INL/MIS-23-71171-Revision-0

# Cybersecurity for the Operational Technology Environment (CyOTE)

January 2023

Changing the World's Energy Future

Jared Delane Smith

Idaho National Laboratory

INL is a U.S. Department of Energy National Laboratory operated by Battelle Energy Alliance, LLC

**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/MIS-23-71171-Revision-0

# Cybersecurity for the Operational Technology Environment (CyOTE)

Jared Delane Smith

January 2023

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

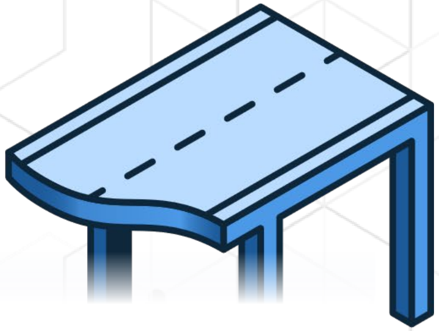
# Cybersecurity for the Operational Technology Environment (CyOTE)

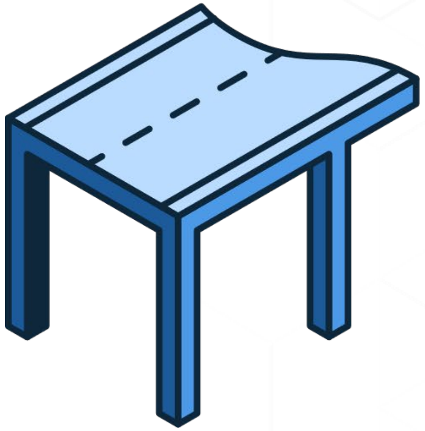
January 2023

CyOTE
Cybersecurity for the
Operational Technology
Environment

# Operational Technology (OT) Security Challenge

- OT resilience requires multidiscipline teams within an organization to see and act on early indicators of attack
- Technology alone is insufficient to defend complex and interconnected energy sector systems – human involvement needed





## Industry-Identified Gaps

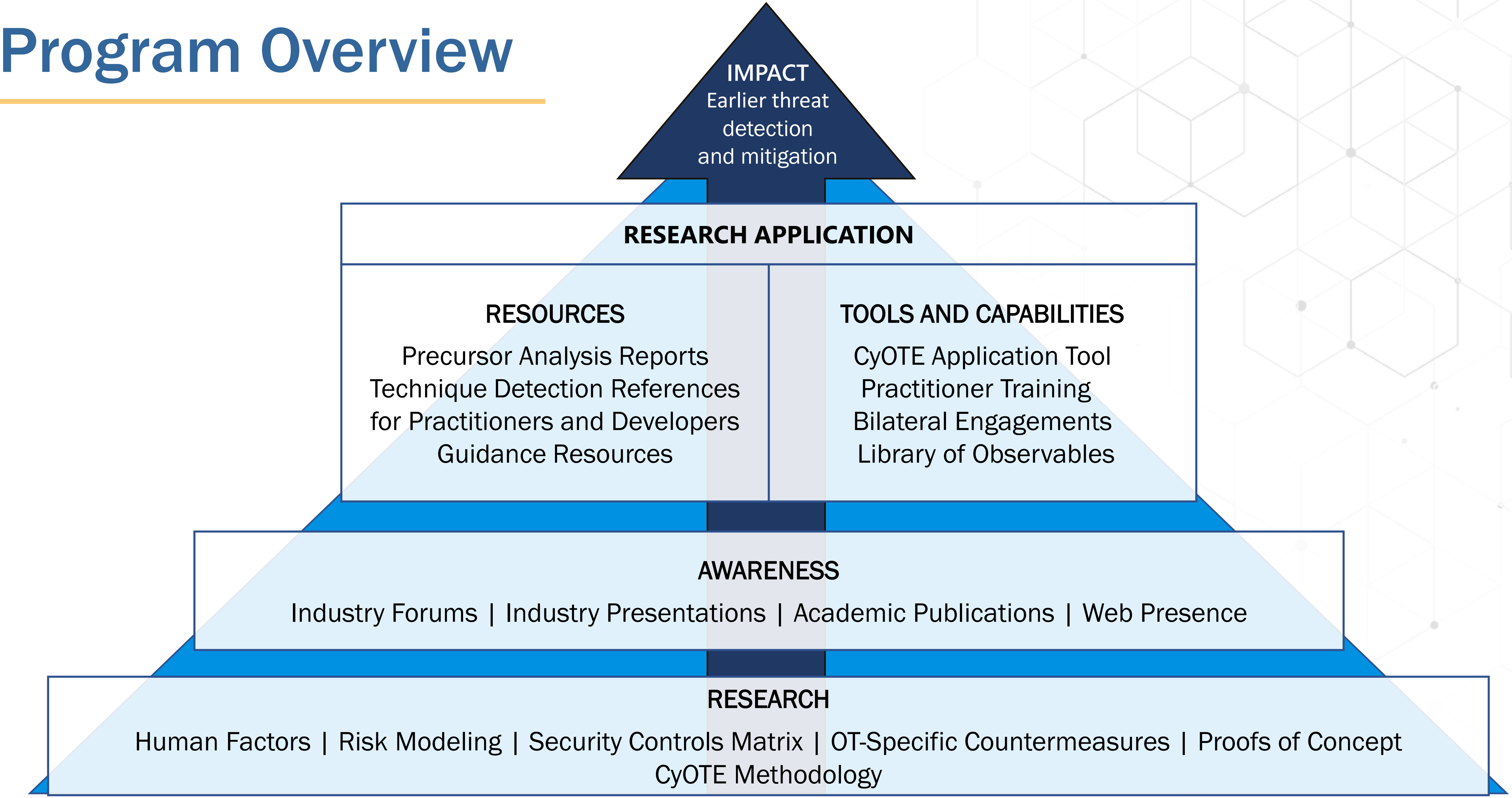
- Role-based cyber training
- Communication across disciplines
- Attention to anomalies
- Comprehension of noise from sensors and other data sources
- Incorporation of physical indicators

# CyOTE Vision

Improved **human-led,** technology-enabled analysis of the OT environment at the strategic, operational, and tactical levels.

The CyOTE approach helps energy sector owners and operators better **detect anomalies** in their operational environments, **identify cyber attacks** earlier in the attack chain, and act decisively to **prevent or limit damage.**

# Program Overview



IMPACT
Earlier threat detection and mitigation

RESEARCH APPLICATION

RESOURCES

Precursor Analysis Reports
Technique Detection References for Practitioners and Developers
Guidance Resources

TOOLS AND CAPABILITIES

CyOTE Application Tool
Practitioner Training
Bilateral Engagements
Library of Observables

AWARENESS

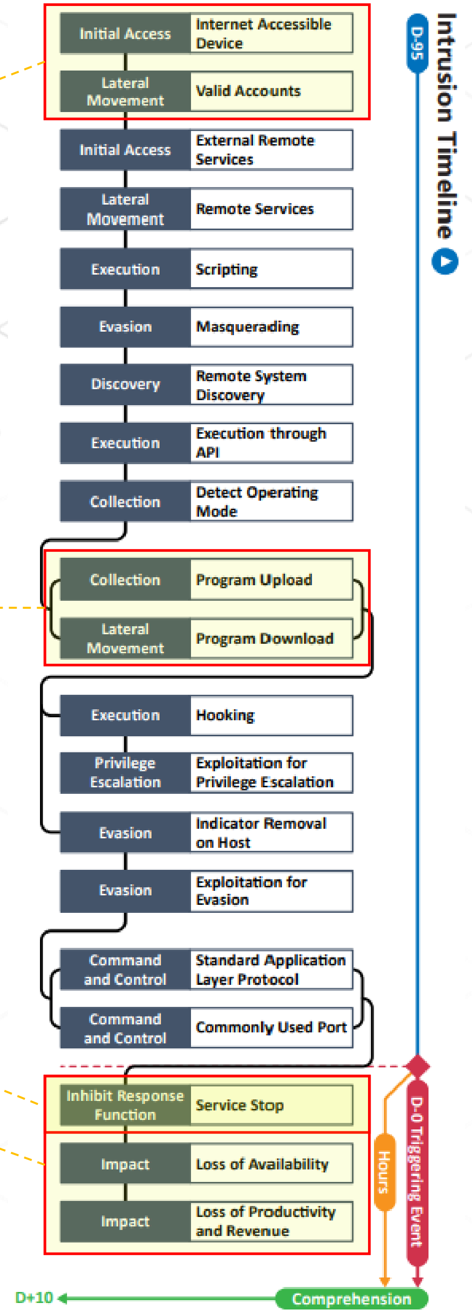
Industry Forums | Industry Presentations | Academic Publications | Web Presence

RESEARCH

Human Factors | Risk Modeling | Security Controls Matrix | OT-Specific Countermeasures | Proofs of Concept
CyOTE Methodology

# Triton Malware Impacts

Adversaries gained access to the IT network by May 2017, at least 90 days before initiating the attack. Then, with valid accounts, adversaries were able to laterally move to the OT network.



Intrusion Timeline

D-95

| | |
|---|---|
| Initial Access | Internet Accessible Device |
| Lateral Movement | Valid Accounts |
| Initial Access | External Remote Services |
| Lateral Movement | Remote Services |
| Execution | Scripting |
| Evasion | Masquerading |
| Discovery | Remote System Discovery |
| Execution | Execution through API |
| Collection | Detect Operating Mode |
| Collection | Program Upload |
| Lateral Movement | Program Download |
| Execution | Hooking |
| Privilege Escalation | Exploitation for Privilege Escalation |
| Evasion | Indicator Removal on Host |
| Evasion | Exploitation for Evasion |
| Command and Control | Standard Application Layer Protocol |
| Command and Control | Commonly Used Port |
| Inhibit Response Function | Service Stop |
| Impact | Loss of Availability |
| Impact | Loss of Productivity and Revenue |

D-0 Triggering Event

Hours

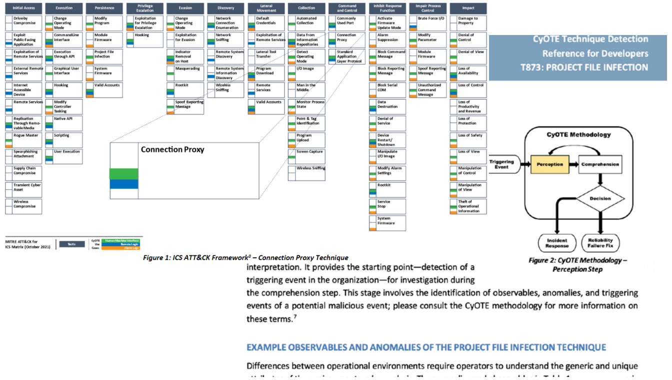
D+10

Comprehension

# Resources

## Technique Detection Reference Portfolio

- For Practitioners - starting point to learn about and identify adversarial techniques and answers “What is it?”
- For Developers - set of directions and recommendations to perceive and comprehend identified adversarial techniques and answers “How do I do it?”



CyOTE Technique Detection Reference for Developers
T873: PROJECT FILE INFECTION

*Figure 1: ICS ATT&CK Framework[8] – Connection Proxy Technique*

*Figure 2: CyOTE Methodology – Perception Step*

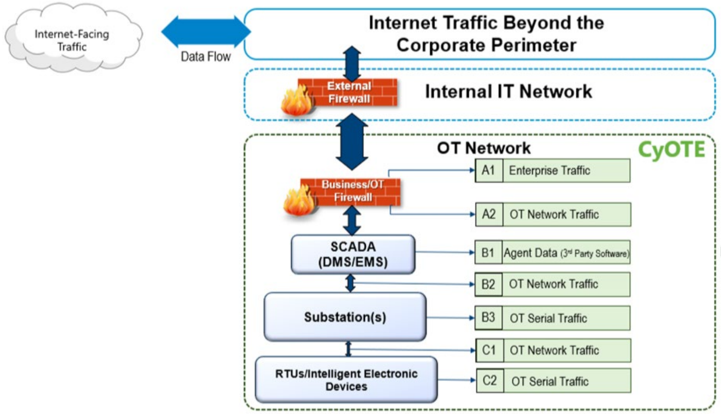
interpretation. It provides the starting point—detection of a triggering event in the organization—for investigation during the comprehension step. This stage involves the identification of observables, anomalies, and triggering events of a potential malicious event; please consult the CyOTE methodology for more information on these terms.[7]

EXAMPLE OBSERVABLES AND ANOMALIES OF THE PROJECT FILE INFECTION TECHNIQUE

Differences between operational environments require operators to understand the generic and unique

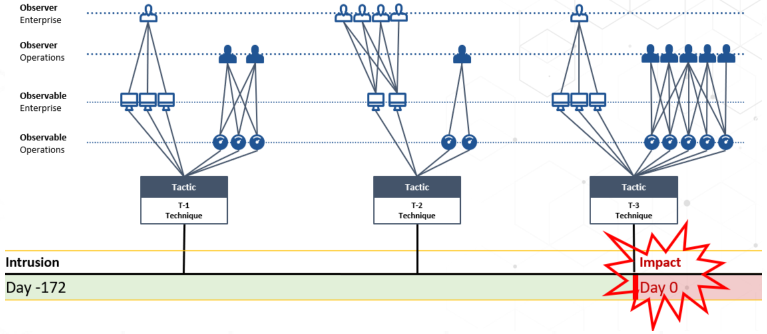
## Guidance Resources

- Written products and resulting activities that guide specific scenarios where the CyOTE approach should be implemented.
- Examples include guidance on sensor placement and specific industry application of the CyOTE approach.



## Precursor Analysis Reports

- Support continued learning through analysis of historical incidents that have impacted OT.
- Provide insights on how similar novel attacks could be detected earlier and therefore mitigated.
- Enumerate adversary techniques and the observables they generate.
- Mine and catalogue those observables.



# Tools and Capabilities

## Application Tool

- Represents the primary human machine interface to run a query of operator observed anomalies (“observables”) in their proprietary OT network.
- Designed to be computer-based and relies upon a database of approximately 4,860 separate common language descriptions of anomalies of how an operator may describe their perception of something being “wrong.”

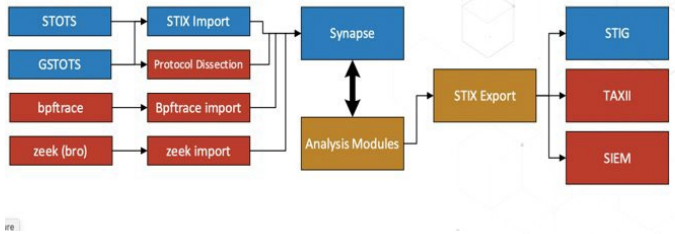
Training scenarios

Real time anomaly analysis

After-action reviews

## Proof of Concept Tools

- Detailed steps needed to implement detection capabilities.
- Requires customization for your environment, depending on existing capabilities and requirements.



## Bilateral Engagements and Training

- Bilateral Engagements: Purposeful collaboration with a single owner/operator.
- Practitioner Training: four-hour course designed for energy system owners and operators.

# Awareness

## Outreach

- Outreach at targeted venues for energy sector partners and/or cybersecurity professionals to provide awareness of the CyOTE approach, encourage its adoption, and offer access to products and tools.
- Outreach to academic organizations and publications to gain validation and circulation of CyOTE research topics.

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

CyOTE Overview

## Industry Exchange

- Monthly virtual opportunity for industry stakeholders, asset owners and operators, DOE CESER leadership, and subject matter experts to share ideas.
- Topics include CyOTE capability demonstrations, approach discussions, attack precursor exercises, and more.

## Web Presence

Smart delivery of content and capabilities through multiple paths (e.g., role, need, content search).

Office of Cybersecurity, Energy Security, and Emergency Response

CyOTE Resources Related Programs

CyOTE Cybersecurity for the Operational Technology Environment

Incorporating context for better threat detection

Fact Sheet

# Highlighted Current/Future Research

**Risk research** demonstrates likelihood of cyber events, therefore providing a measure for risk reduction.

- Directly supports energy sector implementation of the CyOTE approach.
- Applicable to Artificial Intelligence and decision analysis.

**Validation and verification** of observables, technique detection methods, and effectiveness of proof-of-concept capabilities build a foundation to identify OT-specific controls and mitigations and prompt further research and development throughout the community.

**Human factors research** leverages decades of industrial safety efforts, applying proven tactics and techniques to prevent, find, and fix critical organizational weaknesses—both new and latent—that impact OT cybersecurity outcomes.

Sandia National Laboratories

Lawrence Livermore National Laboratory

THE UNIVERSITY of TULSA

Tufts UNIVERSITY

MITRE

# For more information or to get started:

Visit cyote.inl.gov

Jessica Perry, CyOTE Program Manager
DOE CESER
CyOTE.Program@hq.doe.gov

# Thank You

@DOE_CESER

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

energy.gov/CESER

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

# Colonial Pipeline Ransomware Impacts

With access to the network, the ransomware gathered

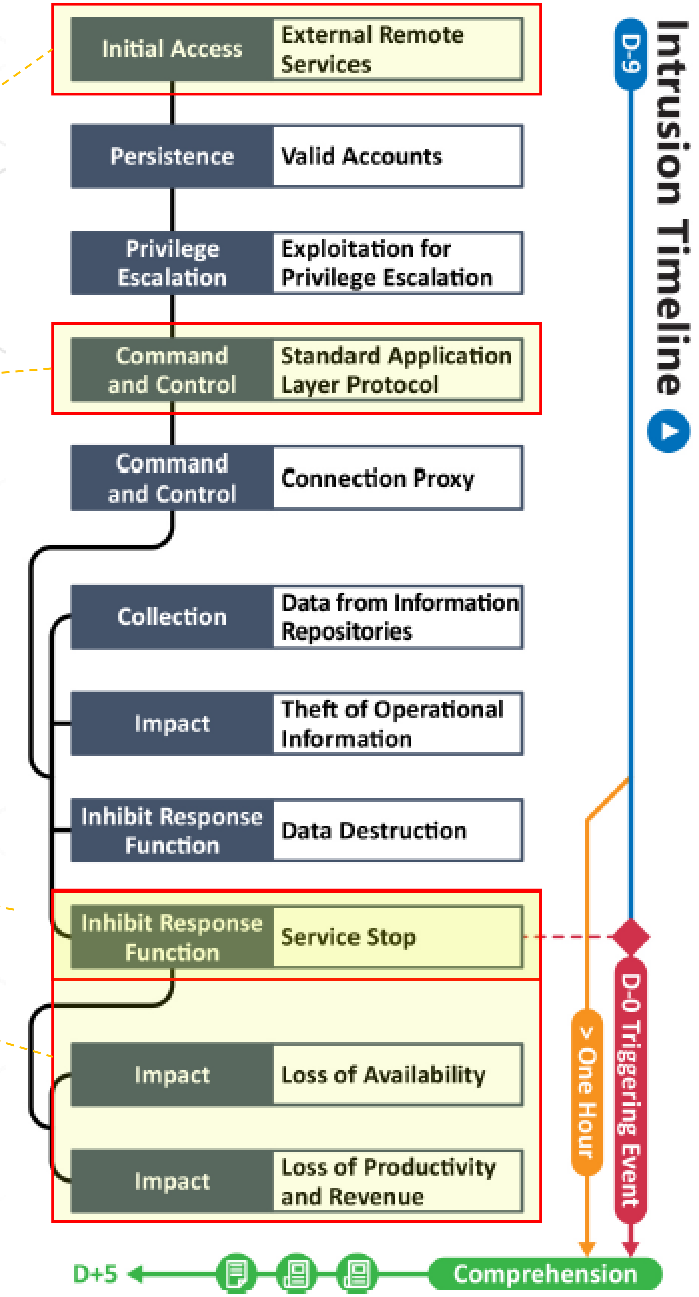
e

Adversaries gained access through a VPN connection on 29 April 2021, nine days before the ransomware attack was executed.

om

vn.

nave observea communications witn externai IP addresses.



Initial Access — External Remote Services

Persistence — Valid Accounts

Privilege Escalation — Exploitation for Privilege Escalation

Command and Control — Standard Application Layer Protocol

Command and Control — Connection Proxy

Collection — Data from Information Repositories

Impact — Theft of Operational Information

Inhibit Response Function — Data Destruction

Inhibit Response Function — Service Stop

Impact — Loss of Availability

Impact — Loss of Productivity and Revenue