METHODOLOGY FOR CYBERSECURITY IN OPERATIONAL TECHNOLOGY ENVIRONMENTS

REVISION 1

SEPTEMBER 23, 2021

CyOTE Cybersecurity for the Operational Technology Environment

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

This document was prepared by Idaho National Laboratory (INL) under an agreement with and funded by the U.S. Department of Energy.

Idaho National Laboratory

SUMMARY OF REVISIONS

This table contains changes that have been incorporated into the Cybersecurity for the Operational Technology Environment (CyOTE™) Methodology Revision 1. Updates can include corrections, clarifications, and other minor changes in the publication. Any potential updates for this document that are not yet published—including additional issues and potential corrections—will be posted here as they are identified.

Revision Number	Comments	DATE
Revision 0	Initial release	06-30-2021
Revision 1	Updated cover page, added funding language, and implemented editorial updates	09-23-2021

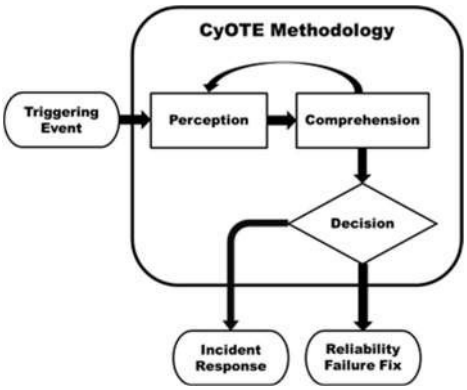
Click for More Information	CyOTE Program || Fact Sheet || CyOTE.Program@hq.doe.gov
DOE Senior Technical Advisor	Edward Rhyne || Edward.Rhyne@hq.doe.gov || 202-586-3557

Table of Contents

EXECUTIVE SUMMARY

The U.S. Department of Energy's (DOE) Office of Cybersecurity, Energy Security, and Emergency Response (CESER), through the Cybersecurity for the Operational Technology Environment (CyOTE) Program, worked with energy sector asset owners and operators (AOOs), partners, and Idaho National Laboratory (INL) to develop capabilities for AOOs to independently identify adversarial tactics, techniques, and procedures (TTPs) within their operational technology (OT) environments. Unlike the approach taken with commercial security solutions, CyOTE seeks to tie anomalies in operations to a cyber-attack. By stringing together multiple techniques in the OT environment, AOOs can identify attack campaigns with ever decreasing impacts.

CyOTE's methodology applies fundamental concepts of perception and comprehension to a universe of knowns and unknowns increasingly disaggregated into observables, anomalies, and triggering events. MITRE's ATT&CK® Framework for Industrial Control Systems (ICS) is used as a common lexicon to identify a set of triggering events related to three Use Cases – alarm logs, human-machine interface (HMI), and remote logins – which together account for 87 percent of the techniques commonly used by adversaries. CyOTE's methodology is also appropriate for OT-related anomalies perceived outside the three Use Cases, such as through the energy system itself.



CyOTE provides a general approach for an AOO to use, starting from the point in time and space an anomalous event or condition meriting investigation – a triggering event – is perceived, and continues to the point where the anomaly is comprehended with sufficient confidence to make a business risk decision on the appropriate resolution. If sufficient evidence of a malicious nexus is found, the situation is addressed through existing organizational incident response procedures. Failure to find sufficient evidence of malicious activity defaults to the situation addressed through existing organizational corrective maintenance and work management procedures.

By leveraging CyOTE's methodology with existing commercial monitoring capabilities and manual data collection, energy sector partners can understand relationships between multiple observables which could represent a faint signal of an attack requiring investigation. CyOTE can assist AOOs in prioritizing their OT environment visibility investments. Over time, AOOs' triggering events will move towards fainter signals, detected earlier, to interdict incidents before more significant harms are realized in the face of infrastructure changes, new technologies, and determined and sophisticated adversaries.

BACKGROUND

Cybersecurity is not easy nor inexpensive to attain and maintain. This is perhaps even more true for operational technology (OT) systems. Too often, security professionals are lulled into thinking the right process or checklist is the key to security, whereas others in the organization may believe acquiring and installing a particular technology will provide security. Although both processes and infrastructure are necessary, individually they are not sufficient, and overemphasis on either can inadvertently drive an organization to pursue compliance with a process or standard as opposed to security. Just because an individual or an organization believes an asset or capability is protected does not mean it cannot be compromised by an adversary with sufficient motivation and resources. Compliance can breed complacency, and complacency is the antithesis of security. A questioning attitude and intellectual curiosity are powerful antidotes to complacency.

Adversaries commonly vary their activities to produce different static indicators of compromise (IOCs). This variance is a straightforward, quick, and low-cost way for an adversary to avoid basic automated detection capabilities. Changing these fixed indicators, which already exist in a time-bounded context, results in asset owners and operators (AOOs) expending resources in enduring low-payoff "whack-a-mole"[a] activities. The broader context in which those static IOCs appear as signatures is harder for an adversary to change, however. This is the essence of David Bianco's Pyramid of Pain[1] shown in Figure 1, which relates the volume of different types of indicators to the adversary's difficulty in changing them to avoid detection.

Figure 1. The Pyramid of Pain

Adversary behaviors are at the tip of the pyramid. These indicators of attack are mostly unconcealable and need to be investigated. The challenge is to identify a behavioral indicator of attack that exists not at a fixed logical and temporal location such as an IOC, but rather as a chain of related events across time and space. Each individual link in the chain can be obfuscated or hidden to some degree (sometimes substantially obscured, though all events display a signature

[a] In this context, "whack-a-mole" refers to the practice of surveying defended environments for static IOCs used in previous attacks or shared from an external source with limited context. The term relates to the arcade game, where another mole pops up as soon as one is hit down, where "winning" is a matter of how fast you can respond to the new stimuli. See https://www.securityweek.com/root-cause-analysis-stop-playing-whack-mole for an IT-centric description of why this is a poor strategy.

somewhere), but are much clearer when recognized as a chain instead of a collection of individual links. Behavioral indicators of attack are difficult if not impossible for an adversary to completely hide as faint signals and will always be detectable within the noise of regular operations. Recognizing a behavioral indicator of attack is much more challenging in real life than in hindsight. The faint signals typically appear as anomalies in operations, OT, information technology (IT), and business processes; just as a behavioral indicator of attack can span many of these areas, so must an AOO's internal and independent investigation. Questioning attitudes and intellectual curiosity are critical to this investigative process, just as they are to combatting complacency.

> *"When trouble is sensed well in advance it can easily be remedied; if you wait for it to show itself any medicine will be too late because the disease will have become incurable. As the doctors say of a wasting disease, to start with it is easy to cure but difficult to diagnose; after a time, unless it has been diagnosed and treated at the outset, it becomes easy to diagnose but difficult to cure."*
>
> *Niccolo Machiavelli,* The Prince[2]

Since 2016, the Cybersecurity for the Operational Technology Environment (CyOTE) Program under the auspices of the U.S. Department of Energy's (DOE) Office of Cybersecurity, Energy Security, and Emergency Response (CESER), in collaboration with Idaho National Laboratory (INL), partners with industry to develop targeted strategies to increase the cybersecurity and resiliency of America's energy sector. CyOTE was conceived to facilitate OT data sharing and analysis with cleared government resources, philosophically similar to but separate from the IT-centric Cybersecurity Risk Information Sharing Program (CRISP). At the start, CyOTE established collaborative partnerships with a small number of AOOs through a Pilot activity to determine the most useful information to collect from AOO OT environments, and how to share it with other CyOTE Program participants. The goals of the Pilot were to improve AOO cyber defenders' and operators' ability to detect, investigate, and mitigate malicious activity within the OT environment to reduce risk and increase efficiency. The Pilot consisted of two phases which informed the transition to an enduring Program in 2019. Figure 2 depicts the CyOTE Program's evolution.

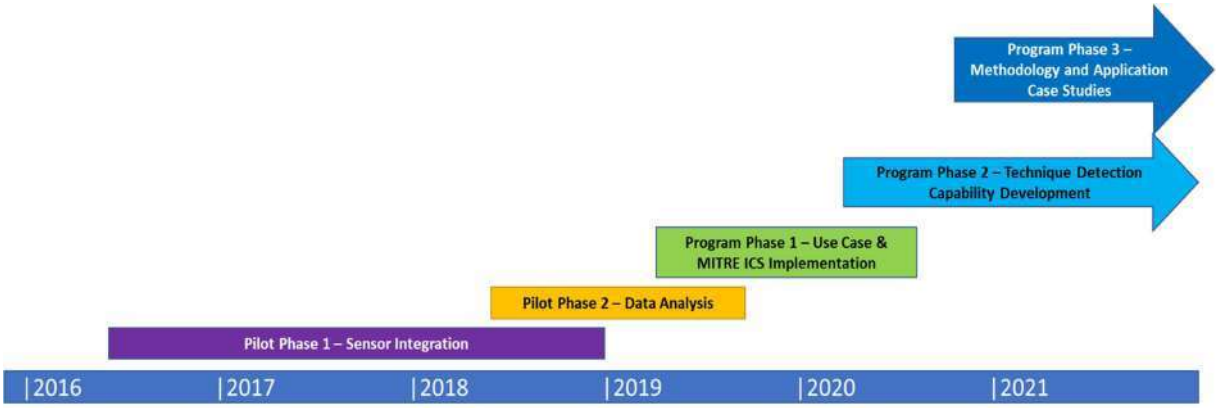


Figure 2. CyOTE Pilot and Program Phases

PILOT PHASE I - SENSOR INTEGRATION

First, the CyOTE team worked with a small representative group of electric industry AOOs through Pilot engagements to identify what data streams to monitor, where to place sensors, and how to bidirectionally share data before and after enrichment while protecting confidentiality and data sources. This effort resulted in Program alignment to the Industrial Control Systems (ICS) Cyber Kill Chain[3] and a feasibility evaluation for creating a repeatable, industry-wide approach for OT threat data analysis. To address how the identified data could be securely collected and transmitted to a central location for analysis and enrichment, the CyOTE team explored research topics such as firmware integrity, OT sensor capabilities, and data anonymization. Several of the lessons learned[b] from Phase I are relevant to CyOTE's methodology, including:

- Data observations of interest, which drive OT alerting and alarming capabilities, should be prioritized based on the potential impacts to the operational process.
- Sensor deployment should align with the organization's overall defensive priorities and be prioritized with an understanding of the overall system's visibility.
- Sensor capabilities should align with the characteristics of OT environments being monitored.
- Accounts, assets, and network activity should be audited at regular intervals to supplement sensor data.

Phase I of the Pilot culminated when further progress began to be impeded by data custodial issues, some related to interpretation of North American Electric Reliability Corporation (NERC) Critical Infrastructure Protection (CIP) requirements. This challenge eventually drove the realization CyOTE would be most successful in eventual production when its capabilities could be employed independently by the AOO, free from external dependencies along the critical path, such as data transfer.

[b] For a more comprehensive discussion of insights from the Pilot and the Program to date, see the forthcoming "Observations and Lessons Learned from the CyOTE Program" white paper; contact CyOTE.Program@hq.doe.gov for further information.

PILOT PHASE II – DATA ANALYSIS

The second phase of the Pilot involved administrative and logistical activities to successfully transfer a sizeable volume of AOO data to the CyOTE team for analysis. The analysis of these data sets yielded further lessons learned, including:

- Worthwhile data analysis requires context, not just content.
- Data collected should be filtered according to the analytical questions to be answered. Relevant data is more useful than simply more data, as the law of diminishing marginal returns applies beyond some point.
- Analysis should incorporate understanding of adversary techniques and behaviors, and not rely solely on expertise in the OT domain.
- Data analysis can and should be used to identify gaps in data availability to prioritize further OT monitoring investments.

Phase II of the Pilot culminated when second-party analysis of the transferred data, absent of the deep and broad firsthand context only the originator and owner of such data can truly possess, had proceeded as far as possible. The CyOTE team identified multiple anomalies through analysis of this real-world data, demonstrating the value in the effort. The perception of these anomalies came several months after the data was collected, however, and meaningful comprehension of the anomalies required significant collaboration with the AOO providing the data.

Partially overlapping with the conclusion of this second phase of the Pilot, CyOTE transitioned from a Pilot to a Program in early 2019. As expected, the challenges and barriers identified in the Pilot phases informed the inception of the CyOTE Program as stakeholders recognized the value and efficiency of starting with a recently perceived abnormality instead of analyzing data to find abnormalities after the fact and with less than adequate context. Most importantly, this transition coincided with a fundamental shift in thinking. Rather than collecting bulk raw data from multiple AOOs with centralized analysis, the CyOTE Program realized AOOs must lead this effort with event-driven sharing. AOOs maintain firsthand access to whatever data exists and have the best and most context to accurately interpret that data. Ultimately the AOO owns the most risk and has the most straightforward management options.

PROGRAM PHASE I – USE CASE AND MITRE ICS ATT&CK FRAMEWORK IMPLEMENTATION

Upon its transition to a Program, CyOTE represented the OT portion of CESER's overarching situational awareness Program and capabilities. Collaboration with industry participants identified the need to take a use-case approach to identifying types of events with the potential to trigger event-driven metadata sharing through an established and protected channel, and the corresponding metadata elements and sources necessary for effective analysis to be shared.

Like most other industries, the energy sector contains a broad variety of organizational and individual perspectives, beliefs, and words to describe the same universe of items and ideas.[c] Due to the importance of interdisciplinary communication within AOOs, and the need to normalize and thus trend information from multiple AOOs with the eventual goal of sharing actionable insights across the sector, a common language was necessary. The CyOTE team decided the use of MITRE's ATT&CK® Framework for ICS,[4] would provide the shared lexicon necessary for consistent description and understanding of detection and evaluation concepts.

CESER formed three Working Groups to explore OT data Use Cases with volunteers from several participating energy companies. These Working Groups examined the 120+ adversary techniques in the ATT&CK Framework for ICS and mapped them to generic OT data sources not specific to any participant's OT architecture. The three Use Cases—alarm logs, HMI, and remote logins—were identified by CESER and validated through INL analysis as situations where OT log data may have a high likelihood of containing attack indicators. Together, these three Use Cases provide coverage for more than 86 percent of all techniques described in the ATT&CK Framework for ICS as shown in Figure 3.[d] With only *a priori* assumptions on adversary behaviors and intentions, detection of a technique relevant to multiple Use Cases (as shown by the colored bars at the bottom of the technique boxes in Figure 3) is a stronger indicator of potential malicious activity.

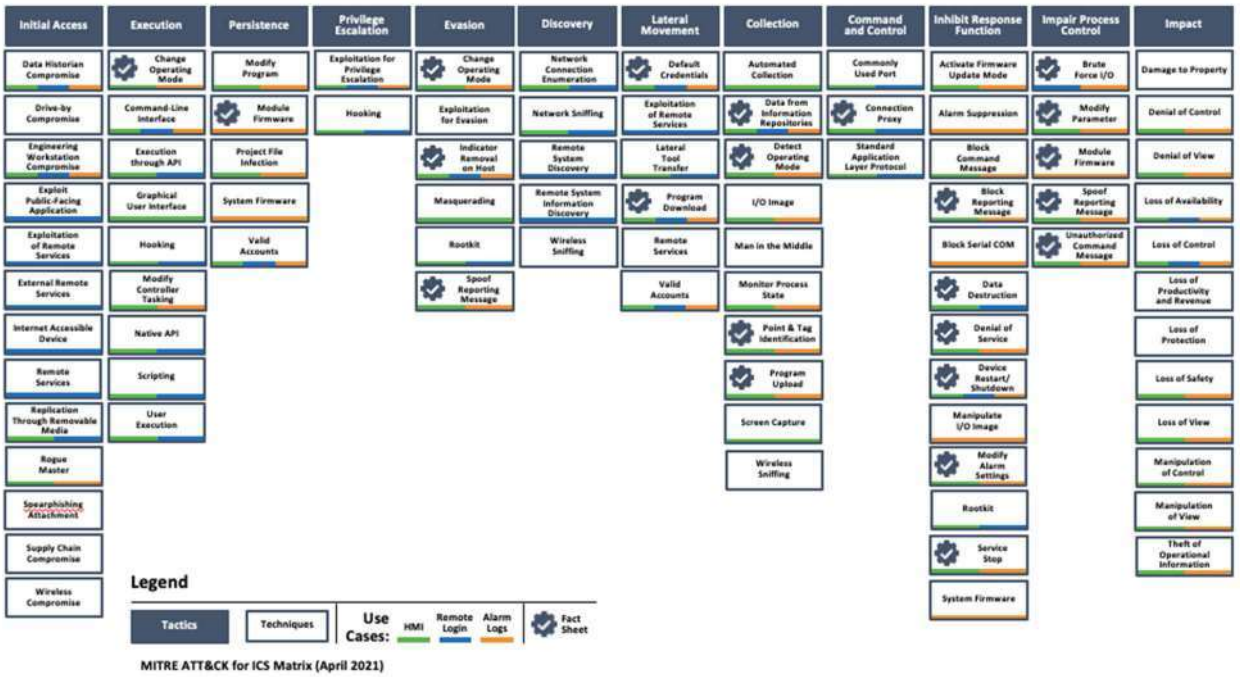


Figure 3. CyOTE Tactics and Techniques Chart

[c] See https://www.ncbi.nlm.nih.gov/pmc/articles/PMC3575067/ for a deeper treatment of the importance of shared language to achieve effective communication.

[d] The Use Case analysis work was conducted based on the original (January 2020) release of the ATT&CK Framework for ICS, and covered 82 percent (80 of 96) of the techniques in that version. The 86 percent figure is calculated from the current (April 2021) release of the Framework, where 77 of 89 techniques are covered.

With the techniques mapped to Use Cases, the Working Groups moved forward to build out how an AOO could identify evidence of technique use in a production OT environment. This activity centered on triggering events, data sources, and data availability, with the initial goal of enabling programmatic event-driven sharing. For each Use Case, AOOs identified possible triggering events based on their experience which would initiate data collection, analysis, and sharing. These triggering events were then mapped to the adversary techniques for which there could be a signature. Next, the team enumerated a comprehensive set of data fields and elements to support comprehensive analysis, and from what sources those data fields may be available. This "wish list" of data sources and elements was subdivided into three high-level buckets: data collected today; existing data which could be collected today but is not at present; and data that does not exist or cannot be collected without new capabilities. This process is depicted in Figure 4.

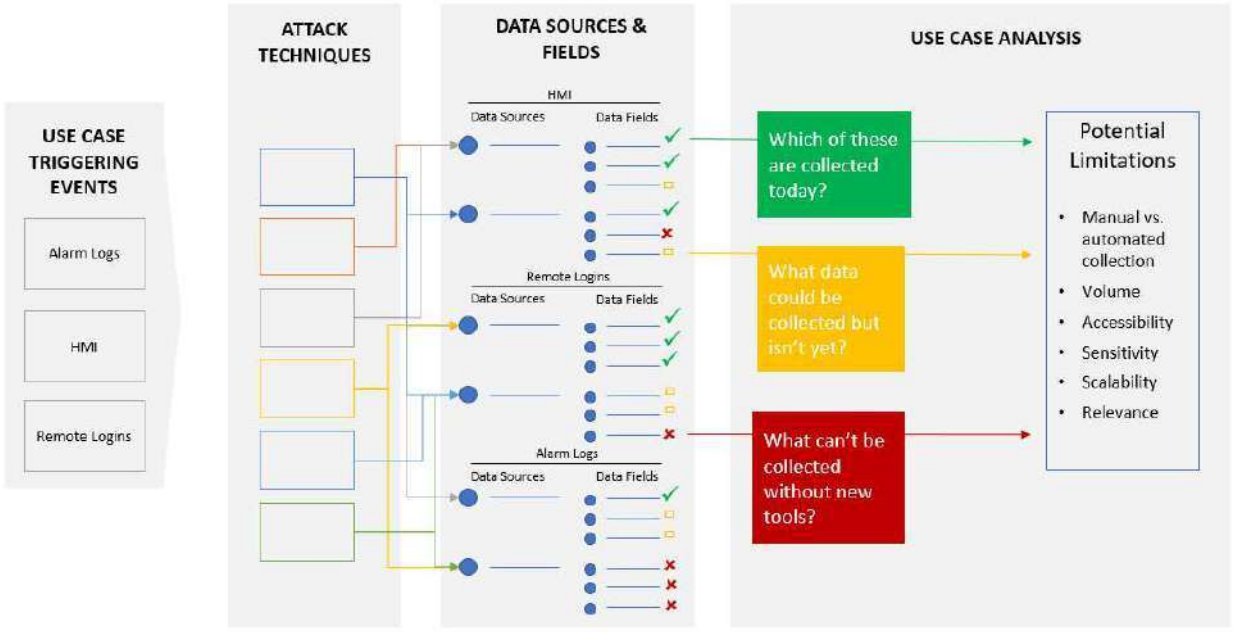


Figure 4. Mapping Adversary Techniques to Data Availability

Coming out of the Working Groups, the AOOs and CyOTE team recognized their findings and insights were applicable to enabling event-driven intelligence sharing as much, if not more, than the initial goal of metadata sharing. Moving from sharing raw information captured following a triggering event, to sharing intelligence[e] based on analysis of that data with the benefit of firsthand context, avoids some of the practical pitfalls common to data-sharing aspirations and may even encourage increased sharing because the data owner retains more control over sharing decisions.

[e] The difference between information and intelligence (in an IT cyber threat intelligence context) is described in this 2015 *Dark Reading* article: https://www.darkreading.com/analytics/threat-intelligence/cyber-threats-information-vs-intelligence/a/d-id/1316851

Through this effort, the AOOs and CyOTE team increased the collective understanding of challenges and opportunities, and validated or refuted commonly held, but not rigorously studied, beliefs. Key takeaways from the Use Case identification and ATT&CK Framework for ICS implementation included:

- Current OT data collection primarily supports operations. Data collected and transmitted to control centers is mostly in support of monitoring and control of the operational processes. Much of the data beneficial for cyber-attack technique detection is not currently collected. Some devices could be reconfigured to capture additional useful data, for automated transmission or manual retrieval.
- Data at the field device or substation level may be more valuable but requires significant effort—and potentially new capabilities—to monitor.
- Today's OT environments mostly lack automated capture capabilities. Event-driven data sharing will likely require manual action by AOOs to retrieve and share data.
- Network-level data gathered from firewalls and switches is far more readily available and easier to collect than system-level or device-level data today.
- Programmatic sharing of data with external parties requires legal agreements and certain regulatory and liability protections. These mechanisms take a significant amount of time to develop and execute.
- AOOs generally desire access to near real-time OT threat information and detection tools to enhance risk mitigation and complement, not replace, existing cybersecurity solutions.
- Large volumes of data are necessary for establishing initial baselines, but programmatic value from large-scale collection is currently confounded by challenges with encryption, transfer, analysis, and privacy.
- Data without context is not helpful in identifying anomalous activity within OT environments.
- Data correlation is necessary to provide context to information and identify anomalous "trigger" events.
- MITRE's ATT&CK Framework for ICS is more useful than the ICS Kill Chain in this situation because of its greater breadth and specificity.
- Interdepartmental and interdisciplinary cooperation within an AOO organization is essential to adequately identify, collect, and understand all the available data and contextual information.
- The value of event-driven information sharing increases when the time and place of the analysis and decision to share shifts earlier and towards AOOs. This has the added benefit of retaining complete control of what to share with the organization who owns the data and has the best context to interpret it.

This activity culminated with the publication of the *Use Case Working Group Results* report[f] in June 2020, documenting the complete findings of the three Use Case Working Groups.

[f] This report is designated Official Use Only and TLP:AMBER; contact CyOTE.Program@hq.doe.gov for more information.

PROGRAM PHASE II – TECHNIQUE DETECTION CAPABILITY DEVELOPMENT

Based on the results of the three Use Case Working Groups' identification of potential triggering events and data sources, CyOTE developed an inventory of Fact Sheets to provide information to AOOs to increase understanding of adversary techniques (Figure 3). These Fact Sheets provide foundational knowledge to enable technique detection capabilities whether manual or automated. The capabilities described in the Fact Sheets can speed the detection of suspicious and potentially malicious activity when implemented in an AOO's OT environment.

The Fact Sheets of technique descriptions are identified in the *CyOTE Technique Detection Capabilities* report.[g] The CyOTE team is working directly with a subset of AOO partners using AOO-supplied data and insights from the Use Case Working Groups to better understand the requirements and efforts needed to deploy a detection capability created from a Fact Sheet to the level where it is implemented in an AOO production OT environment.

Throughout the CyOTE Pilot and Program Phases, participating AOOs and the CyOTE team gained valuable insight from recurring themes across phases. Perhaps the most important realization was to look beyond technologies and networks and recognize *everything* is a sensor.[h] Given the faint signals and operational anomalies available to initially detect malicious cyber activity in an OT environment, an AOO must seek out and take full advantage of every potential source of useful information available to them. The Fact Sheets, with their technology-agnostic and holistic approach, provide a vehicle to begin this journey.

PROGRAM PHASE III – METHODOLOGY AND APPLICATION CASE STUDIES

The CyOTE Program is currently in Phase III, Methodology and Application Case Studies. The goal is to capitalize on the investments in the CyOTE Pilot and Program to build the body of knowledge around OT attacks and defenses to position AOOs for independent success regardless of size, experience, or business model.

A main activity for this phase is to validate the assumption for attacks on OT environments. Although the first point of entry and the final effects realized may vary significantly across incidents, the intermediate adversary techniques and procedures used in the middle of the kill chains are frequently reused. This adversary reuse increases the chances to detect and interdict an attack before the most significant impacts can be realized because the signatures are understood even though they may not have been detected – an AOO knows what to look for in their OT environments.

Already underway is an initial compilation of Case Studies of historical OT attacks and OT-related incidents analyzed using CyOTE. Although differences exist in a historical application based on

[g] At the time of publication of this report, the "CyOTE Technique Detection Capabilities and Fact Sheets" report is not public; contact CyOTE.Program@hq.doe.gov for more information.

[h] The CyOTE team recognizes this perspective is nearly identical in principle to the "every Soldier a sensor" approach used by the U.S. Army in the early 2000s, as described by AUSA: https://www.ausa.org/sites/default/files/TBIP-2004-ES2-Every-Soldier-is-a-Sensor.pdf

external information versus a real-time employment by an AOO, what these Case Studies lack from firsthand context they compensate for with the clarity of hindsight. Over time, the intent is to add voluntarily shared insights and Case Studies from AOOs employing CyOTE's methodology to provide a well-rounded body of knowledge with both broad insights and specific tactics. The CyOTE team expects this effort will provide actionable perception and comprehension recommendations as well as incremental improvements to CyOTE's methodology itself.

CyOTE KEY CONCEPTS

As CyOTE's methodology is focused on identifying certain occurrences of interest and developing an understanding of them in their broad context, it is essential to have a common understanding of the key concepts and terms used throughout. The concepts and terms in this shared mental model are universally applicable to all AOOs regardless of their size, business model, or resources. As concepts, they are also applicable to other sectors and industries with little to no tailoring.

OBSERVABLES, ANOMALIES, AND TRIGGERING EVENTS

First, to establish a common way to describe things happening, Figure 5 below shows the nested relationship between observables, anomalies, and triggering events.

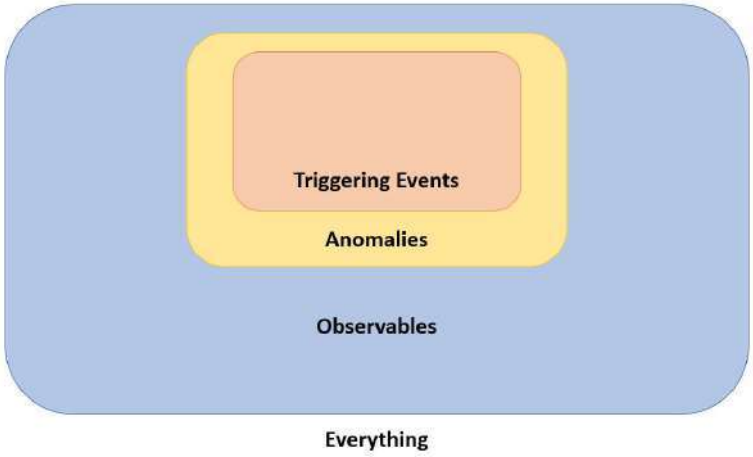


Figure 5. Hierarchy of Observables, Anomalies, and Triggering Events

An observable is the signature of an occurrence – something happened or is happening – that is able to be perceived. Depending on the facts and circumstances, an observable may be immediately comprehended with high confidence, or not yet comprehended. Most events will have a set of associated observables in more than one domain, area, or dimension; this drives the importance of identifying and leveraging data and perspectives from operations, OT, IT, and business processes.

Anomalies are the subset of observables which deviate from what would be expected and understood as normal in the same or similar circumstances. This implies some comparison to a baseline of what constitutes normalcy, and in the frequent absence of data-driven baselines for

OT environments, the baseline defaults to individual experience and organizational memory. Anomalies by definition are not presently comprehended. Anomalies can be occurrences that happened or failed to happen when expected, or they can be conditions that exist deviant from what is expected and intended for a point in time and space. The existence of an anomalous condition does imply some occurrence that produced it; for the purpose of CyOTE's methodology it is helpful to separate those two situations as practical differences exist in how to approach the investigation of each situation.

A triggering event is an anomaly which, when perceived, initiates investigation and analysis to comprehend the anomaly. It is the first anomaly discovered in a set of related occurrences, but does not need to be (and often is not) the earliest chronological occurrence once additional investigation and analysis are underway. Triggering events in this sense are effects as opposed to causes and can be malicious or non-malicious. They are also just one point in a linked sequence of causes and effects, for which the endpoints are not yet known. CyOTE's methodology helps gain visibility on more links in the chain.

PERCEPTION AND COMPREHENSION

CyOTE uses the terms perception and comprehension as opposed to the more recognizable detection and understanding. This deliberate decision is based on a body of work undertaken by NERC's Operating Committee from 2016 to 2017, which uses Dr. Mica Endsley's 1995 model of situation awareness.[5] Although CyOTE is not designed or intended to support real-time situational awareness, the cognitive processes described in Level 1 (Perception) and Level 2 (Comprehension) as shown in Figure 6 are exceptionally well aligned with CyOTE's approach. Perception requires information and comprehension requires context.

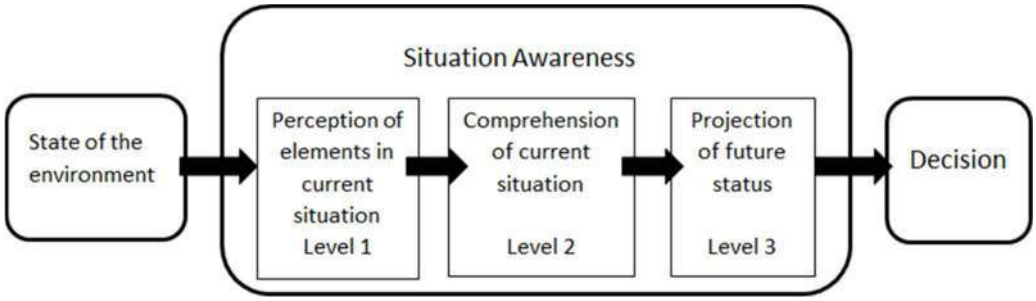


Figure 6. Endsley's Model of Situation Awareness, as Adapted by NERC[6]

Perception is the individual human ability to detect a signature of an occurrence so one or more humans are consciously aware of its existence. For the purposes of CyOTE, the term 'perception' is a more generalized instance of the capability commonly referred to as 'detection' in earlier CyOTE programmatic references and in general cybersecurity parlance. Perception here means a signature capable of being detected by a human was actually detected; perception here does *not* mean opinion or subjective interpretation. A popular saying in the ICS security industry refers to the value of asset visibility, "you cannot defend something you do not know you have." In a similar vein, one cannot comprehend or act on an anomaly never perceived.

Perception is generally synonymous with detection for the purposes of CyOTE, understanding detection sometimes carries the connotation of automated systems, whereas perception is a deliberately human action and ability. As an example, the existence of a Supervisory Control and Data Acquisition (SCADA) alarm (an observable) never consciously seen by a human was not perceived.

Comprehension is the organizational human ability to understand an observable, in all its relevant context across the operations, OT, IT, business, and cybersecurity domains. Comprehension of anomalies usually requires one or more cycles of deliberate investigation to gather and analyze additional data, which may reveal additional anomalies. Because of the multidisciplinary approach used for a sufficient investigation, comprehension for the purposes of CyOTE is an organizational ability, not an individual one. Absolute certainty is rare in the eventual comprehension of anomalies, and the requisite level of confidence in the comprehension of an anomaly in its context necessary to make a business decision is a matter of organizational risk appetite.

Figure 7 provides a helpful mental model to think about the role of perception and comprehension relative to the popular knowns and unknowns thought framework.[i]

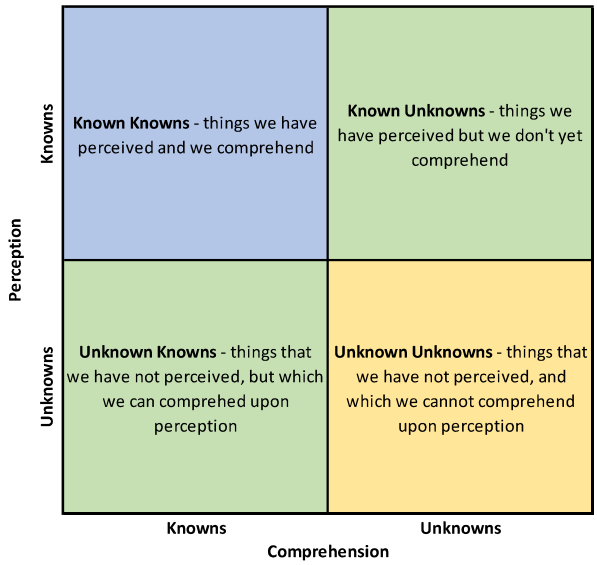


Figure 7. Knowns and Unknowns in Perception and Comprehension

Anomalies as defined in CyOTE fall into the 'Known Unknowns' quadrant because something has been perceived, but is not yet able to be assessed for placement into a Known Known subcategory of either malicious or non-malicious (these subcategories are not shown in the graphic, but should be thought of as 'we are here now so what do we do given that' – which is addressed later in CyOTE's methodology). Things in the bottom two quadrants are not anomalies because they may or may not have occurred, but nobody (at least nobody from the AOO) has perceived it. By improving organizational capability to perceive anomalies – moving from the lower right to the upper right quadrant – we are in effect shrinking the volume of the unknown

[i] See https://uxdesign.cc/the-knowns-and-unknowns-framework-for-design-thinking-6537787de2c5 for a discussion and examples of the Knowns and Unknowns framework.

universe and expanding the known (perceived, not all comprehended) universe. This is depicted in Figure 8 below.

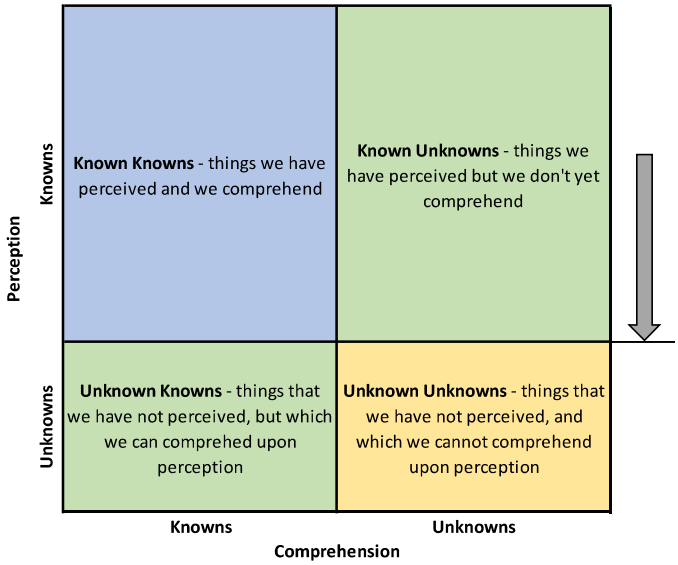


Figure 8. Reducing the Volume of the Unknown World Through Increased Perception

Recently perceived Known Unknowns can then be correlated to malicious cyber activity as enumerated using the ATT&CK Framework for ICS, and detected with capabilities such as those described in the technique detection Fact Sheets or equivalent commercial solutions where those capabilities exist. Through disciplined application of a multidisciplinary process to understand perceived anomalies, and the foundational research from the Use Case and ATT&CK Framework for ICS implementation phase to explain the use of malicious techniques against a generic energy sector AOO, the volume of the unknown universe is shrinking and known (comprehended, whether perceived or not) universe is expanding. This is depicted in Figure 9 below.

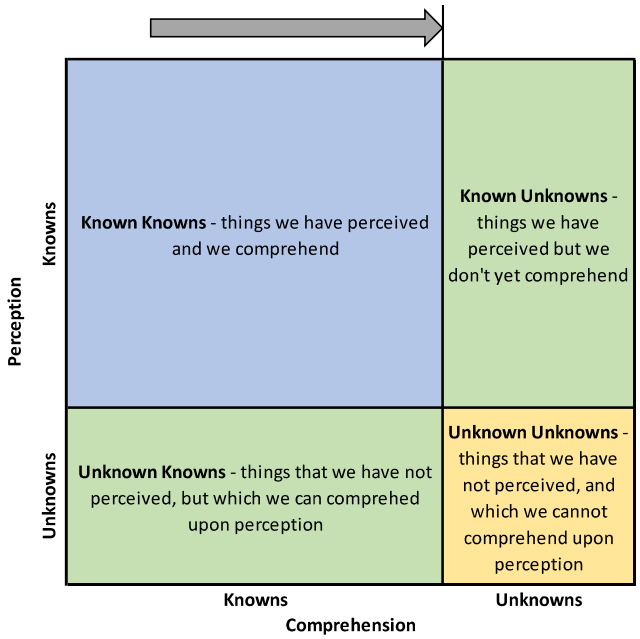


Figure 9. Increasing the Volume of the Known World Through Increased Comprehension

With this mental model of perception and comprehension in a universe of knowns and unknowns in hand, a final key concept must be understood: the Case Study. Born from the insight gained during the Use Case and ATT&CK Framework for ICS implementation activity as the enduring and focused extension of the Use Cases, Case Studies are the process and documentation of analyzing a situation using CyOTE's methodology. Case Studies differ from real-world application of the methodology in their starting point at the logical beginning of the incident as opposed to the time of perception. They can be used to retrospectively learn from noteworthy historical incidents, and also to proactively analyze prospective anomalies of interest to an AOO, whereas CyOTE's methodology is used in the present to investigate actual triggering events. Typically the historical Case Study is based on external accounts of actual situations and conducted by a third party lacking firsthand access to information and the surrounding context that can only come from the subject AOO involved, but has the benefit of hindsight and no performance pressure.

ORGANIZATIONAL MATURITY AND CAPABILITIES

CyOTE allows an AOO to think innovatively and creatively about proactive solutions for OT security, providing a path to advance beyond more reactive traditional approaches based on monitoring to detect certain situations into a new paradigm of holistic analysis to understand anomalies across the entire organization. Although the barrier to entry and ongoing cost to use CyOTE's methodology is intended to be low, it is not a no-cost proposition. Employing CyOTE's methodology requires effort from several different functions within the organization, some of which do not have existing collaboration structures and most of which are in high demand and low supply.

This section provides an overview of seven organizational capabilities that are enablers and multipliers for the value realized by CyOTE. Although organizations exhibit variability in how they are realized given the facts and circumstances, these capabilities apply to all AOOs regardless of their size, business model, or resources. Each capability is required to some degree to be able to employ CyOTE's methodology, but greater maturity, proficiency, and comfort with each should drive greater results. Some of these enabling capabilities are well aligned with domains in DOE's Cybersecurity Capability Maturity Model (C2M2).[7]

RELATIONSHIPS BETWEEN DEPARTMENTS

The success or failure of CyOTE rests on the input and active cooperation of skilled individuals from disparate parts of the AOO organization. Perhaps more pronounced than other examples, this requirement is fundamentally no different than any other organizational effort requiring interdepartmental collaboration. Techniques already familiar to organizations to achieve this collaboration are likely to be adequate when applied to operations, OT, IT, business management, and cybersecurity in the context of CyOTE as well.

> *"This work cannot be done in a silo. Results come from the awareness and the realization that we need the right smart people in the room to be able to have these conversations and find a solution that works well for all."*
>
> *CyOTE Industry Participant, 2020*

ENERGY MONITORING CAPABILITIES AND PRACTICES

Regardless of size or business model, energy sector AOOs adequately monitor their operations (i.e., energy flow) and energy infrastructure status. Many have expansive and increasing high-fidelity visibility of their real-time operations, and advanced decision support and analytic systems on top of the foundational data. This operational information comes from SCADA alarms and telemetry, outage management systems, and asset and maintenance management systems (e.g., SAP or Maximo).

With years of designing, implementing, maintaining, and using these capabilities comes a refined understanding of how the systems and infrastructure are supposed to work, and a strong familiarity with the patterns associated with normal operations as well as some set of abnormal conditions. This knowledge is best when it exists in shared organizational consciousness, but this is built on the collective individual experience of the operators, engineers, and technicians using these systems 24 hours a day, every day, for years. The more this understanding of the system is an accurate shared mental model across more of the organization, the more efficient employing CyOTE's methodology is likely to be.

> *"If you know the enemy and know yourself, you need not fear the result of a hundred battles. If you know yourself but not the enemy, for every victory gained you will also suffer a defeat. If you know neither the enemy nor yourself, you will succumb in every battle."*
>
> *Sun Tzu,* The Art of War[8]

CAPABILITY TO RESPOND TO AND RESOLVE RELIABILITY FAILURES

Similar to the energy monitoring practices described above, AOOs all demonstrate some level of capability to identify, track, and repair the mechanisms of non-malicious failures: equipment failures from old age or mechanical failures, automated systems operating in ways not anticipated by design, damage from the effects of weather and climate, failures compounded by organizational or individual human error, and so on. Without this ability to correct acute deficiencies and to manage the effective age of infrastructures on an ongoing basis, the overall system would have failed catastrophically some time ago.

Different organizations will have a variety of philosophies (e.g., routine diagnostic testing versus run-to-failure), priorities, and resources to impact the mean time to remediate a failure. Whatever this capability may be for an AOO, it represents the default choice for addressing conditions of uncertain causes. This is the null hypothesis in scientific terms, and from a causal analysis perspective it represents a response to the apparent cause, but not necessarily the root cause. Failures whose root cause is not adequately identified and addressed are likely to recur, leading to continued inefficiency and assumption of more risk than necessary.

CAPABILITY TO RESPOND TO AND RESOLVE CYBERSECURITY INCIDENTS

In today's world, cybersecurity is an inescapable aspect of doing business. The capability to respond to and recover from cybersecurity incidents is a necessity for AOOs of any size or business model. Many larger organizations have a robust in-house incident response capability, and some smaller organizations choose to outsource this capability. Others may maintain basic incident response capabilities, and outsource certain niche capabilities (e.g., malware reverse engineering) as needed.

Getting to a high-confidence, risk-informed decision on whether to declare an incident and initiate response actions is the purpose of CyOTE's methodology. Incident response is the alternate hypothesis in scientific terms and in conditions of uncertainty represents a more

conservative choice from a security perspective. This capability to respond to and resolve cybersecurity incidents is well aligned with the Event and Incident Response, Continuity of Operations domain in C2M2.

UNDERSTANDING OF ORGANIZATIONAL RISK APPETITE

When CyOTE's methodology is used, there will come a point where a decision must be made based on the results of the investigation. This is a binary decision. Where inadequate evidence has been found to suspect a malicious cyber nexus, the situation will be handled through existing reliability failure processes; this amounts to failure to reject the null hypothesis. With sufficient evidence, the situation will be handled through cybersecurity incident processes. The question of how much evidence or suspicion is sufficient to reject the null hypothesis is the point of interest here.

This threshold is a direct reflection of an organization's overall risk appetite, and where cybersecurity falls in their prioritized risk register. Although it will certainly vary from organization to organization, it is helpful to have a general idea of what the internal evidentiary standard is to decide. This is best accomplished ahead of time, instead of deciding in the heat of the moment. This understanding of organizational risk appetite is well aligned with the Risk Management domain in C2M2.

> *"If you choose not to decide, you still have made a choice."*
> *Neil Peart,* Freewill[9]

CAPABILITY FOR ORGANIZATIONAL LEARNING AND CONTINUOUS IMPROVEMENT

Events initiated and driven by equipment failure and organizational and individual human error offer valuable insight into the fundamental ways in which complex socio-technical systems fail. The observed impacts of these events are part of the intended effects an adversary can focus on creating intentionally, so an organization can identify and implement improved perception capabilities to identify failure scenario precursors whether they are "normal" or intentional and malicious. Organizations should continue (or begin, if not already part of their culture) to conduct high-quality full-spectrum root cause analyses of significant reliability events, as part of or comparable to NERC's Electric Reliability Organization (ERO) Event Analysis Process.[10]

Development and implementation of barriers against recurring causal drivers can drive improved results in reliability, security, and business over time. This requires habitual analysis and trending of an organization's adverse events, however, and a feedback loop to ensure the analytical insights are available to senior management with the authority to set priorities and allocate resources.

The ability of an AOO to detect fainter and fainter signatures of malicious activity, earlier and earlier in the kill chain over time is what continuous improvement looks like in the context of CyOTE.

> *"It's not enough to do your best. You must first know what to do, and then do your best."*
>
> *W. Edwards Deming*[11]

OT-INSTRUMENTED VISIBILITY

Visibility into network traffic and device behaviors in OT networks today is less than adequate across the sector; no matter the capability of a particular organization in this regard, there is a nearly universal desire for more. As an AOO better understands their OT environment, they may be able to correlate a smaller anomaly to a potential attack, moving the asset owner's threat detection capability earlier into an attack campaign and preventing more significant impacts to operations.

To that end, CyOTE has developed a portfolio of novel technique Fact Sheets, Proof of Concept tools, and Tool Recipes to understand how to detect adversary techniques in a few pilot environments. As CyOTE is not a tool development effort, each of these items provides generalized information for AOOs to procure and deploy their own production-grade tools and capabilities from commercial sources or in-house development. CyOTE's methodology complements these investments by providing a way for AOOs to derive more value from the data they already possess and will acquire through investments in the future.

Both sensors and a way to make sense of the sensor data are needed. The CyOTE Program does not seek to compete with the established and growing commercial sensor market, but rather to provide a way to make sense of the data. Ideally, CyOTE's insights can inform the state of the art in the marketplace. There is a relationship between the capability of OT-instrumented visibility and the Situational Awareness domain in C2M2.

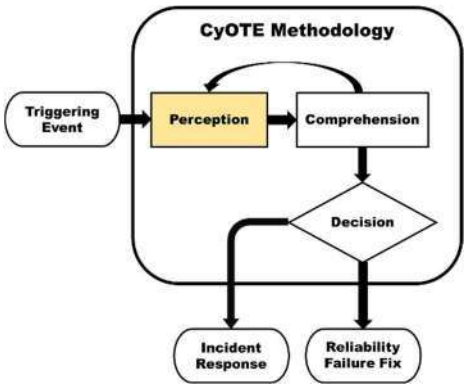
> *"The level of trust we have in our systems has to be limited by the visibility of those systems, and the level of visibility we need must match the consequences of a system failure."*
>
> *Anne Neuberger, 2021 SANS ICS Security Summit Keynote*

EMPLOYING THE CyOTE METHODOLOGY

The prior sections explain the fundamental concepts necessary to understand CyOTE, the prerequisite organizational capabilities needed to employ it, and the history of how these insights were realized. This has set the stage for an explanation of how an AOO starts to put CyOTE into practice and learns how its methodology works with the facts and circumstances of their organization.

PERCEPTION

Perception is the first active step in employing CyOTE's methodology. It provides the starting point—detection of a triggering event in the organization—for investigation during the comprehension step.



Defining a Triggering Event

As described in Key Concepts, triggering events are a subset of anomalies. Not all anomalies are created equal, but can be most generally defined as "any perceived event or lack of an expected event that failed to occur as intended and anticipated, for reasons not presently comprehended." It is important to note that it is expressed as "as intended" not "as designed" since latent error in designs can be a cause of an anomaly, and comparison of as-intended to as-designed to as-built states is useful for the comprehension stage later. In other words, anomalies are something out of the normal and triggering events are anomalies requiring further investigation because they could be a signal of the use of adversary techniques.

Proactively identified triggering events will answer the question of "what anomalies would an adversary's actions to use a particular procedure to implement a technique against my organization create?" Although the adversary techniques of interest are the same, the anomalies that could be generated will vary due to the details of an AOOs' infrastructure and operations. Likewise, it is impossible to standardize the threshold of what constitutes a triggering event resulting in deeper investigation across all AOOs. Rather, the Use Cases generated examples to inform each entity, which must then be tailored for their architecture, organizational structure, asset mix, and philosophy.

An AOO's list of identified triggering events is by necessity a living document, which must be updated as OT environments change, energy infrastructure is commissioned and retired, monitoring and control capabilities evolve, and adversary TTPs and behaviors adapt to changes in their targets and intentions. This living list is the practical embodiment of continuous improvement in an OT cybersecurity context, and also a reflection of the organization's evolving risk appetite as practice at employing CyOTE's methodology over time grows capabilities, which in turn allows the organization to perceive fainter signals, comprehend them more efficiently, and make timely, confident decisions on whether or not to declare a cybersecurity incident and begin response procedures.

Perceiving a Triggering Event

OT systems are typically predictable in behavior in response to external conditions such as weather, with understood causal relationships behind these predictable fluctuations. Therefore, organizations typically have a well-developed understanding of what normal looks like on their system as seen through their tools and processes. At a human physiology and psychology level, perceiving an anomaly is better thought of as perceiving the absence of normal even though these are linguistically equivalent. CyOTE uses three common ways a triggering event can be perceived: programmed alarms, human pattern matching, and business process exception reporting.

Programmed Alarms

The most common initial perception is via human awareness of an automated alarm. Here, alarm is used in the broadest sense, and includes programmatic or routine manual review of logged data from process instrumentation or ICS and network devices, as well as the more common understanding of a visual or audible alarm intended to alert a human operator in near real time. Because of the nature of alarms, these situations are usually tied to an event that occurred and typically include a date and time attached to the alarm.

The success rate of this is dependent on the alarm logic being complete and correct to fire for the intended condition, and the transmission of the required data elements to make the programmed-in determination from the sampling, transduction, or tap point to where the logic engine resides with no compromise of integrity.

In the operations domain, many alarms are defined and presented to a human system operator in a control center via the HMI of the SCADA system. Most SCADA alarms feature a corresponding alarm in the substation control house and/or at the initiating device itself, usually with more details available than in the control center. Depending on the alarm, the system operator may dispatch an appropriate field employee to the facility for further investigation and response. These alarm frameworks and supporting processes are mature for their intended purposes of maintaining safety and reliability, and in the aggregate over time, also can identify anomalies other than those for which the alarms were specifically designed.

In the energy sector OT domain, however, alarms are rarely aggregated or automatically presented to a human for perception purposes. Alarming and logging capabilities do not exist on the oldest legacy devices still in significant production use, and although such capabilities are increasingly more common with newer devices, they are often not configured or used today. In these instances, the “normal” operations are more dependent on human recognition of the behavior of the systems.

Although enterprise IT is not a focus of CyOTE, as a comparison with the IT domain, alarms are defined by the network or endpoint device generating them and typically presented to a human analyst in a security operations center (SOC) or network operations center (NOC) via a security information and event management (SIEM) tool. Frequently, historical trend data is available from the SOC and NOC. In many cases, the analyst will be able to remotely connect to the initiating device for further investigation. These alarm frameworks and supporting processes are

relatively mature for their intended purposes of maintaining information security for an enterprise IT system, and similar to the operations domain, can also be used to identify anomalies through analysis in the aggregate over time. AOOs employing CyOTE's methodology may benefit from adopting modified IT-centric processes and practices for their OT environments, and incorporating threat-focused perspectives more commonly found in IT professionals today.

Human Pattern Matching

Somewhat less frequent, but arguably both more powerful and less dependable at the same time, is human awareness of a situation that, based on their experience and training, is 'out of the normal' but for which there was not an automated alarm. These situations are usually tied to anomalous conditions discovered separately from the event causing them to exist.

Experienced professionals commonly perceive anomalies without the benefit of an automated alarm or a manual review of logs (which could be automated and alarmed) in two ways. The first uses a deadband – a mental model of the acceptable range of results for a given data point – compared to measured values. Assuming a sufficiently well-calibrated mental model, anything falling out of the deadband is an anomaly. Every data point has its own specific deadband parameters for evaluation. The second way humans perceive anomalies is by mentally constructing conditional statements using rules following Boolean if-then-else logic. Related conditionals can also be combined to form more complex logic to be satisfied before human perception is triggered. Much of this cognitive process is subconscious in real time.

Business Process Exception Reporting

A third programmatic way to perceive anomalies is through existing business process monitoring. This is a nontraditional approach for OT cybersecurity, but the practice of exception reporting – identification and explanation of situations where actual performance differs significantly from expectations – is a common business tool. It is most commonly used in accounting and key performance indicators, but in principle can be applied to almost any measure for which data is periodically collected and assessed.

Exception reporting is a type of detective internal control. As such, it is reactive when used as designed, but the anomalies perceptible through exception reporting processes precede the principal harm when it comes to OT cybersecurity, consistent with the ICS Kill Chain. A body of knowledge does not exist to reference here, but possible measures of interest could include increased telecommunications usage, changes in the patterns of service calls, or increased ordering of parts suggesting elevated failure rates. Arguably closer to enterprise IT than business operations, routine audits of user and administrative accounts, privileges, access logs, and other measures are similarly worthwhile measures to monitor.

The goal of anomaly perception through business process exception reporting is to move the sort of "hindsight is 20/20" recognitions further to the left. Surveying existing business reporting processes and making the results available to those responsible for OT and IT security in the organization is a reasonable first step to develop such capabilities. Identifying information of potential interest generated in the course of ongoing business, and where it is created (and

archived, if applicable) would likely come next to permit manual analysis if needed. A significant amount of this exception reporting can be automated using commercial software packages. The challenges in doing this are identifying the measures worth automating, and then developing a baseline of expected results for comparisons.

Who Else Needs to Know?

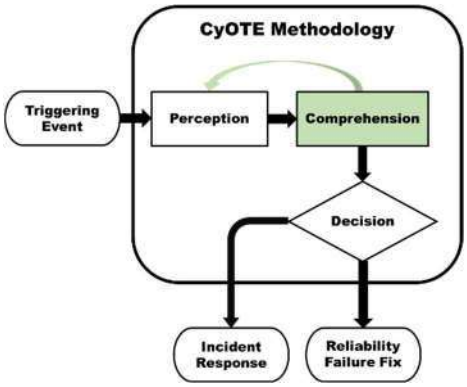
As perception is an individual human activity, transitioning this awareness from the individual to the organization requires a necessary step: reporting and notifications. Although most organizations support an established chain of communications, experience has shown existing communications are inadequate to involve all the necessary groups to investigate triggering events.

An AOO employing CyOTE's methodology should identify the key individuals and departments possibly involved in investigating a triggering event – including, but not limited to those with responsibility for operations, OT, IT, and business processes – and develop a process to notify these points of contact whenever triggering events are perceived.

Beyond triggering events, anecdotal evidence from CyOTE Program participants suggests some departments in otherwise successful organizations maintain less than adequate awareness of relevant occurrences perceived in other departments within the organization. More research and experience are needed to make a confident recommendation in this regard to find a generally acceptable balance between proactive notification of occurrences that could be a triggering event with the added context of other departments, and further loading already strained resources with additional information of infrequent value.

COMPREHENSION

Perception is necessary, but perhaps the easier piece of CyOTE, and arguably of cybersecurity in general. Understanding the nature and possible origins of the triggering event and expanding to develop deeper comprehension and broader awareness of the overall context in which that triggering event came to be—to the point an organization has sufficient confidence to make a risk-informed decision on whether or not to declare a cybersecurity incident and begin response procedures—is the decisive point.



Getting to the risk-informed decision point is a pervasive challenge, however. It is individually and organizationally tempting to take the path of least resistance and choose to categorize anomalies as reliability failures without expending the resources to comprehend the broader context around the triggering event. The significant majority of anomalies do not have malicious causes, and a segment of the industry dismisses the notion an adversary could be behind any anomaly. This is a concerning situation, because advanced adversaries intentionally engineer

their activities to leave very few clues, but there is always a faint residual signature that cannot be completely explained away. In this sense, adversaries use our sense of economic stewardship to not "waste resources looking for ghosts" to help the faint but unescapable traces of their presence continue to be not comprehended as malicious.

To build comprehension, an AOO must first identify useful elements of data and information, who in their organization owns the information, and how it can be accessed. Next this information is used to build context around the triggering event and identify questions and related anomalies from the triggering event. From this point, the AOO pivots to investigating these new questions and anomalies in a recursive process.

Sources of Additional Information: Who, What, and Where

To adequately understand the anomaly will likely require data from systems under the control of different departments, and collaboration with practitioners from those departments to correctly interpret the data. Experience in CyOTE and in other real-world and experimental and exercise conditions has consistently shown developing comprehension around an anomaly is most effective and efficient when small core teams of full-time system operators, OT technicians, and cybersecurity analysts from different departments come together to purposefully focus on the problem in the context of their shared organization. In fact, one of the main indicators further investigation is needed is that no single expert, armed with only their department's data sources, can completely and confidently explain an anomaly.

A psychologically safe environment[j] where operators, analysts, technicians, and management alike all feel free to provide well-intentioned input including bad news without fear of reprisal or being ignored, will empower this information gathering process. Many laypeople describe an organization with an enduring environment of psychological safety as having a healthy culture. If the organization lacks this safe environment, limited opportunity exists to create it from scratch during the course of an investigation, but each engagement will either reinforce or incrementally alter the existing culture.

Although the names vary between organizations, System Operations, Engineering, and Cybersecurity departments should all be involved in the investigation.

System Operations Departments – including both control center and field operators, and real-time engineers – should be one of the first sources consulted. Common industry practice likely will have driven the routine production of manual logs, notes from field personnel investigations, or other records if the anomaly involved a disruption in the system above some established threshold. Although these notes are rarely sufficient to adequately comprehend an anomaly for the purpose of CyOTE's methodology, they often provide a useful frame of reference to define the scope and identify questions to guide the investigation. Even without documentation, the collective understanding of normal and abnormal behavior of the organization's portion of the

[j] See https://web.mit.edu/curhan/www/docs/Articles/15341_Readings/Group_Performance/Edmondson%20Psychological%20safety.pdf for more information on the importance of psychological safety to team learning.

larger grid is useful. Traditional interviews and discovery methods – "let the operators vent and talk" – are often useful because operators frequently know more than they believe they know, and unstructured discussion helps draw out knowledge. This applies to the entire team with knowledge of the systems related to the anomaly, not just the shift supervisor and department manager. Gaining clarity and confidence in core issues usually involves asking the same questions several times in different ways; listen for and expound on the "what if" statements.

Engineering Departments – in this context, meaning those responsible for the design, construction, and maintenance of the ICS infrastructure allowing System Operations to operate the energy infrastructure – can provide unique insight into the environment. Their knowledge of how the system was designed and commissioned for operation most accurately describes normal and abnormal conditions in the context of both network and OT data. Their expertise is required for both the OT communications network and the configuration and operation of the ICS devices on the network.

Cybersecurity Departments – those responsible for the confidentiality, integrity, and availability of the organization's digital assets – provide the threat-informed perspective and bring experience and capabilities to analyze situations and data for security issues. Across the energy sector today, there is no single consistent name or organizational construct for the Cybersecurity department, nor a consistent scope of responsibilities and authorities. Identify and enlist the support of those with responsibility for security of OT environments as well as those with knowledge and experience of adversary behaviors and the investigation of them, however they are aligned in the organization.

Since access to raw data typically requires coordination with human organizational oversight, it is typically better to pursue information and context from different departments within the organization, and when needed have them provide the identified data under their control for shared analysis. These datasets can come in many forms, but from the AOO's perspective for an OT domain observable full packet capture (PCAP) data from network tap points with visibility of the device where the anomaly was perceived, complete device logs (everything that is generated), and netflow data are all valuable sources of information. For observables in the operations physical domain for an AOO example, digital fault recorder (DFR) data including sequence of event recording and oscillography from a point with electrical visibility of the anomaly, discrete event and time-series historian data, and SCADA alarm logs are valuable.

Building Context Around the Anomaly

Anomalies come in many shapes and sizes, so it is counterproductive to follow a one-size-fits-all approach. Comprehension is not a checklist, but rather the creation of a shared mental picture used to form a hypothesis about the non-deterministic world. Although the groupings of the more specific example questions in Appendix C may appear as a checklist-based approach because of the format, it is important to realize applying it with such a deterministic approach will likely fail to deliver the needed comprehension. For the first pass through this step of CyOTE's methodology these processes apply to the triggering event, and these same comprehension processes apply recursively to additional anomalies discovered while investigating the triggering event.

These groupings of questions should be thought of more like different batteries of medical tests experienced specialist physicians can use to help diagnose a patient whose symptoms are clearly perceived, but not yet comprehended in the context of the patient's particular facts and circumstances[k] – do they have a disease, and if so what is it? No single list of questions about an anomaly will provide sufficient information to be able to determine if the anomaly has a malicious nexus, and if so, what it implies (i.e., what adversary technique(s) could it map to in the ATT&CK Framework for ICS).

At this point, the organization needs to start a documentation and knowledge management process instance in support of their investigation. Recording and organizing the datasets and contextual information discovered in some logical manner will not only improve the efficiency and effectiveness of the investigation, but will also prevent duplication of effort by those responsible for the eventual resolution action whether that is incident response or reliability failure management.

Start with a determination of what was actually perceived in the triggering event. Was it a change in:

- the physical domain (something involving telemetered quantities such as voltage, current, frequency, pressure, flow, volume or temperature, or the physical configuration of a piece of infrastructure); or
- the OT domain (something involving traffic or signals transiting a communication medium, or the logical configuration of a piece of infrastructure); or
- both the physical and the OT domains?

Given the determination of a physical or OT starting point, identify what expected corresponding perceptible observables would exist in the other domain and search for their presence or absence. For example, a circuit breaker physically changing state from closed to open in the physical domain would be expected to have either a relay target set in an associated protective relay, or a manual 'open' command from either local or remote control, and a corresponding SCADA alarm message in either case in the OT domain. Similarly, a DNP3 message requesting a select and operate of a circuit breaker in the OT domain would be expected to have a corresponding physical operation of the circuit breaker, an associated change of local electromechanical indicators including semaphores and status lights at the breaker control and local control house, and a record of the breaker operation command in system operator logs. Consistency between the anomaly as perceived in the first domain and the presence of the expected corresponding signature in the other domain is an indication a potential malicious nexus is beyond the present scope of comprehension, but not necessarily a nexus does not exist.

From this point, several general questions will provide insight into where to look next, based on how the actual answers compare to what would be expected in similar known-good circumstances. They should be augmented by other investigative and cause analysis techniques familiar to the organization. NERC's *Cause Analysis Methods for NERC, Regional Entities, and*

[k] *How Doctors Think,* by Jerome Groopman, MD, inspired the author's understanding of this challenge. https://www.amazon.com/How-Doctors-Think-Jerome-Groopman/dp/B0029LHWKY

Registered Entities[12] provides a helpful survey of the most familiar techniques. A selection of representative questions for use is included as Appendix B, intended to give a better idea of extent-of-condition and apparent causal relationships at a point in time.

There are two goals sought from the information gained through asking such questions. The first is to form a rebuttable hypothesis for what technique implementing which tactic (a technique cell on the ATT&CK Framework for ICS tactics and techniques) this anomaly maps to, keeping in mind for physical anomalies this could require significant generalization given the sector-agnostic design of the ATT&CK Framework for ICS. In some circumstances, such a confident hypothesis cannot be formed; although this suggests a potential malicious nexus is beyond the present scope of the anomaly as presently comprehended, it is not sufficient to rule out the existence of such a nexus.

The second goal, more important to driving the process forward and not dependent on whether the first goal was met, is to enumerate all the lines of questioning identified through this stage of the analysis of the anomaly. At this point it is particularly helpful to begin a node and link diagram from the information documented in the knowledge management processes to help visualize relationships between observables; this observables linking diagram is colloquially referred to as a "worm diagram" in the CyOTE Program. The triggering event is the first node, with all its related observables radially connected to it; include both those observables confirmed and those expected but not found, with some sort of visual discriminator between presence and absence (e.g., solid or dashed lines). Highlight the triggering event if it is believed to be the implementation of a specific adversary technique, that is, the first goal from the information gathering process described above was met. Include links emanating from the triggering event representing the as-yet-unanswered questions considered, as well as links and additional nodes for answered questions that confidently satisfy the extent of a particular line of inquiry. A notional example of this diagram, for an investigation in progress, is shown in Figure 10.

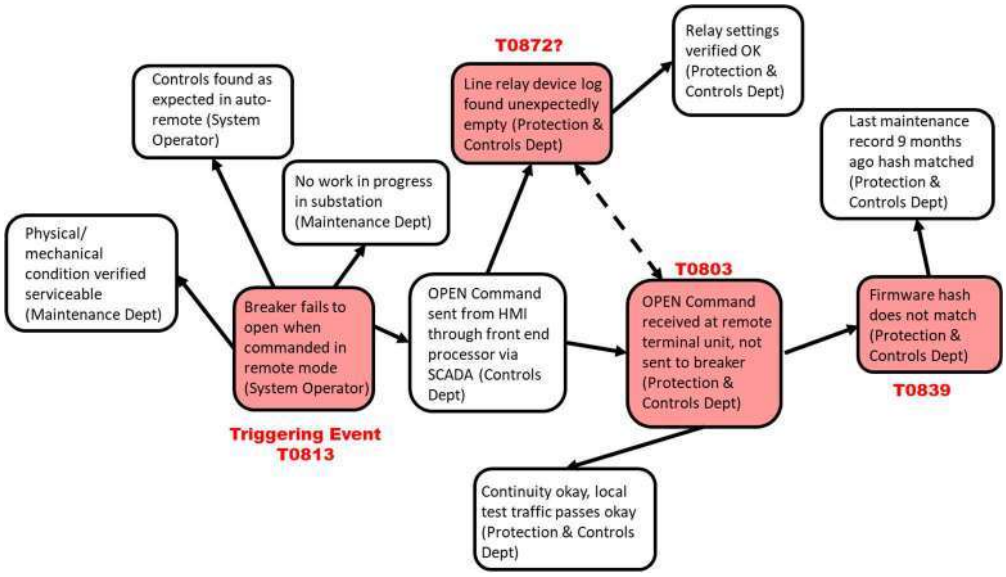


Figure 10. Example CyOTE Observables Link Diagram

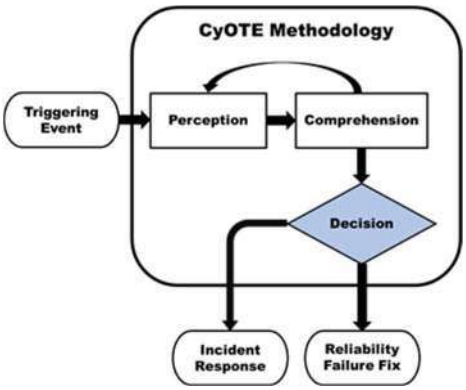
Pivoting to Discover Related Anomalies or Show Their Absence

When a triggering event has been comprehended sufficiently to determine its mapping to a technique, the next step is to is repeat the steps above starting from each of the lines of questioning resulting from analysis of the triggering event. The importance of recording and organizing the information discovered in the comprehension process and visualizing it through a node and link diagram becomes exponentially more important as the triggering event expands into a web of postulated, confirmed, and denied relationships between anomalies.

When the presence of a second ATT&CK Framework for ICS technique (or other anomaly the organization would have considered as a triggering event, had it been the first to be perceived) is identified and mapped, another line of effort becomes available. This is an opportunity to compare the two techniques and consider whether an apparent connection between them exists. This should be analyzed from the technical perspective looking at connectivity and device behavior, as well as from the adversary perspective looking at a plausible sequence of steps in a specific attack campaign. There is not a prima facie assurance the two techniques are sequentially adjacent, and there could be other steps not yet perceived or comprehended to potentially link the two.

This process of pivoting from questions developed in analyzing an anomaly to starting the anomaly comprehension process anew from the starting point should be repeated as needed. Where supported by the data, it may be useful to deliberately switch between the physical and the OT domains in this process of pivoting and expanding. With each iteration through this process, update the node and link diagram to expand the window of visibility into the situation.

ENABLING THE DECISION POINT



The recursive process described above is not intended to be endless. There must come a point to halt this process and make a risk-informed business decision on how to proceed. This decision may be best understood by visualizing the worm diagram of identified techniques, and those occurrences that do not map to an ATT&CK Framework for ICS technique. The presence of one instance of a single technique may be relatively inconsequential in the big picture, but the overall coherence of three or more techniques that do not contradict any un-mapped observations may present compelling evidence of malicious cyber activity.

In the real world, these determinations are unlikely to be clear cut, so the decision may be more of an evolving art form than a hard science. The level of comprehension and detail needed to make the decision will vary from company to company and may be related to resource availability. The length and consistency of a discovered and comprehended "worm diagram" representing a prospective kill chain fragment needed to decide to proceed with incident response will also vary based on a company's risk tolerance, as discussed earlier.

"The Red Pill" – Incident Response Process

In situations where there is sufficient belief the anomalies perceived and comprehended indicate possible malicious cyber activity, the appropriate organizational action is to initiate their cybersecurity incident response process according to organizational policy and procedures. The information and context developed through CyOTE will be useful to incident handlers for developing and implementing appropriate mitigating actions.

Although conducting incident response has a cost, the expected return on that cost is the restoration of trust in OT/ICS that are critical for safety and reliability. This choice could be seen as a demonstration of due care for security.

"The Blue Pill" – Corrective Maintenance Program

In situations where a plausible indication of malicious cyber activity cannot be established, or is confidently disproved, the null hypothesis of a non-malicious failure cannot be rejected, and the appropriate organizational action is to address any deficiencies discovered through corrective maintenance and work management processes according to organizational policy and procedures. It is worthwhile to maintain records of these situations for future reference and comparison to subsequent anomalies.

CASE STUDY EXAMPLES

Case Studies support continued learning through analysis of incidents and events. Some of the richest and most detailed Case Studies are expected to be produced by AOOs who have employed CyOTE's methodology to perceive and comprehend actual triggering events in their OT environments, with the benefit of unfettered access to the best data and context. To bootstrap the learning process and complement anticipated AOO-generated Case Studies, the CyOTE team has begun compiling Case Studies of historical OT attacks and OT-related incidents.

These historical Case Studies are based on publicly available reports of the incidents from media outlets and cybersecurity firms instead of the full context and data that an AOO would have. They are not, nor are intended to be, completely comparable in detail or structure, nonetheless they each provide examples of how key concepts in CyOTE's methodology look in the real world. Perhaps more importantly, these historical incident Case Studies inform learning from the perspective of "how could this have been detected?" instead of "why was this missed?" to grow the body of knowledge on perception, comprehension, and organizational capabilities.

After reviewing a Case Study, AOOs should consider how a similar scenario could unfold in their operating environment, determine the level and location of visibility necessary for them to perceive the triggering event and other anomalies, and identify accessible information sources to build comprehension. The following questions for reflection and discussion can help AOOs prepare to employ CyOTE's methodology in their organization.

- Could you perceive a similar triggering event in your organization? How would it be perceived, and by whom?
- What observables exist that could have been perceived earlier than the triggering event was? How would each be perceived, and by whom?
- Who will you contact from the System Operations, Engineering, and Cybersecurity departments to build comprehension? Would they be willing and able to assist today?
- How much evidence would you need to confidently reject the null hypothesis of a reliability failure, and initiate cybersecurity incident response procedures?
- Who else in your organization needs to be aware of the outcome?

CASE STUDY: OLDSMAR, FLORIDA WATER TREATENT PLANT INCIDENT

On February 5, 2021, an unidentified attacker gained control access to change chemical concentrations of the water supply for nearly 15,000 people at the Oldsmar, Florida water treatment facility. The attacker gained access through a TeamViewer account, which allows remote use of the computer controlling chemical content of an underground water reserve.[13]

The attack occurred in between employee maintenance periods and was discovered when an operator noticed a second occurrence of un-commanded and unusual mouse cursor movement on the computer screen. Although the operator had observed this earlier in the day, there was a lack of comprehension that this was malicious, and it was not registered as being a triggering event requiring further investigations. The attacker accessed and manipulated the plant engineering and automation systems and took action to increase sodium hydroxide levels to

unsafe levels.[14] Upon observing this a second time, the operator took swift action to restore the process to correct parameters, and the organization initiated its cybersecurity incident response process.

Perception - Triggering Event: The triggering event for this incident was the operator perceiving un-commanded and unusual mouse cursor movement changing a critical process setting. In this incident, an individual human operator actually perceived abnormal mouse cursor movement twice, but it was not recognized as abnormal and thus a triggering event until the mouse movement resulted in an inappropriate change to sodium hydroxide levels. Reportedly, it was not uncommon in the organization for an authorized remote user to briefly take control of the HMI to check readings without notifying the operator beforehand, so the addition of inappropriate actions elevated the mouse movement from an event to a triggering event. This highlights the fact individual baselines of what constitutes normal activity will vary from organization to organization.

Comprehension: The Oldsmar incident involved the use of adversary techniques from two of the three CyOTE Use Cases – Remote Login and HMI. Four techniques, used in series, were identified as part of this relatively simple incident. These techniques, in chronological sequence as employed by the adversary and not in order of detection by the victim, are shown in Figure 11.

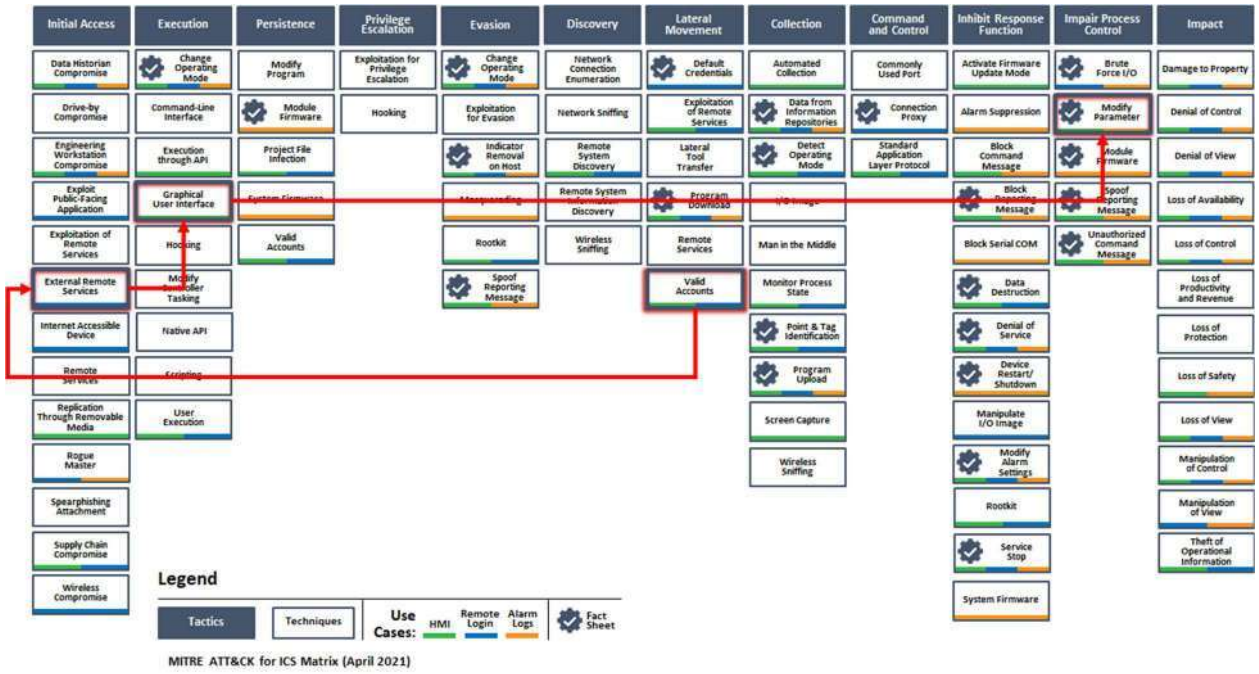


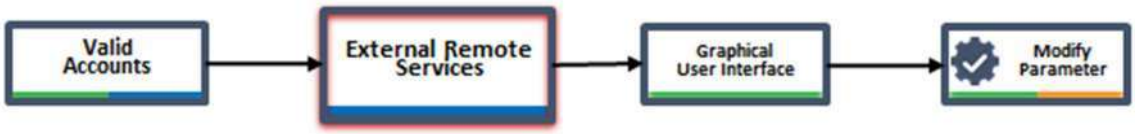
Figure 11. Oldsmar Incident Adversary Techniques Chain

Anomalies, possible related adversary techniques, and example perception methods for the anomalies are detailed below.

Anomaly: Oldsmar passwords were discovered in a password data leak that occurred days prior to the attack.[15]

Technique: Valid Accounts. An attacker gained access to the HMI system using valid user credentials.

Perception Opportunities: Account breach detection services could have alerted the AOO to compromised credentials, which could then be used to alert operators to intrusion attempts if used. A security audit also may have revealed password sharing between employees and services.



Anomaly: With a valid credential, remote access may not appear anomalous on its own.

Technique: External Remote Services. The attacker used the stolen credential to remotely access the system.

Perception Opportunities: Anomalous behavior may be revealed as an unknown source IP, multiple users from the same source IP, one user from multiple source IPs, or a user with valid access pivoting to use the control network in ways not intended or authorized. Remote service logging and monitoring, or VPN host scans or health checks may aid in detection.

Anomaly: Equipment was operated from the HMI, with impacts to the process being controlled, which was not initiated by the control room operator or by an otherwise expected remote access user. This anomaly was the triggering event in this Case Study.

Technique: Graphical User Interface. The attacker used remote access to gain control of the HMI system.

Perception Opportunities: Human operators may identify an uninitiated change on the HMI by observing mouse movement. A more sophisticated attacker may operate the system using keyboard and minimize mouse movement to avoid detection.

Anomaly: The target level of lye in the water treatment facility was raised from 100 to 11,100 parts per million.

Technique: Modify Parameter. The attacker modified an operational parameter outside of safe limits.

Perception Opportunities: Human operators may identify an unexpected change, alarms from the HMI or historian could indicate an out-of-bounds change, automated or human consistency checks with redundant systems could reveal a discrepancy, or downstream alarms from the physical environment could detect the process effects of the change (here, unsafe chemical levels in the water).

CyOTE Proof of Concept Tool: The T836 Modify Parameter uses the ConfigEngine monitors directories and files for modifications. ConfigEngine, one of the Structured Threat Observable Tool Set (STOTS) tools, monitors directories and files for modifications. ConfigEngine uses a custom script to periodically remotely connect to a device, download a user-defined file, and compare it for any changes. If a change is identified, ConfigEngine will generate a Structured Threat Information Expression (STIX™) object and transmit it to the STIX™ monitor.

Decision: Oldsmar's water treatment facility leadership decided this was a cybersecurity incident and initiated their response procedures. In this case, the decision point was reached as soon as the triggering event was perceived, due to the obvious malicious nature of this particular triggering event.

CASE STUDY: TRITON PETRO RABIGH INCIDENT

In June 2017, a section of the Petro Rabigh refinery complex in Rabigh, Saudi Arabia shut down as a result of a Safety Instrumented System (SIS) controller entering a failed "safe state." Since there was no apparent reason for the shutdown, the AOO conducted further analysis.[16] Testing and analysis of a "glitchy" Triconex SIS controller was conducted onsite and in a California laboratory. These analyses drove a review of logs from the plant and determined that the failure was mechanical in nature.

The same incident reoccurred in August 2017, again causing operations disruptions. This prompted engineers to conduct a more thorough causal analysis. Identification of unusual communications beaconing between the complex's IT environment and engineering workstations located in the OT environment were the key to uncovering an ongoing cyber campaign targeting the complex's Triconex SIS controllers.[17]

Perception - Triggering Event: The triggering event for this incident was the discovery of unusual network traffic between the complex's IT environment and engineering workstations in the OT environment subsequent to investigation of the second instance of a shutdown of a section of the plant with an SIS controller in a failed state. This apparent beaconing traffic was the revelation

that changed the effort from an investigation of a repeat equipment failure to an investigation of a security concern.

Comprehension: The Petro Rabigh incident involved the use of adversary techniques from all three CyOTE Use Cases – Alarm Logs, Remote Login and HMI. Nineteen techniques across six series-parallel steps were eventually identified as part of this complex and protracted attack campaign. These techniques, in chronological sequence as employed by the adversary and not in order of detection by the victim, are shown in Figure 12.

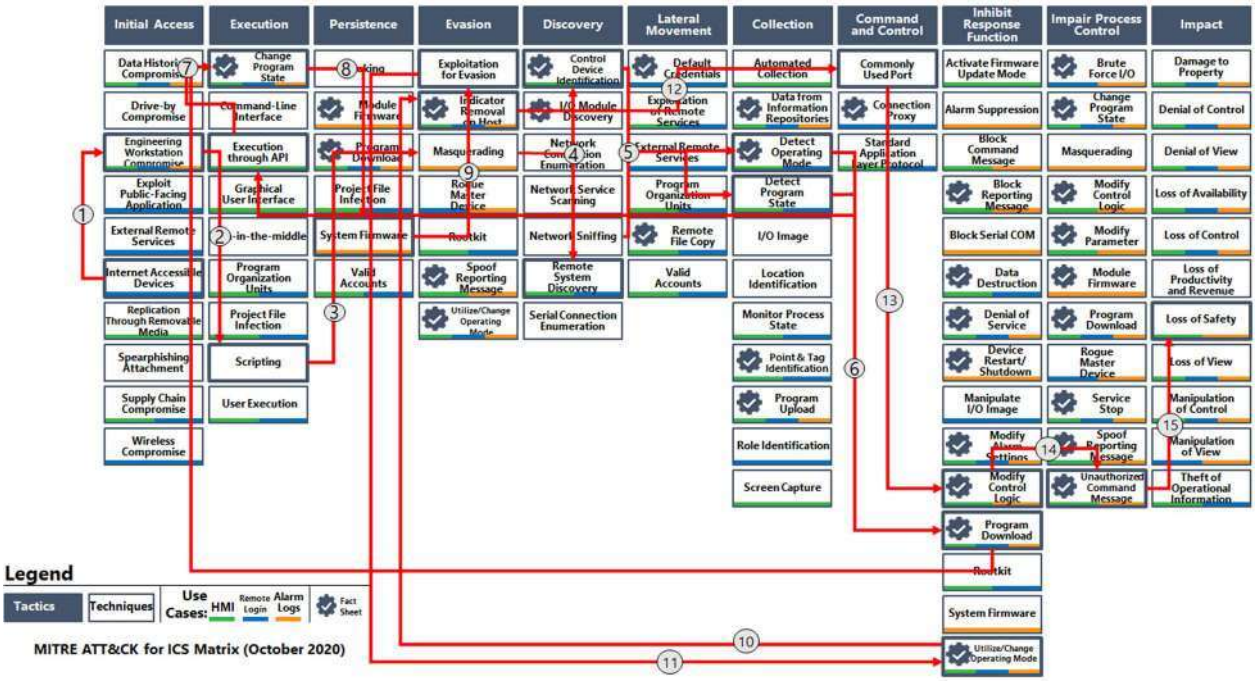
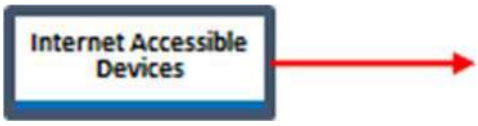


Figure 12. Petro Rabigh Incident Adversary Techniques Chain

Anomalies, possible related adversary techniques, and example perception methods for the anomalies, broken down by general adversary campaign steps, are detailed below.

IT Network Compromise



Anomaly: Increased demilitarized zone (DMZ) traffic between IT and OT networks and beaconing coming from the control network. This anomaly was the triggering event in this Case Study.

Anomaly: Anti-virus software alerted to the presence of the MIMIKATZ credential harvesting tool in the IT network.[18]

Anomaly: Employee phone numbers modified from expected numbers.

Technique: Internet Accessible Device. Remote attackers gained access to corporate computers through a poorly configured firewall, then pivoted to OT networks.

Perception Opportunities: Investigating identified attacks against IT assets for potential to traverse networks. Verifying modifications to important employee information. Monitoring traffic between networks. Assessing new or unusual connections such as Remote Desktop Protocol sessions.

Movement to OT Network

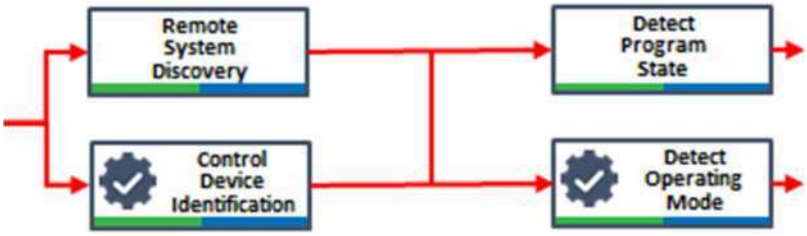
Anomaly: Unfamiliar Py2exe compiled binaries present in an OT environment.

Technique: Engineering Workstation Compromise. "The attacker gained remote access to an SIS engineering workstation and deployed the TRITON attack framework to reprogram the SIS controllers...The malware was delivered as a Py2exe compiled python script dependent on a zip file containing standard Python libraries, open-source libraries, as well as the attacker-developed Triconex attack framework for interacting with the Triconex controllers."[19]

Technique: Masquerading. The name of the Triton malware, "trilog.exe", mimicked the legitimate Triconex Trilog application.

Perception Opportunities: Periodic endpoint scans for unexpected or inappropriate file types or locations.

OT Attack Capability Development



Anomaly: IP addresses for Triconex SIS were discovered in malware code.

Techniques: Control Device Identification, Remote System Discovery. The malware on the engineering workstation contained the ability to send a UDP broadcast packet to identify Triconex devices on the network. This functionality was not used, however, and the IP addresses for the Triconex devices were input directly indicating the adversaries had already obtained the IP addresses.

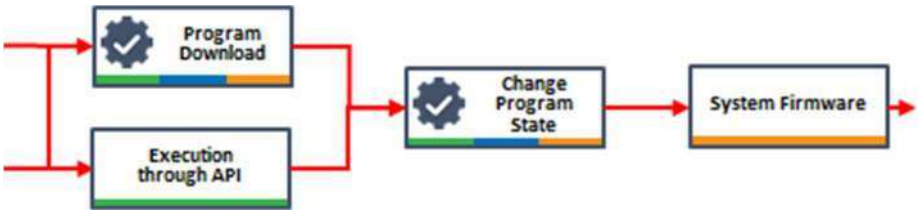
CyOTE Proof of Concept Tool: The T808 Control Device Identification Proof of Concept Tool logs the use of network traffic which can be used to fingerprint or identify a control device. This capability could be leveraged by the AOO to support the Triconex protocol and the broadcast packets used in this attack. The AOO could use the Control Device Identification tool to monitor supported devices and protocols through either live (via a span port) or recorded (via PCAP files)

network traffic. The Proof of Concept tool allows an AOO to define a list of hosts allowed to communicate with a device, such as an engineering workstation.

Techniques: Detect Operating Mode, Detect Program State. The script contained a function which collected key and operating states, and other project information.[20]

CyOTE Proof of Concept Tool: The T868 Detect Operating Mode Proof of Concept tool performs deep packet inspection of Modbus protocols to alert when a "read register" command is identified for the operating mode register. An "allow/deny" configuration file is used to filter alerts from approved hosts and flag unapproved host commands. This capability could be leveraged by an AOO to support the Triconex protocol and command used to detect the operating mode of the device.

OT Attack Capability Delivery



Anomaly: Unexpected shellcode was present on six Triconix SIS controllers.[21]

Techniques: Execution through API, Program Download, Change Program State. A script uses the TriStation protocol for program download, allocation, and modifications. The program was transferred to the Triconex device multiple times overwriting with an empty program checking and then overwriting with the malicious program.

CyOTE Recipe: The T843 Program Download Recipe guides an AOO through the development of a network monitoring capability to detect traffic which would download a device's program. The current capability outlines the process an AOO should consider when building a tool to analyze the OT network traffic and through deep packet inspection to identify potential indicators arising from an attempt to download the program.

CyOTE Recipe: The T875 Change Program State Recipe describes a capability to read and analyze network traffic captures based upon set criteria, located in a separate configuration file. The criteria compare protocol layer fields to static values (e.g., MAC and statically defined IP addresses of hosts). The Recipe identifies the need to alert on trusted IP lists for unauthorized traffic detection, monitors for PLC program download commands from unauthorized host(s), and controllers' running programs forced to a new state (e.g., reset, start, halt) from an operator or engineering workstation

Technique: System Firmware. Shellcode containing two parts, one for running on the system and another for command and control, was injected.

Supporting Attack – Hide

Technique: Exploitation for Evasion. Triton malware disables RAM/ROM consistency checking.

Technique: Utilize/Change Operating Mode. Triton malware only affects controllers left in "Program Mode." Once installed, however, it modifies the system to allow code to ignore key-switch position.

Technique: Indicator Removal on Host. Triton malware attempts to reset the controller to a previous state. If this failed, it would write a dummy program overwriting the malicious program.

CyOTE Recipe: The T872 Indicator Removal on Host Recipe provides industry standard remote process monitoring, remote log aggregation, and best practice host-based access control configuration. The Recipe identifies remote process and log monitoring via a SYSLOG messaging service or a host-based agent, depending on the host's capabilities. The Recipe highlights the data collected and analysis using Elasticsearch and potential alerts resulting from finding indicators of compromise using Kibana messaging.

Technique: Commonly Used Port. The malware communicates with the implant on the Triconex device using specifically crafted legitimate network packets.

OT Attack Execution and Impact

Anomaly: A portion of the plant shut down with the SIS controller in a failed state.

Technique: Modify Control Logic. The malware can reprogram the SIS logic of the Triconex device to trip or shutdown while in a safe state, or conversely to not trip and continue running to allow unsafe conditions to persist.

CyOTE Recipe: The T833 Modify Control Logic Recipe guides an AOO on analyzing OT network traffic and uses deep packet inspection to identify potential indicators arising from an attempt to modify control logic.

Technique: Unauthorized Command Message. An adversary can manipulate the process into an unsafe state from the DCS while preventing the SIS from functioning appropriately.

CyOTE Proof of Concept Tool: The T855 Unauthorized Command Message Proof of Concept tool reads a network traffic capture and analyzes it based upon a set of criteria defined in a separate configuration file. The criteria compare the protocol layer fields to static values, alerting on trusted IP lists for unauthorized traffic detection, and validating the CIP protocol. The tool output provides statistics about triggered criteria, such as number of times triggered, which packets caused the trigger, data about the network streams, and which network streams included the full protocol cycle or only a part. The protocol validation summary also identifies the packets associated with validation (or lack thereof).

Technique: Loss of Safety. The malware has the capability to reprogram SIS logic allowing unsafe conditions to persist or to allow an unsafe state while using the distributed control system (DCS) to create an unsafe state or hazard.

Decision: Petro Rabigh's leadership decided this situation was a cybersecurity incident, and initiated their response procedures. Without the firsthand knowledge and records an AOO would have, the specific point in time this decision was reached is not known, but generally understood to be shortly after the perception of the triggering event.

CASE STUDY: NON-MALICIOUS MEMORY EXHAUSTION

The following case study is based on events which took place during the September 2020 iteration of the Defense Advanced Research Projects Agency's (DARPA) Rapid Attack Detection, Isolation, and Characterization Systems[22] (RADICS) experiment, conducted with the support of DOE. The overall RADICS storyline assumes an adversary actively countering AOO efforts to restore power in a blackstart scenario 30 days into a protracted outage. As a unique aspect of this Case Study, through experience in RADICS up to this point, participating AOOs were conditioned to presume most anomalies perceived were due to a cyber threat in the experiment, instead of collecting information and analyzing the situation to determine a likely cause. This scenario event did not directly affect any specific participant.

During the experiment, an AOO's control center unexpectedly lost communications with the automation controller device in a substation. Power-cycling the unresponsive device did not resolve the problem, so a technician was dispatched to the substation to investigate. Following seven different threads of troubleshooting, the AOO ruled out potential use of 18 adversary techniques with sufficient confidence to decide the loss of communications was a reliability failure and not the result of malicious cyber activity. At this point, an onsite device original equipment manufacturer (OEM) representative was brought in and determined the device had lost communications because its memory was full due to a failure of the local log rotation routine. The AOO had focused its troubleshooting on the communications path instead of the device, likely lengthening the time required to reach a decision on response actions. Forensic analysis by the OEM determined a prior software update had been unsuccessful, and resulted in a specific log file ceasing to rotate once it exceeded a certain file size; because this log file is infrequently written to, it took several months for the non-rotating log file to grow large enough to consume all the storage on the device.

Perception - Triggering Event: The triggering event for this situation was the loss of communications between the control room and a remote substation automation controller. Of note, although this anomaly initiated further investigation, field devices temporarily losing communication is not typically a noteworthy event in and of itself. The experimental context and environment likely drove the AOO to use a somewhat lower threshold for such a triggering event than may be appropriate in a production environment.

Possible adversary techniques investigated and ruled out, and example perception comprehension methods for use of those techniques, are detailed below.

Techniques: Remote File Copy, Program Organization Units, Project File Infection, Manipulate I/O Image, Modify Control Logic, Program Download, Module Firmware, and System Firmware.

Comprehension Opportunities: These techniques all require file uploads, evidence of which could be seen through PCAP analysis and possibly through SIEM capabilities.

Techniques: Valid Accounts.

Comprehension Opportunities: Reviewing logins for irregularities of user, system, location, time and duration could provide evidence of inappropriate use of valid credentials.

Techniques: User Execution.

Comprehension Opportunities: Inspection of physical access logs and network traffic, including web interface traffic, commands which are indicative of user interaction, and traffic authenticated as a user could provide evidence of user execution.

Techniques: Modify Parameter.

Comprehension Opportunities: Application layer packets containing device command messages could provide evidence of parameter modification.

Techniques: Execution through API.

Comprehension Opportunities: In the context of the experiment environment, abnormal or unauthorized API usage detected in network traffic associated with recent technician access to the suspect device could provide evidence of API execution.

Techniques: Command Line Interface, Scripting, Data Destruction, Denial of Service, Service Stop, Masquerading.

Comprehension Opportunities: In the context of the experiment environment, cooperation with the AOO's vendors who have remote access capabilities could provide evidence of these techniques.

Techniques: Supply Chain Compromise, Hooking, Exploitation for Evasion, and Rootkit.

Comprehension Opportunities: Deeper forensic inspection of implicated devices after removal from service could provide evidence of these techniques.

Decision: The AOO's staff ultimately decided this situation was a reliability failure, at the point where they took action to replace the involved device with a spare. Their continued investigation into the causes behind the failure, even in the context of the experiment, gives some insight into their organizational risk appetite, and is an indication of their continuous improvement capabilities.

CONCLUSION

CyOTE's methodology is the product of a combination of research, collaboration with AOOs and government partners, and continuous learning over the course of more than five years. As stakeholders materially increased their understanding of the problem space and opportunities to improve, the energy sector as a whole will benefit from all AOOs having the capability to independently identify potential indicators of malicious cyber activity in their OT environments, sooner and with higher confidence.

The paradigm for OT cybersecurity is due for change to a more holistic analysis starting with the identification of anomalies and leveraging information and context from operations, OT, cybersecurity, and business operations. CyOTE offers a framework to assist asset owners in prioritizing their OT visibility investments likely to give the most benefits the soonest (i.e., identify the low-hanging fruit). CyOTE Use Case participation already has encouraged AOOs to partner internally across departments in their organizations, and exchange insights and ideas on how other companies are tackling OT environment monitoring challenges.

Looking forward, CyOTE seeks to improve through use and feedback to grow the body of knowledge for application by AOOs, tailoring to organizational facts and circumstances. Over time, AOOs' triggering events will move towards fainter signals, detected earlier, to interdict incidents before more significant harms are realized in the face of infrastructure changes, new technologies, and determined and sophisticated adversaries.

The CyOTE team would like to hear about experiences using the methodology to define triggering events, to perceive anomalies in environments, and take a holistic analytical approach to gain comprehension of anomalies. Please share observations with the CyOTE team at CyOTE.Program@hq.doe.gov to help the energy sector continue to maintain its OT cybersecurity.

APPENDIX A: GLOSSARY

Anomaly: An observable deviating from what would be expected and understood as normal in the same or similar circumstances. Anomalies by definition are not presently comprehended.

Asset Owner and Operator (AOO): An entity that owns or operates energy infrastructure assets.

Case Study: The process and associated report describing the analysis of an attack using CyOTE's methodology. A complete Case Study includes identification of the anomalous activity, correlation of the technique(s) associated with the anomalous activity, and creating a view of associated (by time, historical attack tactics, etc.) techniques to understand and identify current risks of potential on-going attacks.

Comprehension: The organizational human ability to understand an observable, in all its relevant context across the operations, electrical, operational technology, and cybersecurity domains.

Data Fields: The individual elements of information type contained in a particular Data Source. These are best thought of as the column headers in a spreadsheet format.

Data Sources: The logical and physical locations where information of potential use in comprehending an anomaly are created and stored. In some cases, the point of creation is different from the point(s) of storage.

Fact Sheet: A high level overview of a MITRE ATT&CK Framework for ICS technique and example cyber-attacks that have employed the identified technique.

Observable: A signature of an occurrence able to be perceived.

Operational Tool: A Proof of Concept tool which has been adapted by and for implementation in an asset owner environment.

Procedure: The lowest-level, highly detailed, environment-specific sequence of steps taken to implement a technique.

Proof of Concept Tool: A representative implementation of a set of steps and methods for detecting techniques.

Recipe: A more detailed product describing a set of steps and methods for detecting techniques.

Tactic: The behavior of an adversary described at a high level in terms of the standalone task to be accomplished.

Technique: A named description of how a tactic can be accomplished.

Triggering Event: An anomaly that, when perceived, initiates investigation and analysis to comprehend the anomaly.

TTP: An acronym for Tactics, Techniques, and Procedures. Often used as a shorthand and informal term to describe the manner in which some action was accomplished, each word has a specific and nested meaning and application such that they are not precisely or formally interchangeable. Unless specified otherwise, TTPs in the context of CyOTE refer to the specific ATT&CK Framework for ICS knowledge base references.

Use Case: The process and associated work products describing a prospective attack of interest using CyOTE's methodology. A complete Use Case includes a description of the postulated high consequence event; an enumeration of the potential Triggering Events that could be perceived; the associated observables in the operations, engineering, cybersecurity, and business domains for each triggering event; and the locations and means of access to data and information helpful to comprehend the Triggering Event and subsequent anomalies. Use Cases are proactive.

APPENDIX B: QUESTIONS FOR COMPREHENSION

These questions are intended to be used as a guide during to gain comprehension of anomalies while employing CyOTE's methodology. They are representative, not exhaustive, and are intended to give a better idea of extent-of-condition and apparent causal relationships at a point in time. AOOs should tailor and augment these suggested questions based on their own experience and context.

- How does the device or system where the anomaly was perceived provide business value to the organization?
    - Describe the tasks (things it does) and purpose (why the organization needs it) for the device or system.
    - Describe what the device is understood to be capable of from its supplier, regardless of whether this functionality is used by the organization.
- Enumerate the observables related to this anomaly, both those perceived and also those expected but not perceived. Although some or most may not be readily apparent, and not all the examples below will relate to every anomaly, there should be multiple observables in different physical and logical locations for most anomalies. These could include, but are not limited to:
    - Digital logs on endpoint ICS devices;
    - OT network traffic ;
    - Telemetered change in system electrical quantities;
    - Change in physical status of electrical infrastructure;
    - Change in other physical condition e.g., damage or changed operating parameters; and
    - Don't discount the five senses, such as hot device enclosures or smelling the 'magic smoke' that should remain contained inside the device.
- Was this the first time such an anomaly has been perceived or do records or institutional memory show similar previous occurrences?
    - If the latter, describe the periodicity or any apparent patterns.
- Was a single device involved, or multiple devices?
    - If multiple devices, describe the as-designed physical and logical relationships between the involved devices.
- With which other devices and systems are the involved device(s) communicating or not communicating?
    - From a network perspective do the observed communications match the as-intended expectation in terms of protocol, endpoints, periodicity, rate, sequence, and relationship to other events?
    - From a device perspective do the observed communications match the as-intended expectations in terms of payloads (structure and content) and relationship to other events?

- Was the anomaly perceived at a time of action/change/movement or discovered in as-found static-at-the-moment condition?
    - If the former, how often does that action/change/movement occur, why does it occur, and from what physical and logical places is it observable?

    - If the latter, what other physical and logical locations and systems in the organization could also show such an anomaly?
- Are any observables related to the anomaly attributable to a specific account or source?
    - When was the last time the permissions for this account were audited or changed? Were these changes intended?

REFERENCES

1. David Bianco, "The Pyramid of Pain." Accessed May 21, 2021. http://detect-respond.blogspot.com/2013/03/the-pyramid-of-pain.html.

2. Machiavelli, Niccolo, and George Bull. 2003. *The Prince*. Penguin Classics. London, England: Penguin Classics.

3. Michael J. Assante and Robert M. Lee, "The Industrial Control System Cyber Kill Chain," *SANS Institute Information Security Reading* Room, October 2015, https://www.sans.org/reading-room/whitepapers/ICS/industrial-control-system-cyber-kill-chain-36297.

4. "ATT&CK® for Industrial Control Systems," MITRE, accessed May 21, 2021, https://collaborate.mitre.org/attackics/index.php/Main_Page.

5. Micah R. Endsley, " Situation Awareness Misconceptions and Misunderstandings," *Journal of Cognitive Engineering and Decision Making* 9, no. 1 (March 2015):4 https://doi.org/10.1177%2F1555343415572631.

6. "Reliability Guideline: Situational Awareness for the System Operator," North American Electric Reliability Corporation, accessed May 21, 2021, https://www.nerc.com/comm/RSTC_Reliability_Guidelines/SA_for_System_Operators.pdf.

7. "Cybersecurity Capability Maturity Model (C2M2)," Department of Energy, accessed May 21, 2021, https://www.energy.gov/sites/prod/files/2014/03/f13/C2M2-v1-1_cor.pdf.

8. Tzu, Sun. 2010. *The Art of War*. PDF. Capstone Classics. Chichester, England: Capstone Publishing.

9. Rush, "Freewill." Recorded September-October 1979. Track 2 on *Permanent Waves*. Mercury, 1980.

10. "EA Program," North American Electric Reliability Corporation, accessed May 21, 2021, https://www.nerc.com/pa/rrm/ea/Pages/EA-Program.aspx.

11. Deming, W. Edwards. 2018. *Out of the Crisis*. The MIT Press. Cambridge, Mass.: MIT Press.

12. "Cause Analysis Methods for NERC, Regional Entities, and Registered Entities (September 2011)," North American Electric Reliability Corporation, accessed May 21, 2021, https://www.nerc.com/pa/rrm/ea/EA%20Program%20Document%20Library/Cause%20Ana

lysis%20Methods%20for%20NERC,%20Regional%20Entities,%20and%20Registered%20Entities_09202011_rev1.pdf.

13. "Lye-Poisoning Attack in Florida Shows Cybersecurity Gaps in Water Systems," NBC News, accessed February 11, 2021, https://www.msn.com/en-us/news/us/lye-poisoning-attack-in-florida-shows-cybersecurity-gaps-in-water-systems/ar-BB1dxMlI.

14. "Plant Automation Yields Immediate ROI," McKim & Creed, accessed February 11, 2021, https://www.mckimcreed.com/portfolio-page/plant-automation-yields-immediate-roi/.

15. "Oldsmar, Florida water facility credentials contained in COMB data leak," CyberNews, accessed February 11, 2021, https://cybernews.com/news/oldsmar-florida-water-facility-credentials-contained-in-comb-data-leak/.

16. "Analyzing the TRITON industrial malware," Midnight Blue Labs, accessed May 5, 2021, https://www.midnightbluelabs.com/blog/2018/1/16/analyzing-the-triton-industrial-malware.

17. "The Inside Story of the World's Most Dangerous Malware," Energywire, accessed May 5, 2021, https://www.eenews.net/stories/1060123327.

18. "Triton/Trisis Attack Was More Widespread Than Publicly Known," Dark Reading, accessed May 5, 2021, https://www.darkreading.com/attacks-breaches/triton-trisis-attack-was-more-widespread-than-publicly-known/d/d-id/1333661.

19. "Attackers Deploy New ICS Attack Framework "TRITON" and Cause Operational Disruption to Critical Infrastructure," FireEye, accessed May 5, 2021, https://www.fireeye.com/blog/threat-research/2017/12/attackers-deploy-new-ics-attack-framework-triton.html.

20. "MDudek-ICS/TRISIS-TRITON-HATMAN," GitHub, accessed May 5, 2021, https://github.com/MDudek-ICS/TRISIS-TRITON-HATMAN/blob/master/decompiled_code/library/TsHi.py.

21. "The Inside Story of the World's Most Dangerous Malware," Energywire, accessed May 5, 2021, https://www.eenews.net/stories/1060123327.

22. "Technologies to Rapidly Restore the Electrical Grid after Cyberattack Come Online," Defense Advanced Research Projects Agency, accessed June 10, 2021, https://www.darpa.mil/news-events/2021-02-23.