This paper describes objective technical results and analysis. Any subjective views or opinions that might be expressed in the paper do not necessarily represent the views of the U.S. Department of Energy or the United States Government.

SAND2022-10474C

U.S. DEPARTMENT OF ENERGY | *Office of* Cybersecurity, Energy Security, and Emergency Response

Development of a Bayesian Network to Model Malicious Cyber-Activity in Operational Technology Environments

Scott Bowman and Lee Maccarone

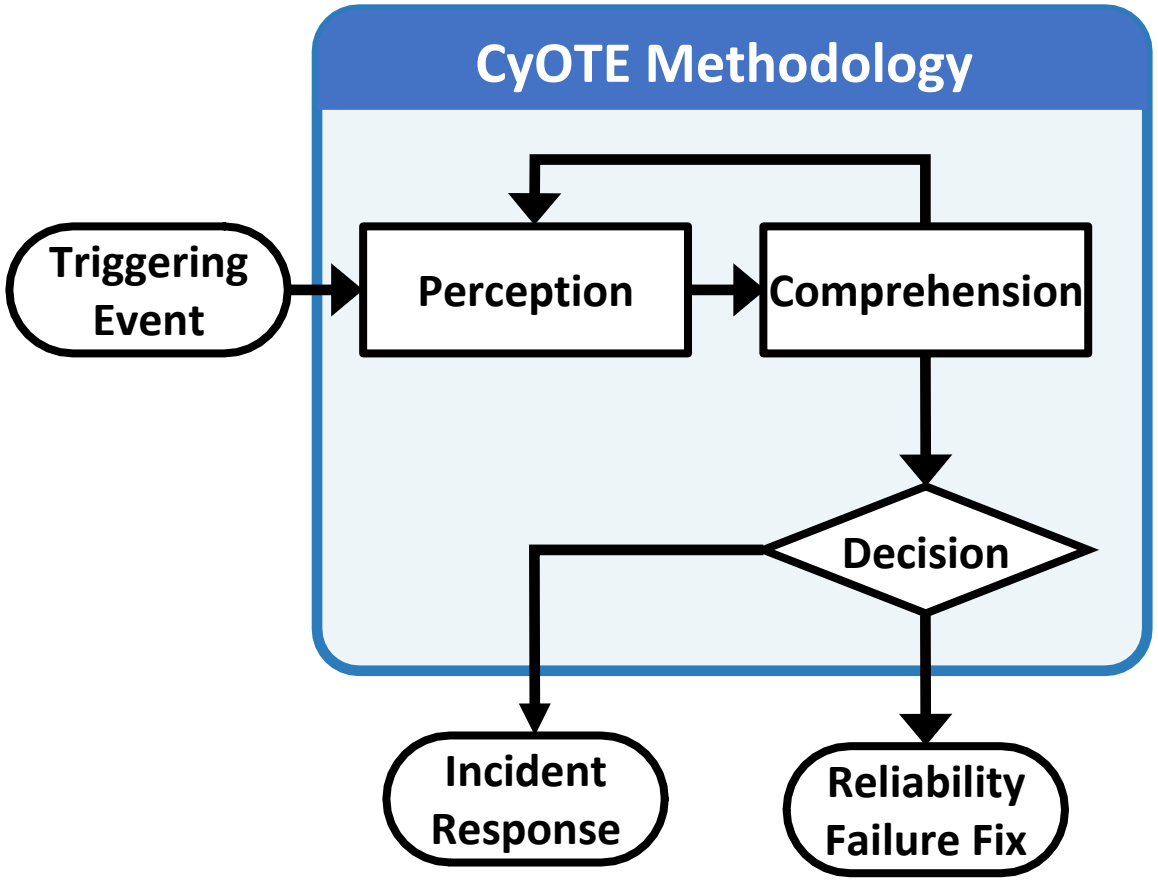
5 August 2022

Sandia National Laboratories is a multimission laboratory managed and operated by National Technology & Engineering Solutions of Sandia, LLC, a wholly owned subsidiary of Honeywell International Inc., for the U.S. Department of Energy's National Nuclear Security Administration under contract DE-NA0003525.

Agenda

- Introduction to CyOTE
- Bayesian network overview
- Refining the network
- Results for EKANS case study
- Take-aways

CyOTE Methodology Overview

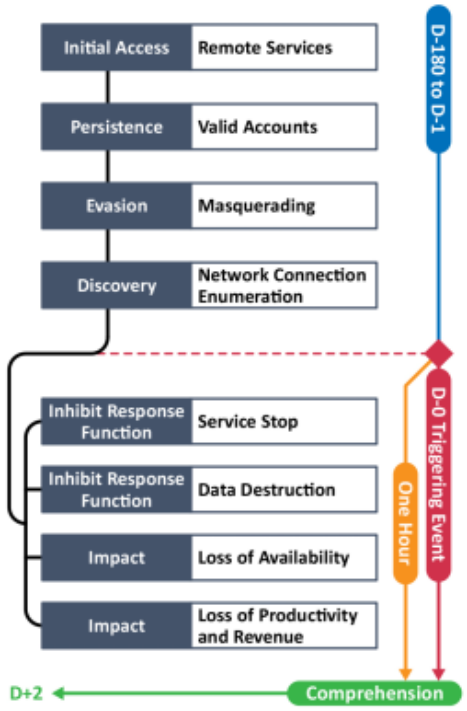


- How to understand the information you have, not get more data
- Applies concepts of perception and comprehension to a world of Knowns and Unknowns
- Endpoint is making a risk-informed decision to conduct incident response or to treat as a reliability failure
- Over time, detect fainter signals sooner

CyOTE Case Studies

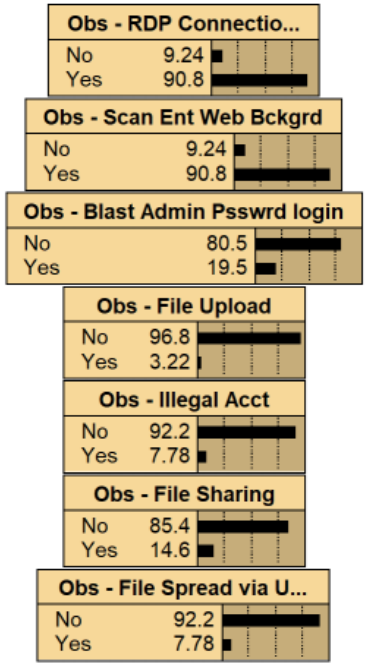
Attack Techniques

- Update risk model



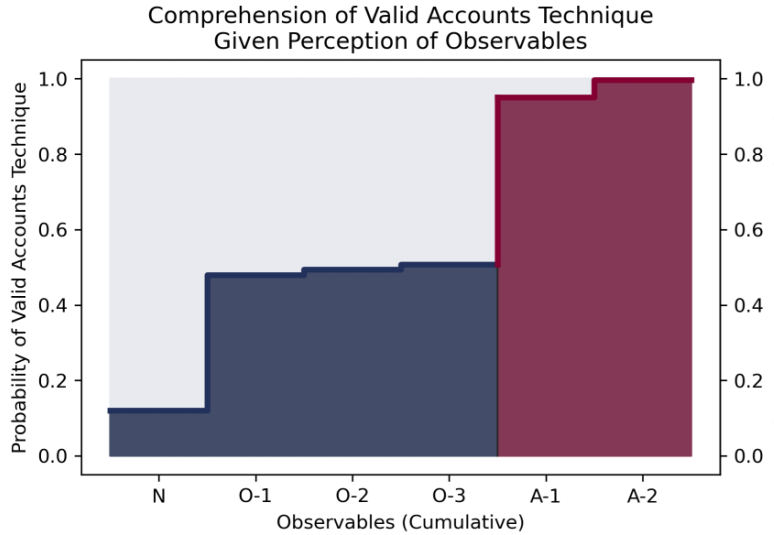
Observables of Techniques

- Update risk model



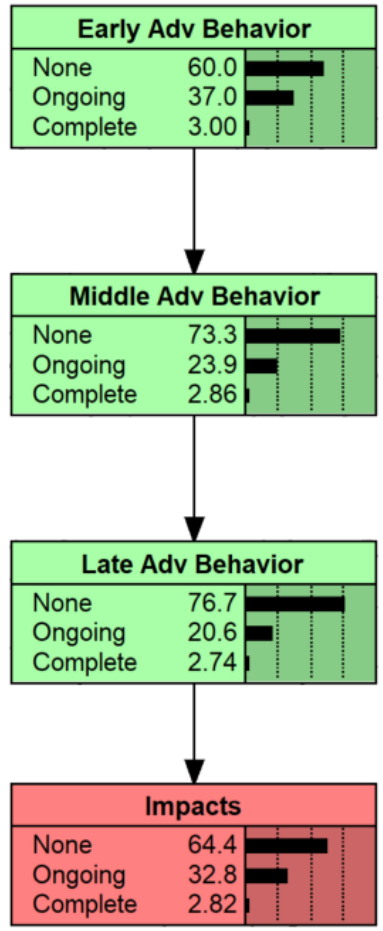
Risk Computation

- Compute risk probabilities



Risk Approach: Bayesian Networks

- Allows user to input perceived evidence via observables
- Propagate evidence via message passing algorithms
- Given observable evidence, posteriors are computed
- Enable “what-if” and sensitivity to findings analyses



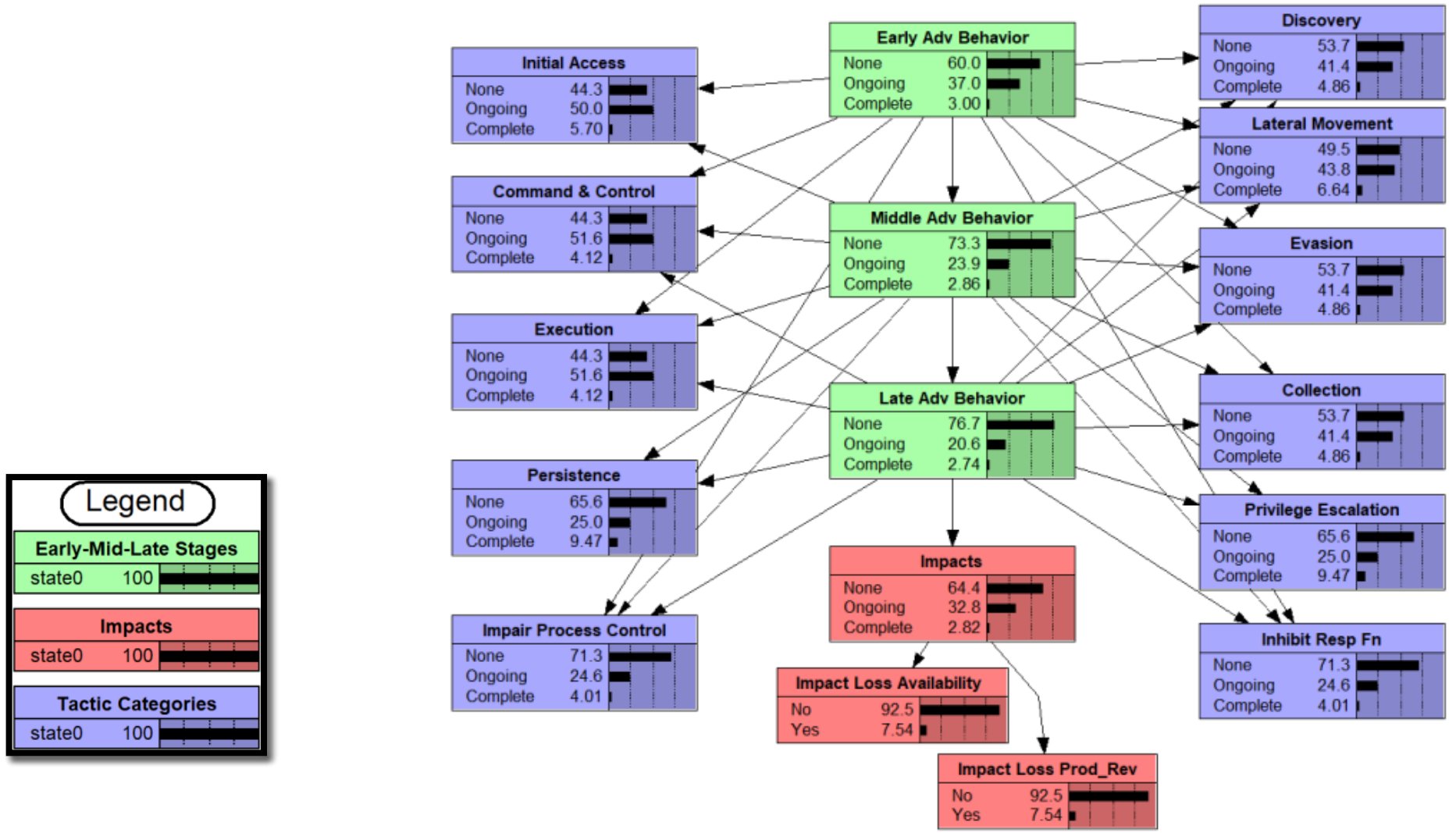
Core attack process

How is the network structured?

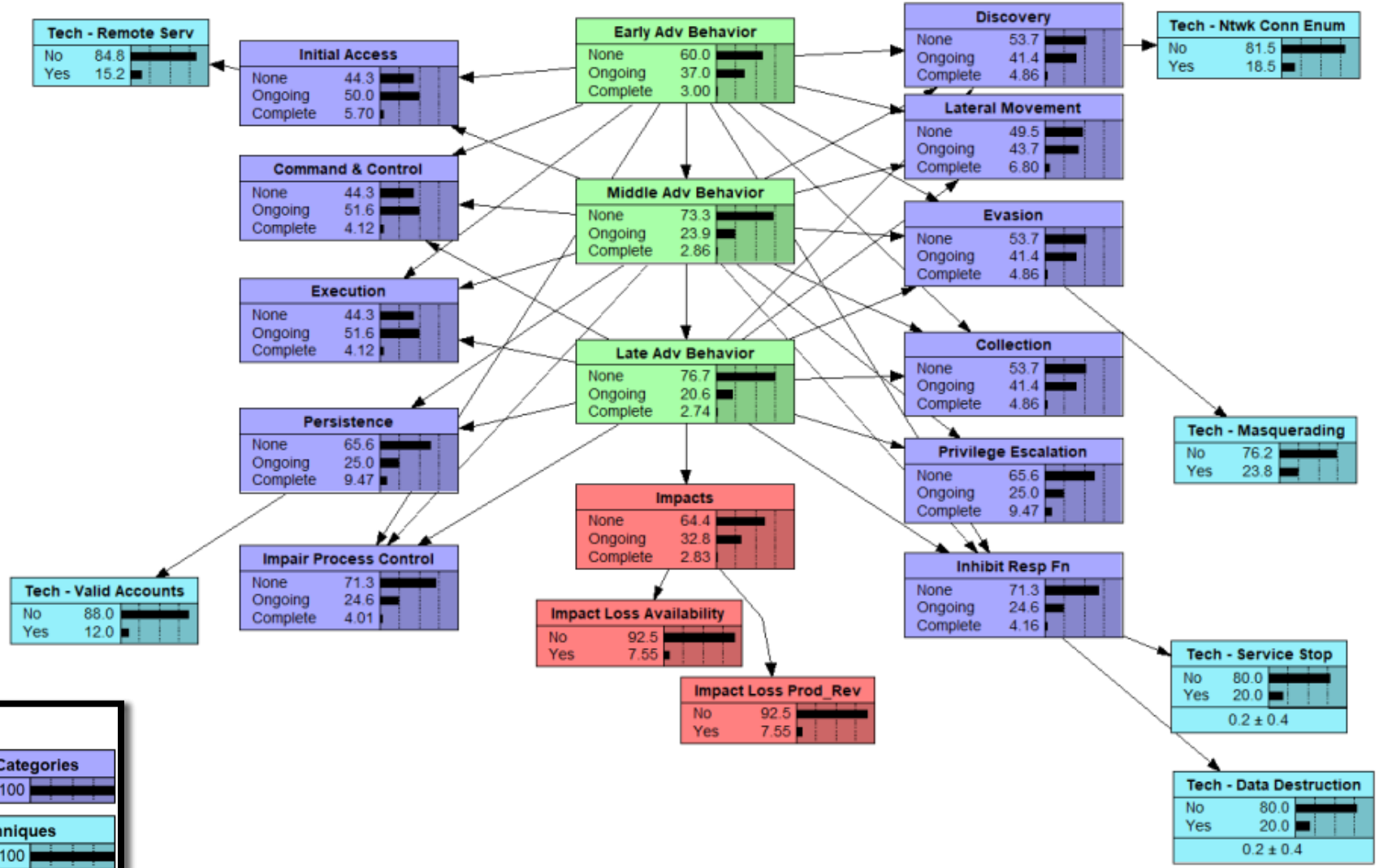
MITRE ATT&CK® for ICS

Initial Access	Execution	Persistence	Privilege Escalation	Evasion	Discovery	Lateral Movement	Collection	Command and Control	Inhibit Response Function	Impair Process Control	Impact
Data Historian Compromise	Change Operating Mode	Modify Program	Exploitation for Privilege Escalation	Change Operating Mode	Network Connection Enumeration	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	Hooking	Exploitation for Evasion	Network Sniffing	Exploitation of Remote Services	Data from Information Repositories	Connection Proxy	Alarm Suppression	Modify Parameter	Denial of Control
Transient Cyber Asset	Execution through API	Project File Infection		Indicator Removal on Host	Remote System Discovery	Lateral Tool Transfer	Detect Operating Mode	Standard Application Layer Protocol	Block Command Message	Module Firmware	Denial of View
Exploit Public-Facing Application	Graphical User Interface	System Firmware		Masquerading	Remote System Information Discovery	Program Download	I/O Image		Block Reporting Message	Spoof Reporting Message	Loss of Availability
Exploitation of Remote Services	Hooking	Valid Accounts		Rootkit	Wireless Sniffing	Remote Services	Man in the Middle		Block Serial COM	Unauthorized Command Message	Loss of Control
External Remote Services	Modify Controller Tasking			Spoof Reporting Message		Valid Accounts	Monitor Process State		Data Destruction		Loss of Productivity and Revenue
Internet Accessible Device	Native API						Point & Tag Identification		Denial of Service		Loss of Protection
Remote Services	Scripting						Program Upload		Device Restart/Shutdown		Loss of Safety
Replication Through Removable Media	User Execution						Screen Capture		Manipulate I/O Image		Loss of View
Rogue Master							Wireless Sniffing		Modify Alarm Settings		Manipulation of Control
Spearphishing Attachment									Rootkit		Manipulation of View
Supply Chain Compromise									Service Stop		Theft of Operational Information
Wireless Compromise									System Firmware		

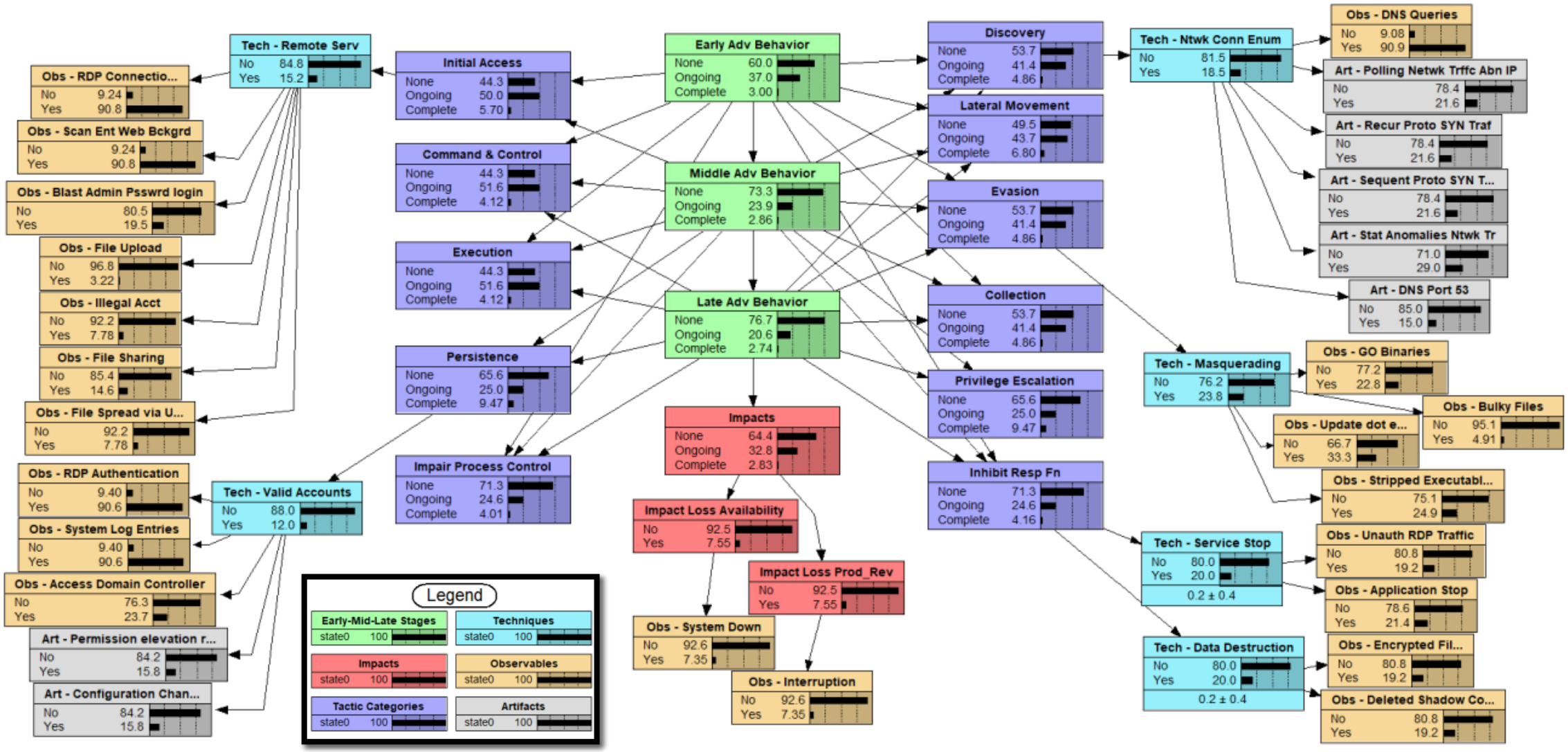
Tactics provide evidence for adversary behavior stage



Techniques provide evidence for tactics



Observables & artifacts provide evidence for techniques



How are the conditional probability tables defined?

Expert beliefs were elicited for observable probabilities

1 **How frequently is the observable seen in normal operation?**

- Weekly
- Monthly
- Quarterly
- Annually

2 **What is the probability of the observable given use of the technique?**

- Low
- Medium
- High
- Very High

Expert beliefs were elicited for observable probabilities

Highly Diagnostic Observable (Annually, Very High)

Observable 1

Technique	No	Yes
No	99.8	0.2
Yes	5	95

Weak Observable (Weekly, Low)

Observable 2

Technique	No	Yes
No	86	14
Yes	80	20

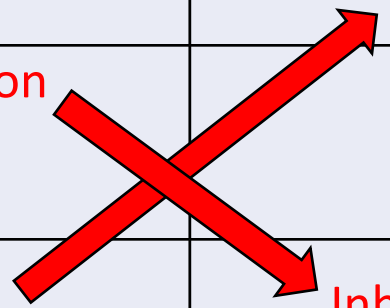
Expert beliefs were elicited for initial tactic probabilities

Tactic	Early Attack Phase (# votes)			
	Common	Occasional	Rare	Never
Initial Access	5			
Execution	3	2		
Persistence	2	1		2
Privilege Escalation	1	2		1
Evasion	4			
Discovery	4			
Lateral Movement	1	2		1
Collection	2	1		1
Command and Control	1	3		1
Inhibit Response Function			1	3
Impair Process Control		1	1	2

Tactic probabilities were refined using sensitivity analyses

What is p(Tactic=Complete | Phase=Complete)?

p(Tactic=Complete | Early Phase=Complete)	Initial Probabilities	Refined Probabilities
0.9 - 1.0	Initial Access	Initial Access
0.8 - 0.9		
0.7 - 0.8		
0.6 - 0.7		
0.5 - 0.6		Lateral Movement
0.4 - 0.5	Inhibit Response Function Command & Control Discovery	Command & Control Discovery
0.3 - 0.4	Lateral Movement	Inhibit Response Function

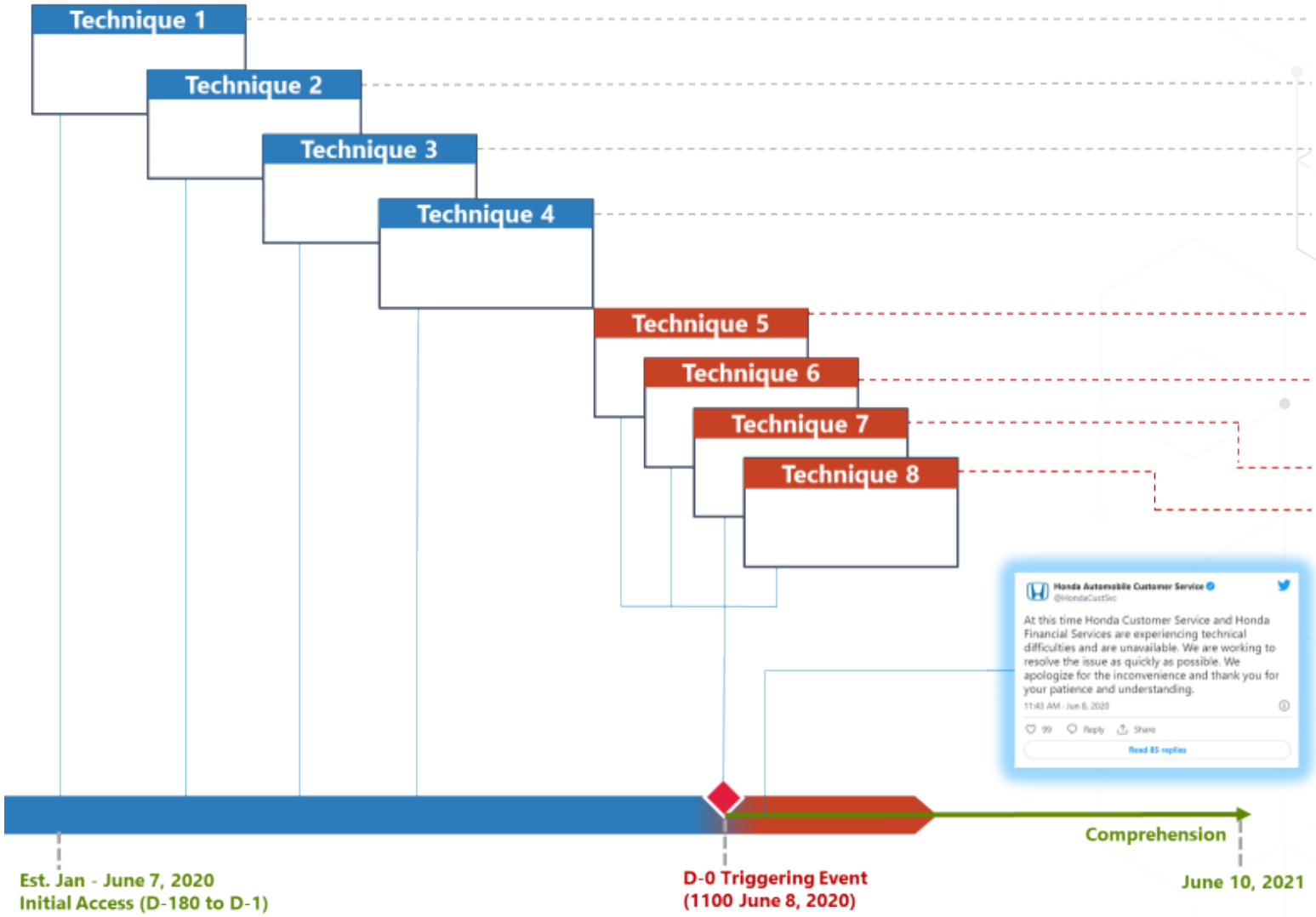


How is this applied to a CyOTE Case Study?

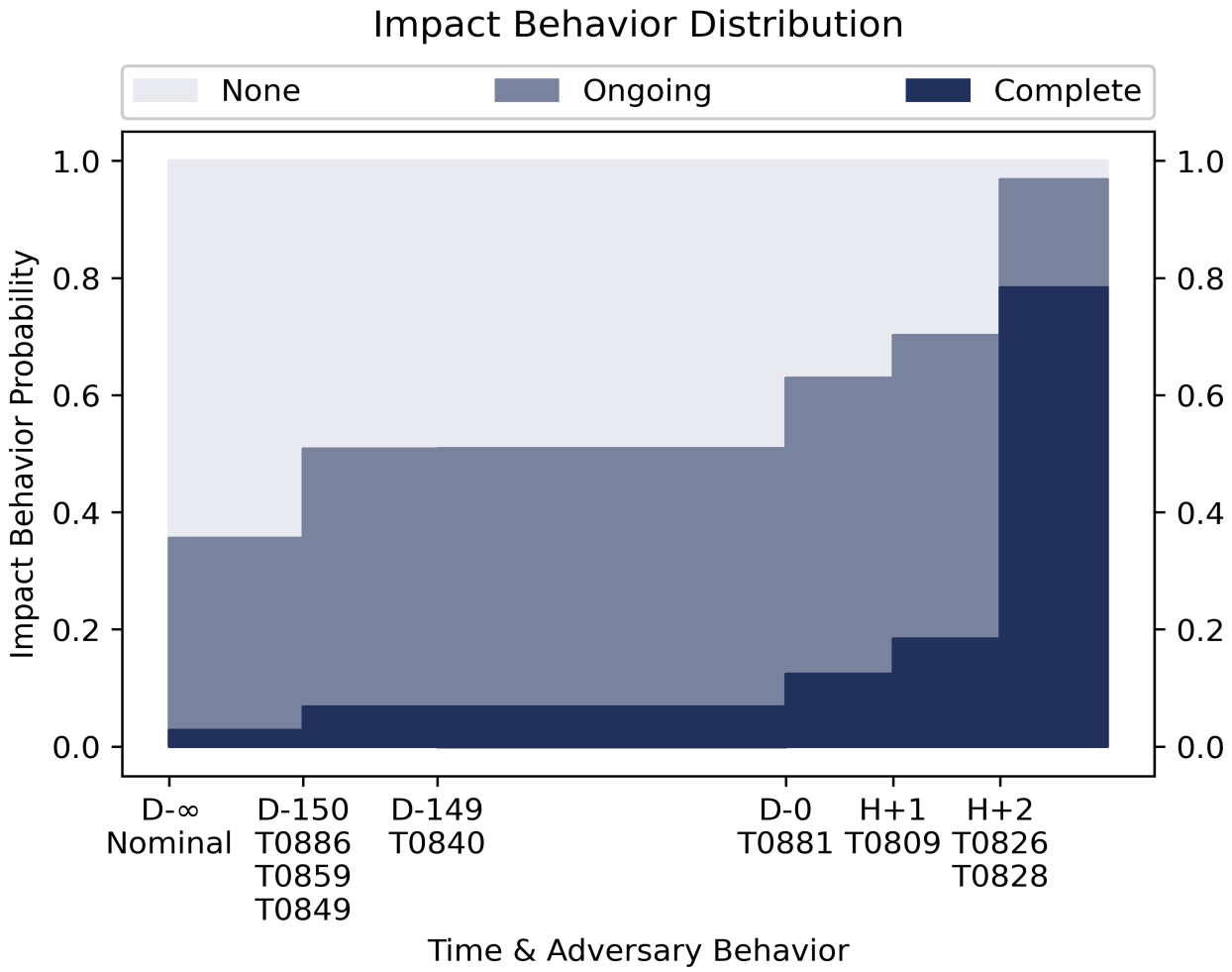
EKANS

- Three victim organizations in the manufacturing sector experienced interruptions to operations and loss of revenue due to ransomware targeting OT specific application services in the early summer of 2020.
- Impacts to Operational Technology:
  - Honda experienced a loss of production and revenue

EKANS Technique Timeline

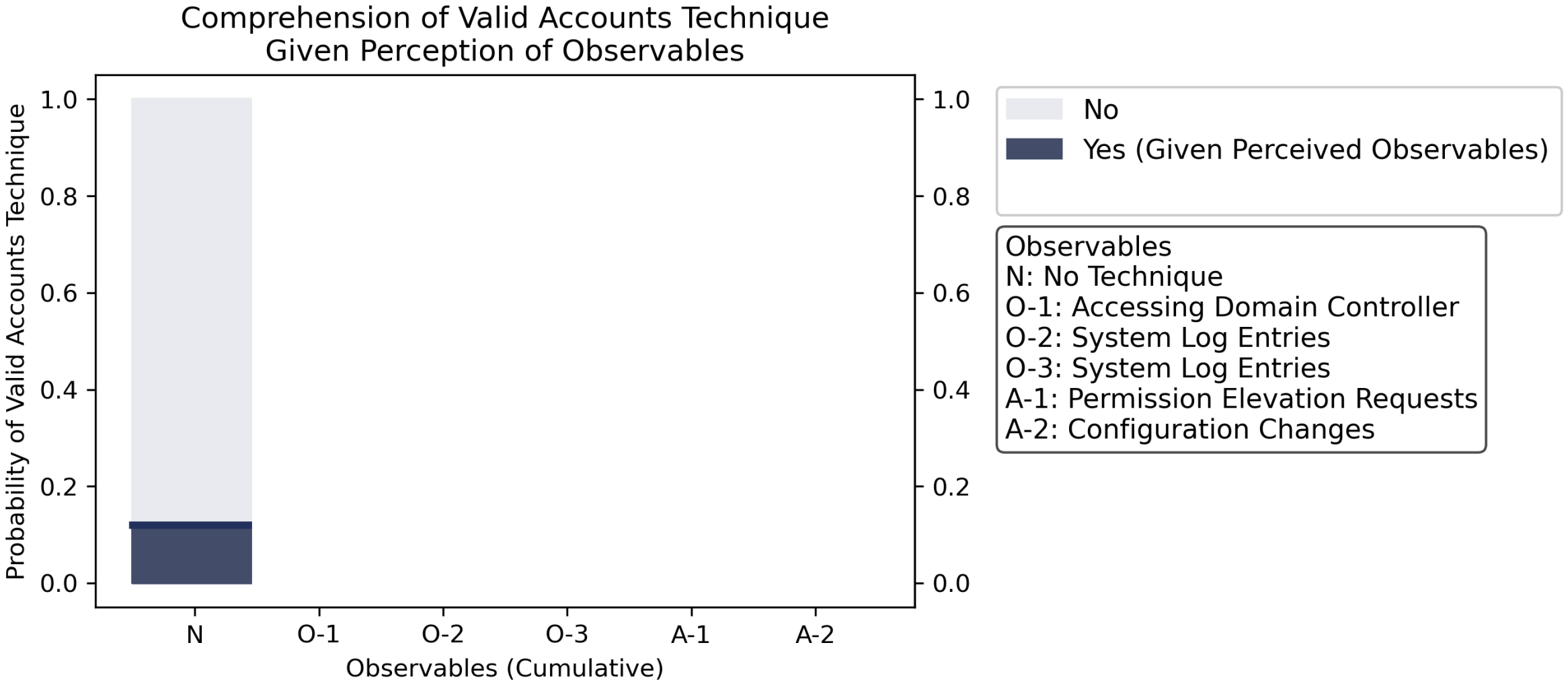


As observables are perceived and comprehended, the likelihood of adversary behavior resulting in impact increases



Adversary Behavior
Nominal: No Adversary Behavior
T0886: Remote Services
T0859: Valid Accounts
T0849: Masquerading
T0840: Network Connection Enumeration
T0881: Service Stop
T0809: Data Destruction
T0826: Loss of Availability
T0828: Loss of Productivity & Revenue

The probability of comprehending adversary behavior increases after implementing CyOTE principles



Take-Aways

- Demonstrates how observers value cyber-events and estimates likelihood of adversarial behavior
- Demonstrates value of cumulative precursor evidence
- Provides justification for investigation of related events
- Demonstrates diagnosticity of the evidence
- Enables improvement of observers' belief systems
- Enables future meta-analysis of case studies

For questions contact:

Scott Bowman, Lead CyOTE Case Studies Analyst, Scott.Bowman@inl.gov

Lee Maccarone, Lead CyOTE Case Studies Risk Analyst, lmaccar@sandia.gov

@DOE_CESER

linkedin.com/company/office-of-cybersecurity-energy-security-and-emergency-response

energy.gov/CESER

This presentation was prepared by Idaho National Laboratory (INL) under an agreement with and funded by the U.S. Department of Energy. INL is a U.S. Department of Energy National Laboratory operated by Battelle Energy Alliance, LLC.

Sandia National Laboratories is a multimission laboratory managed and operated by National Technology & Engineering Solutions of Sandia, LLC, a wholly owned subsidiary of Honeywell International Inc., for the U.S. Department of Energy's National Nuclear Security Administration under contract DE-NA0003525.

U.S. DEPARTMENT OF ENERGY | *Office of* Cybersecurity, Energy Security, and Emergency Response