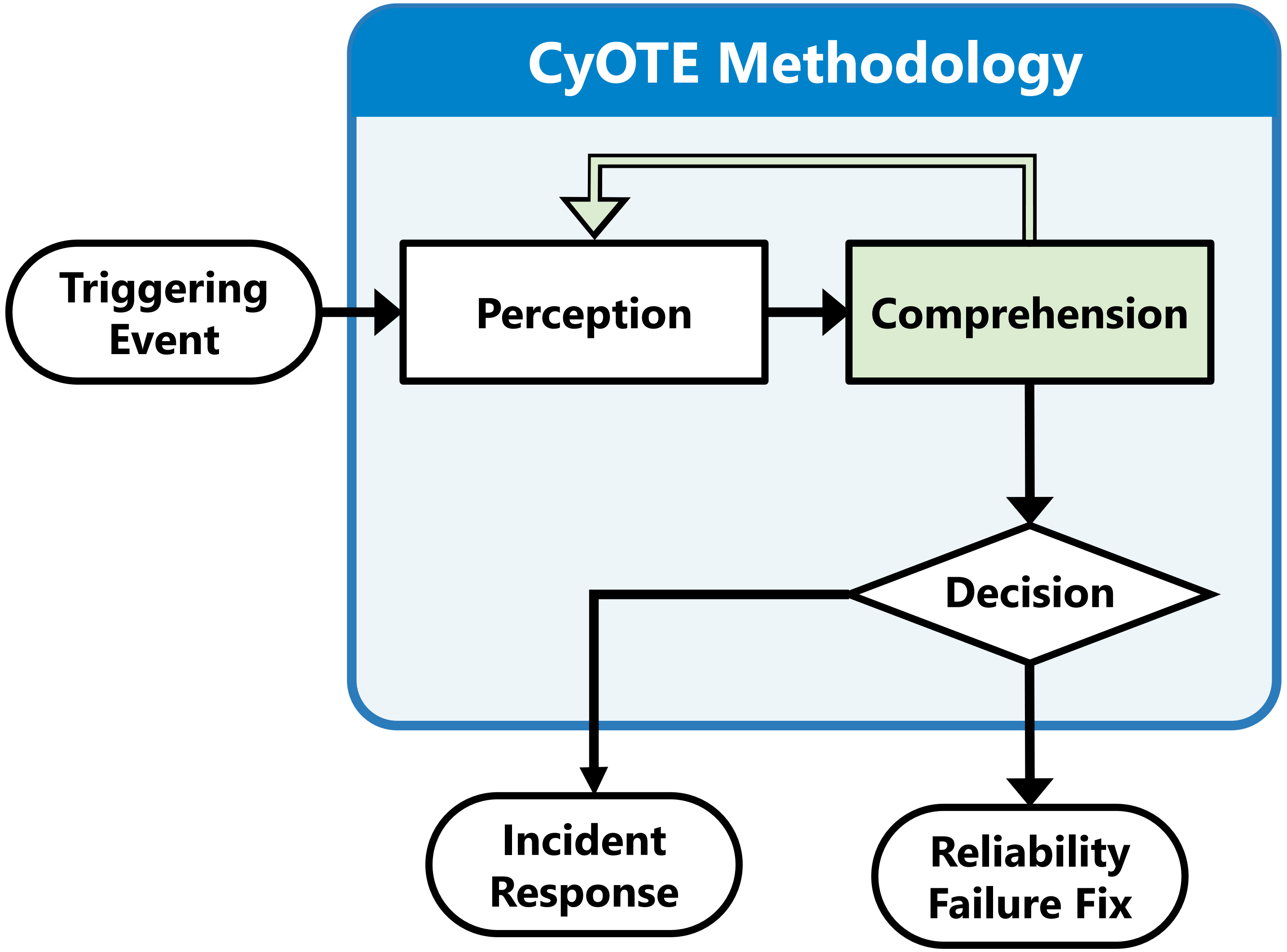
MITRE ATT&CK for ICS Matrix (October 2020)

Employment: Perception



- Define **your** triggering events
- Alarms, human pattern matching, business process exceptions
- Who else needs to know, i.e. transition from individual to organizational awareness

Employment: Comprehension

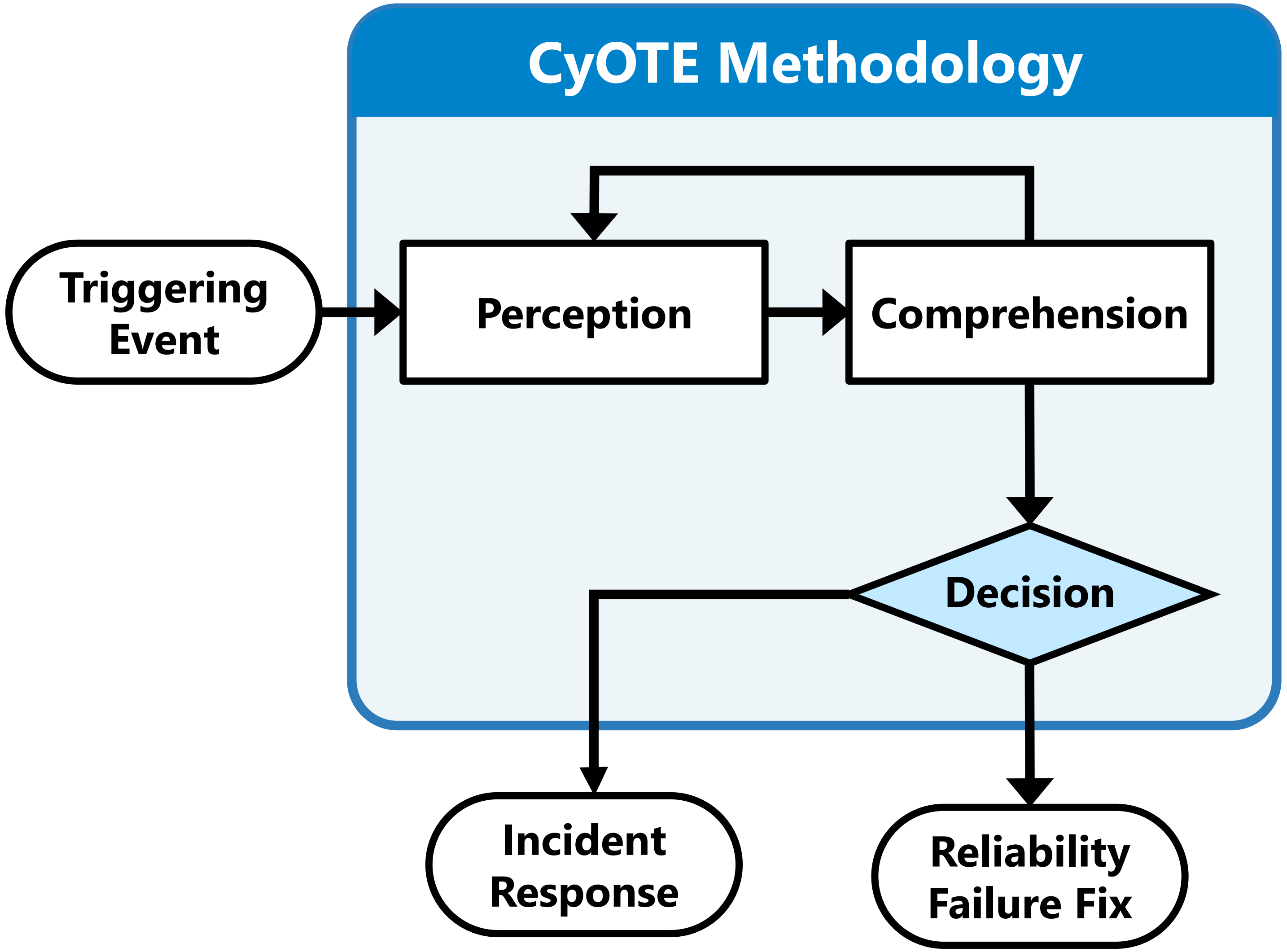


- Identify and locate sources of information
- Build context: are related observables expected or not, present or not?
- How much does this resemble a known technique?
- Knowledge management and documentation
- Recursive pivots to explore related observables

Collaboration

Organizational comprehension requires significant cooperation between disparate roles and responsibilities across an AOO's organization that may not regularly work together, including some roles that do not have traditional security responsibilities.

Employment: Decision



- Risk-informed, binary business decision on how to resolve the situation
- Scientific method analogy
  - H_0: Reliability failure
  - H_1: Incident
  - Confidence level based on risk appetite

Learning through Case Studies

- The CyOTE team is creating Case Studies using both historical OT attack scenarios and scenarios identified with AOO partners to demonstrate where AOOs could **apply the CyOTE methodology to identify effects of malicious cyber activity** and correlate the effects to techniques.
- These Case Studies provide the opportunity to **better demonstrate how the CyOTE methodology could create broader understanding of OT environments and help** identify attack campaigns with ever-decreasing impacts.

Final Thoughts

- We need to **change the paradigm** for security and begin thinking of security as a holistic analysis of business operations to identify anomalies from unmaskable data sources and conduct further investigation of any associated data.
- Correlating **operational anomalies**/observables to techniques and linking them to other anomalies provides the ability to detect attack campaigns with ever-decreasing impacts.
- Read the **full CyOTE methodology paper** at https://inl.gov/wp-content/uploads/2021/07/CyOTE-Methodology-20210625-final.pdf
- **You can help** by employing the CyOTE methodology in your organization:
  - ○ look for anomalies in your environments,
  - ○ identify anomalies that would trigger further investigations,
  - ○ correlate available data sources,
  - ○ associate additional anomalies, and
  - ○ determine if you are in the early stages of an attack campaign.

QUESTIONS and DISCUSSION

CyOTE.Program@hq.doe.gov

Sam Chanoski
Technical Relationship Manager* | *Cybercore Integration Center
samuel.chanoski@inl.gov
Idaho National Laboratory | Atlanta, GA