PRECURSOR ANALYSIS REPORT: BAKU-TBILISI-CEYHAN (BTC) PIPELINE EXPLOSION IN REFAHIYE, TURKEY 2008

Cybersecurity for the Operational Technology Environment (CyOTE)

30 SEPTEMBER 2022

CyOTE Cybersecurity for the Operational Technology Environment

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

INL/RPT-22-69763

TABLE OF CONTENTS

FIGURES

TABLES

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

PRECURSOR ANALYSIS REPORT: BAKU-TBILISI-CEYHAN (BTC) PIPELINE EXPLOSION IN REFAHIYE, TURKEY 2008

1. EXECUTIVE SUMMARY

The Baku-Tbilisi-Ceyhan (BTC) Pipeline Explosion in Refahiye, Turkey 2008 Precursor Analysis Report leverages publicly available information about the BTC Pipeline explosion on 5 August 2008 and catalogs anomalous observables for each technique employed in a cyber attack scenario inspired by actual events. This analysis is based upon the methodology of the Cybersecurity for the Operational Technology Environment (CyOTE) program.

CyOTE analysts used reporting of alleged cyber activity leading up to the explosion to create a cyber attack scenario to demonstrate how internet-exposed devices, unsegmented networks, shared resource between information technology (IT) and operational technology (OT), and operating control systems with vulnerabilities can contribute to difficult-to-detect adversarial behavior that results in a high-consequence event. This report is not a representation of the actual events, nor of privileged information, but a sequence of historically relevant information that enables organizations with OT systems to learn and prepare for similar adversarial behavior.

On 14 December 2014, Bloomberg reported an adversary destroyed the pipeline with a coordinated cyber attack associated with the Russian invasion of Georgia on 8 August 2008.[1] The global impact of the explosion was that BTC could not deliver approximately 1% of the world's oil for 20 days. The victims of the incident were primarily the Turkish state-owned operating company Boru Hatları İle Petrol Taşıma Anonim Şirketi (BOTAS) and the BTC consortium of owners, which includes 11 multinational energy companies. The explosion caused more than 30,000 barrels of oil to spill and cost the BTC consortium $5 million per day ($100 million total) in transit tariffs alone. One of the companies in the consortium lost $1 billion in export revenue over the 20 days of recovery.[2] CyOTE analysts assess that the total financial loss for the consortium is $3 to $4 billion dollars in lost export revenue and legal liabilities.[a]

Researchers and analysts identified 16 unique techniques (used in a sequence of 18 steps) utilized during the alleged attack with a total of 134 observables using MITRE ATT&CK® for Industrial Control Systems. The CyOTE program assesses observables accompanying techniques that adversaries use prior to the triggering event to identify opportunities to detect malicious activity. If observers within the targeted organization perceive observables accompanying the attack scenario techniques and investigate prior to the triggering event, earlier comprehension of malicious activity can take place. Fifteen of the identified techniques, used to create a cyber attack scenario based on the 2008 BTC Pipeline incident, were precursors to the triggering event. Precursor analysis identified 99 observables associated with these precursor techniques, 41 of which were assessed to have an increased likelihood of being perceived in the 547 days preceding the triggering event. Operators' response and comprehension time could be improved by preparing for a similar cyber attack scenario.

The information gathered in this report contributes to a library of observables tied to a repository of artifacts, data sources, and technique detection references for practitioners and developers to

[a] This calculation is based upon the $1 billion loss attributed to the State Oil Fund of the Republic of Azerbaijan and the estimated losses of the 10 other owners according to their shares of BTC.

support the comprehension of indicators of attack. Organizations with OT systems can use these products if they experience similar observables or to prepare for comparable scenarios.

2. INTRODUCTION

The Cybersecurity for the Operational Technology Environment (CyOTE) program developed capabilities for energy sector organizations to independently identify adversarial tactics and techniques within their operational technology (OT) environments. Led by Idaho National Laboratory (INL) under leadership of the Department of Energy (DOE) Office of Cybersecurity, Energy Security, and Emergency Response (CESER), CyOTE is a partnership with energy sector owners and operators whose goal is to tie the impacts of a cyber attack to anomalies in the OT environment to determine whether the anomalies have a malicious cyber cause.

2.1. APPLYING THE CYOTE METHODOLOGY

The CyOTE methodology, as shown in Figure 1. CyOTE Methodology, applies fundamental concepts of perception and comprehension to a universe of knowns and unknowns increasingly disaggregated into observables, anomalies, and triggering events. The program utilizes MITRE's ATT&CK® Framework for Industrial Control Systems (ICS) as a common lexicon to assess triggering events. By leveraging the CyOTE 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 organizations in prioritizing their OT environment visibility investments.

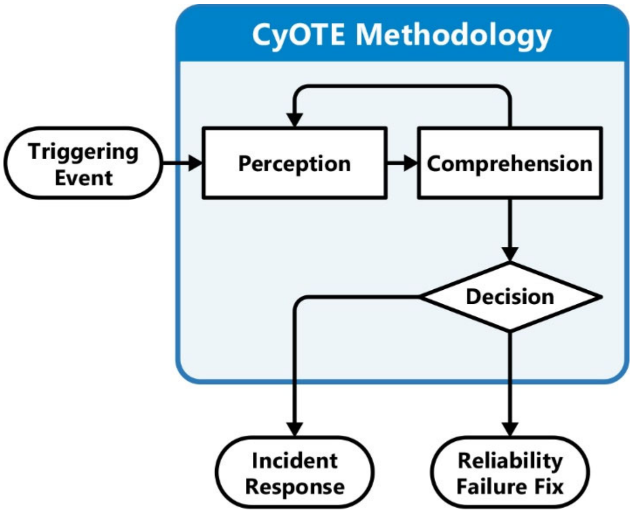


Figure 1. CyOTE Methodology

Historical case studies such as this one support continued learning through analysis of incidents that have impacted OT. This precursor analysis report is based on publicly available reports and provides examples of how key concepts in the CyOTE methodology appear in the real world, providing insights on how similar novel attacks could be detected earlier and therefore mitigated. The analysis enables OT personnel to independently identify observables associated with techniques known to be indicators of attack within OT environments. The identified observables highlight anomalous events for further investigation, which could enhance comprehension of malicious activity.

A timeline of events based on the CyOTE methodology portrays the attack-related observables associated with the case study's cyber attack. The timeline includes assessed dates, the triggering event, and comprehension of malicious activity by the organization. The point on this timeline when each technique appears is critical to the organization's ability to perceive and comprehend the associated malicious activity. Perception of techniques early in the timeline is critical, since halting those techniques will generally have greater potential to limit additional attack vectors using other techniques, defeat the cyber attack, and limit damage to operations.

Each technique has an assessed perceivability. Perceivability is a function of the number of observables and the potential for personnel to detect those observables. If a technique includes effects which personnel may detect, such as deletion or modification of system files or required user execution, then the technique would be more perceivable.

Differences in infrastructure and system configurations may present different challenges and opportunities for observable detection. For example, architecture-wide endpoint monitoring is likely to improve the perceivability of techniques which modify host files, such as the Data Destruction technique (T0809) for Inhibit Response Function and Theft of Operational Information technique (T0882) for Impact. Network monitoring and log analysis capabilities are likely to improve perceivability of techniques which create malicious network traffic, such as the Standard Application Layer Protocol technique (T0869) for Command and Control, External Remote Services technique (T0822) for Initial Access, and Connection Proxy technique (T0884) for Command and Control. Alternatively, enhancing the monitoring parameters of system files would increase the perceivability of techniques such as Data from Information Repositories technique (T0811) for Collection and the Service Stop technique (T0881) for Inhibit Response Function.

Comprehension can be further enhanced by technique artifacts created when adversaries employ certain attack techniques. The CyOTE program provides organizations with a library of observables reported in each historical case. The library can be used in conjunction with a repository of artifacts, data sources, and technique detection references for practitioners and developers to support the comprehension of indicators of attack.

2.2. BACKGROUND ON THE ATTACK

The Baku-Tbilisi-Ceyhan (BTC) pipeline experienced a rupture, explosion, and fire at 11:03 PM[b] on 5 August 2008 (D-0) at block valve 30, about 10 miles east of Refahiye, Turkey, and just 50 meters north of the E80 Highway.[3] As a result, the transnational pipeline through Azerbaijan, Georgia, and Turkey was shut down until 25 August 2008 (D+20).[4] In the wake of the incident, several hypotheses emerged about whether the explosion was due to a reliability event, an act of terrorism, or a cyber attack.

With regard to reliability, maintenance issues involving out of specification welds and failure-prone leak detection systems had been a concern for approximately 18 months prior to the explosion (D-547, estimated as 5 February 2007). As recently as 24 June 2008 (D-42), a maintenance team repaired several welds after inspections identified they were outside of tolerance.[5]

After the explosion at 11:03 PM on 5 August (D-0), operators failed to respond for 40 minutes due to failed alarm notifications (M+40). Operators then closed block valves 29 and 31, isolating the fire until it burned out on 9 August (D+4).[6]

British Petroleum (BP) publicly reported the incident at 1:08 AM on 6 August, (H+2). The pipeline remained shut down and under repair until 25 August (D+20),[7] when pipeline operator Boru Hatları İle Petrol Taşıma Anonim Şirketi (BOTAS) returned it to normal operations.[8]

A Bloomberg article published six years later on 14 December 2014 stated that a cyber attack, conducted by a sophisticated adversary, contributed to the incident. The article reported that footage from infrared cameras near block valve 30 showed men in military-style uniforms with a laptop a few days before the explosion (D-4).

The article quoted several anonymous sources who stated the adversary gained initial access to the pipeline through an unsecured IP-based video camera system four days prior to the explosion (D-4) and moved laterally into the control systems. The alleged attack began with the IP-based CCTV system which shares resources with a Windows system that contained a vulnerability. This vulnerability enabled the adversary to gain access to the system that controls and manages remote terminal units (RTUs) at block valve 30.[9] The adversary then deployed malware to cause a valve to close which over-pressurized the pipeline, resulting in a rupture and explosion. The attackers also managed to suppress pipeline alarms and block reporting messages, resulting in operators not being aware of the explosion until 40 minutes after the fact.[10] CyOTE analyst assess the Bloomberg article represents the final comprehension of the cyber attack scenario (Y+6).

[b] All times are set to the local time zone in Refahiye, Turkey (UTC +3).

2.3. CYBER ATTACK SCENARIO

This section will leverage the conflicting reporting and circumstantial evidence about the pipeline explosion to create a cyber attack scenario to provide organizations with OT systems an opportunity to learn and prepare for possible sequences of techniques that adversaries could use during malicious cyber behavior.

Initial access via internet-exposed devices aligned with the reported maintenance failures that began on 5 February 2007 (D-547), the presence of repair teams on 24 June 2008 (D-42), and the two men with laptops identified via infrared cameras (D-4) before the 5 August (D-0) triggering event.[11] Physical access would not have been a requirement, but an on-site understanding of the block valve equipment would enable more precise cyber-physical coordination.

Once the adversary accessed the cameras, they used default or valid credentials to maintain access and move throughout the network by scanning for an internet-exposed router using a netstat command.[12] The Pelco IP-based cameras used for CCTV shared a common router connection with a database that served as a CCTV data storage and data historian for control systems that were geographically collocated for ease of administration, in this case for the block valve 30 camera and corresponding RTU.[13]

Once the adversary determined the type of RTU, they were able to identify a vulnerability in the RTU control application on the Engineering Workstation (EWS) that had a public exploit available since 16 June (D-50).[14]

The adversary used a Metasploit module to discover valid credentials from various system information repositories to establish persistence on the RTU EWS.[15] The adversary then used the EWS to send unauthorized command messages, block RTU reporting messages, suppress RTU alarms, and manipulate RTU valve positions to over-pressurize the block valve.

A timeline of theoretical adversarial techniques is shown in Figure 2. The timeline includes the estimated number of days prior to and after the triggering event. The timeline after the triggering event includes the assessed victim comprehension timeline.

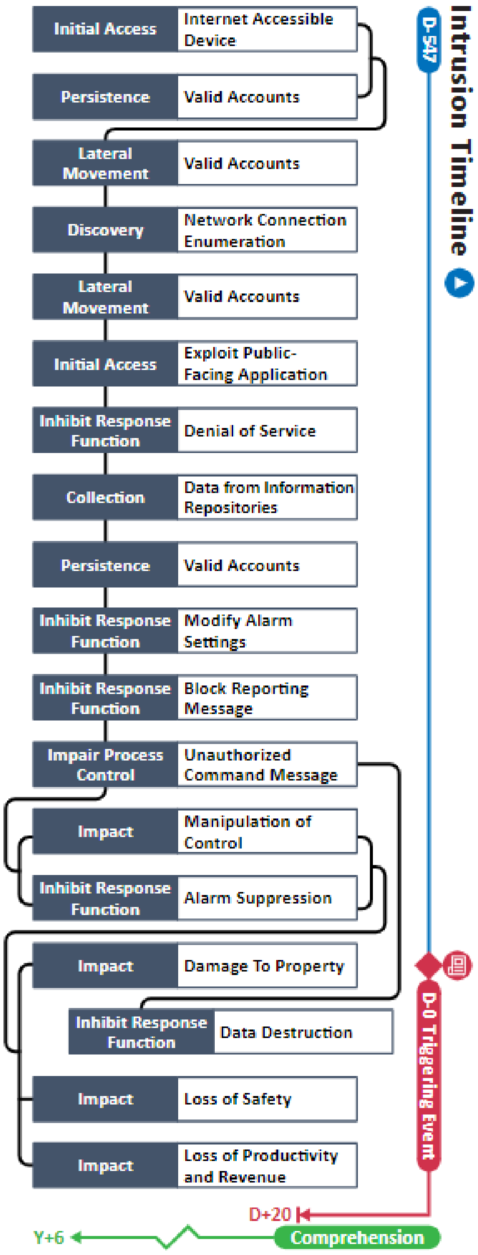


Figure 2. Intrusion Timeline

The theoretical adversary coordinated the attack with an explosives team, which set off a small explosion recorded by CCTV (H-1).[c] The adversary then deleted the footage of the ground team

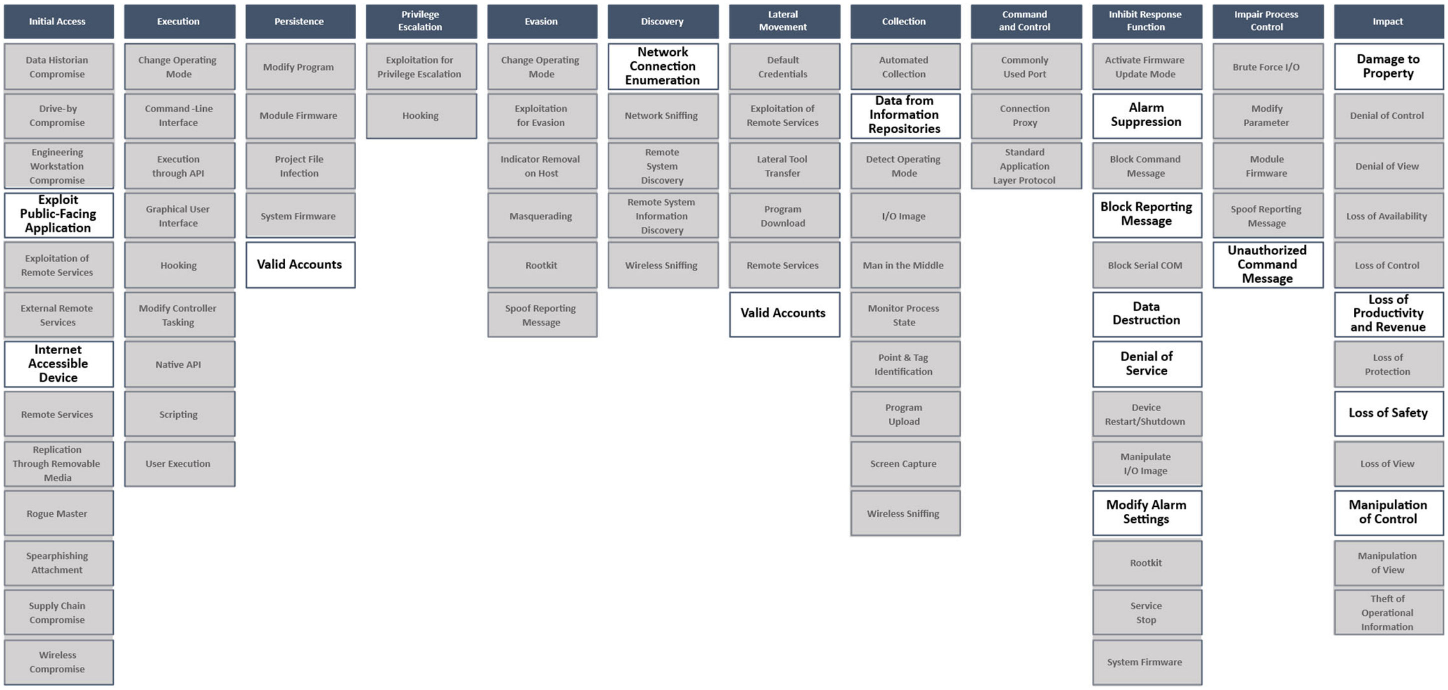
[c] The cyber attack scenario includes a sabotage team because of the reported evidence of "terrorist" activities that included the use of explosives during this event and at other locations along the BTC pipeline throughout 2008.

(M+15) to cover their tracks. The triggering event was the explosion at 11:03 PM on 5 August (D-0), with operators finally receiving notification 40 minutes later at 11:43 PM (M+40).[16]

BTC suffered a loss of productivity and revenue from 5 August (D-0) until 25 August (D+20). Cyber analysts and researchers assess that the comprehension date was 14 December 2014 (Y+6), when Bloomberg made the first public report of the postulated cyber attack.

Analysis identified 16 unique techniques in a sequence of 18 steps and timeframe likely used by the adversary during this cyber attack scenario (Table 1). These attack techniques are defined according to MITRE's ATT&CK® for ICS framework.

Table 1. Techniques Used in BTC Pipeline Cyber Attack Scenario



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

Table 2. Precursor Analysis Report Quantitative Summary

Precursor Analysis Report Quantitative Summary	Totals
MITRE ATT&CK® for ICS Techniques	18
Technique Observables	134
Precursor Techniques	15
Precursor Technique Observables	99
Highly Perceivable Precursor Technique Observable	41

3. OBSERVABLE AND TECHNIQUE ANALYSIS

The following analysis may assist organizations in identifying malicious cyber activity earlier and more effectively. The following techniques and observables were compiled from publicly available sources and correlated with expert analysis. This sequence of techniques supports the development of a cyber attack scenario inspired by historical events.

3.1. INTERNET ACCESSIBLE DEVICE TECHNIQUE (T0883) FOR INITIAL ACCESS

The adversary gained initial access by connecting to an internet accessible Pelco IP-based video camera system used by the BTC pipeline to observe the fenced block valve locations.[17] IP-based cameras commonly use Real Time Streaming Protocol (RTSP) over Port 554 to connect to hosts.[18] The adversary used an external host to connect to the CCTV cameras over a RTSP connection.[19] This activity likely first appeared on 5 February 2007 (D-547) and last appeared on 5 August 2008 (D-0).

IT Staff, IT Cybersecurity, and OT Cybersecurity may have been able to observe the adversary exploiting an IP-based camera system.

Two observables could be identified with the use of the Internet Accessible Device technique (T0883). This technique is important for investigation as industrial operators may not be aware of internet-accessible devices that share resources with control systems. This technique appears early in the timeline and responding to it will degrade an adversary's ability to gain access into the victim's network. Terminating the chain of techniques at this point would minimize the opportunities for an adversary to gain access to the OT environment.

Both observables are assessed to be highly perceivable.

Please see Appendix A for the list of observables.

CyOTE Capabilities for Technique Perception and Comprehension	
Artifacts **(See Appendix B)**	A total of 23 artifacts could be generated by the Internet Accessible Device technique
Technique Observers[d]	IT Staff, IT Cybersecurity, OT Cybersecurity

[d] Observer titles are adapted from the Job Role Groupings listed in the SANS ICS Job Role to Competency Level Poster. CyOTE products utilize these job categories rather than organizational titles to both support comprehensive analysis and preserve anonymity within the victim organization. A complete list of potential observers can be found in Appendix C.

3.2. VALID ACCOUNTS TECHNIQUE (T0859) FOR PERSISTENCE

The adversary used default or common credentials to access the IP based cameras. The adversary likely used open-source explanations of RTSP IP authentication. This activity created a normal successful logon event from an external host over the RTSP Port 554. The user account that logged in was associated with an anomalous external IP address. This activity likely first occurred around 05 February 2007 (D-547) and last appeared on 05 August (D-0).

IT Staff and IT Cybersecurity personnel may have been able to observe the use of default or valid credentials to access IP exposed devices.

A total of five observables were identified with the use of the Valid Accounts technique (T0859). This technique is important for investigation because adversaries may use compromised or default credentials to bypass access controls to various resources within a network or grant an adversary increased privileges to specific systems and devices. Additionally, compromised or default credentials may limit the ability of defenders to detect potential intrusions or compromises due to elevated access levels and privileges afforded by unsecured accounts. This technique appears early in the timeline and responding to it will deny an adversary continued access to any internal resources. Terminating the chain of techniques at this point would prevent an adversary from moving laterally to shared resources.

Of the five observables associated with this technique, three are assessed to be highly perceivable (Network Traffic Over RTSP TCP 554 POST Request Using Default Administrator Credentials with Logon from Anomalous External IP Host; Successful Logon to Device with Public IP Address (Windows Event ID 4624) Network Session Created Over RTSP TCP Port 554 with Anomalous External IP Host).

Please see Appendix A for the list of observables.

CyOTE Capabilities for Technique Perception and Comprehension	
Artifacts **(See Appendix B)**	A total of 16 artifacts could be generated by the Valid Accounts technique
Technique Observers	IT Staff, IT Cybersecurity

3.3. VALID ACCOUNTS TECHNIQUE (T0859) FOR LATERAL MOVEMENT

Once the adversary gained access to the Pelco IP-based cameras and authenticated with default or common administrator credentials, they moved through the camera network segment to determine what they could access.[20,21] The IT and OT Staff configured the network to share resources for devices operating at the block valve 30 location to ease the burden of administering and monitoring field devices and control stations in the same geographic location.

The adversary used valid accounts from the Pelco IP-based cameras to log in to the digital video recording database storage server, Pelco command server, and Pelco application. The adversary used the account on all CCTV resources to determine which devices were accessible and which were not. The adversary logged into two Windows servers 192.10.5.30 (MS SQL Server) and 192.10.5.31 (Pelco Camera Command Server), creating Event IDs 4624, 4648, and 4672 each time they logged on from External Host IP: 10.10.24.36. This activity likely first appeared around 5 February 2007 (D-547) and last appeared on 05 August (D-0).

IT Staff, IT Cybersecurity, and OT Cybersecurity personnel may have been able to observe the anomalous use of valid accounts across a variety of servers and resources associated with IP-based cameras.

A total of 11 observables were identified with the use of the Valid Accounts technique (T0859). This technique is important for investigation because the use of valid accounts across shared resources is one way an adversary could remain undetected as they move toward control system resources. This technique would appear early in the attack and responding to it would deny the adversary the ability to discover shared resources with control systems. Terminating the chain of techniques at this point would severely degrade the adversary's ability to exploit vulnerabilities in software related to control systems.

Of the 11 observables associated with this technique, five are assessed to be highly perceivable (User Successfully Logs On to Local IP-Based Security Camera from Anomalous External IP Host; Local IP-Based Security Camera Special Privileged Assigned to New Logon (Windows Log Event ID 4672); User Successfully Logs On to Local Security Camera Control Server from Anomalous External IP Host; User Successfully Logs On to Local MS SQL Server Camera Storage Database from Anomalous External IP Host; Local MS SQL Server Camera Storage Database Special Privileged Assigned to New Logon (Windows Log Event ID 4672)).

Please see Appendix A for the list of observables.

CyOTE Capabilities for Technique Perception and Comprehension	
Artifacts **(See Appendix B)**	A total of 16 artifacts could be generated by the Valid Accounts technique
Technique Observers	IT Staff, IT Cybersecurity, OT Cybersecurity

3.4. NETWORK CONNECTION ENUMERATION TECHNIQUE (T0840) FOR DISCOVERY

The adversary used the netstat command on the Pelco CCTV control server using the valid credentials from an external host.[22] This command discovered shared resources within the network segment. The adversary discovered that the segment associated with the Pelco IP-camera contained a camera control server operating on Windows XP, Pelco camera application, and SQL database with various resources storing data over an Open Database Connection (ODBC) application programming interface (API).[23] The netstat command showed the adversary which database host IP addresses communicate over the common SQL Server TCP Port 1433 and the dedicated administrator connection TCP Port 1434. The adversary discovered the camera database was Microsoft SQL Server 2005 at IP: 192.10.5.30.

The use of nmap revealed that the pipeline IT staff installed the SQL server pack on 19 March 2008 (D-139) and the database communicated with 200 different private IP addresses in the 192.10.5.0/24 subnet.[24] The adversary identified 63 Pelco IP-Based cameras communicating with the camera control server running the Pelco camera application communicating over RSTP TCP 554. An additional host, identified as the EWS, communicated with the MS SQL Server over TCP Port 1433. The adversary determined that the MS SQL server was communicating with 63 Schneider Electric RTU controllers over TCP Port 1433. These cameras and RTUs were associated with the 63 block valves on the pipeline within Turkey. This activity likely took place between 5 February 2007 (D-547) and 15 April 2008 (D-112).

IT Staff, IT Cybersecurity, and OT Cybersecurity personnel may have been able to observe the use of the network discovery command from the camera control server.

A total of eight observables were identified with the use of the Network Connection Enumeration technique (T0840). This technique is important for investigation because it generates observable host-to-host network traffic across a network segment that shares resources with a control system. This technique appears early in the sequence of techniques and responding to it will delay the adversary’s ability to discover shared resources with internet facing devices. Terminating the chain of techniques at this point would prevent the adversary from gaining awareness of targeted OT systems.

Of the eight observables associated with this technique, two are assessed to be highly perceivable (Valid User Account Logons to IP-Based Camera Control Server from Anomalous External Host IP; Valid User Account Logons to Internal Camera MS SQL Server from Anomalous External Host IP).

Please see Appendix A for the list of observables.

CyOTE Capabilities for Technique Perception and Comprehension	
Artifacts **(See Appendix B)**	A total of 33 artifacts could be generated by the Network Connection Enumeration technique
Technique Observers	IT Staff, IT Cybersecurity, OT Cybersecurity

3.5. VALID ACCOUNTS TECHNIQUE (T0859) FOR LATERAL MOVEMENT

After the adversary discovered the internal hosts communicating over SQL network services, they checked for weak authentication methods. The pipeline operator's IT staff configured the SQL Server for authentication with default administrator privileges over MS SQL network service, TCP port 1434. The adversary logged on to the SQL server with administrator privileges that created successful logon Event ID 4624, as well as Event IDs 4648 and 4672. The user logon ID associated with the external IP host logs was first seen on 15 April 2008 (D-112) and last seen on 05 August (D-0).

IT Staff, IT Cybersecurity, OT Staff, and OT Cybersecurity personnel may have been able to observe the repeated use of special privileges to log on to the MS SQL server from an external IP.

A total of four observables were identified with the use of the Valid Accounts technique (T0859). This technique is important for investigation because the adversary gained access to many assets that share resources with the database server. This technique appears as the transition from the early to the middle stage of the attack and responding to it will deny the adversary access to the vulnerable RTU application on the EWS. Terminating the chain of techniques at this point would isolate the adversary from the OT systems connected to the database.

All four observables are assessed to be highly perceivable.

Please see Appendix A for the list of observables.

CyOTE Capabilities for Technique Perception and Comprehension	
Artifacts **(See Appendix B)**	A total of 16 artifacts could be generated by the Valid Accounts technique
Technique Observers	IT Staff, IT Cybersecurity, OT Staff, OT Cybersecurity

3.6. EXPLOIT PUBLIC FACING APPLICATION TECHNIQUE (T0819) FOR INITIAL ACCESS

The adversary exploited vulnerabilities within the control environment after gaining access to the shared SQL database that served as CCTV data storage and data historian for the 63 Schneider Electric RTUs along the pipeline. Vendor Citect SCADA reported on 11 June 2008 (D-55) that their control application had a vulnerability that would allow a publicly available Metasploit module to force an abnormal termination of the CitectSCADA software or remotely execute code over a SQL ODBC connection with Schneider Electric RTUs.[25] Cyber researchers reported CVE 2008-2639 to Citect's team on 30 January 2008 (D-188) and stated that the vulnerability could have existed for 6 years (Y-6).[26]

In this scenario, the adversary discovered the CitectSCADA application's abilities to provide remote SQL access. The SQL server ODBC component listened over TCP Port 20222 and the vulnerability in the CitectSCADA software allowed the adversary to cause intermittent Denial of Service (DoS) and remotely execute code on the EWS hosting the CitectSCADA application. The intermittent failures at block valve 30 reported from 5 February 2007 (D-547) until 5 August 2008 (D-0) suggest that the adversary could have exploited this vulnerability the entire time, but it is more likely the adversary exploited the vulnerability using the public Metasploit module from 16 June (D-50) until 5 August (D-0).

IT Cybersecurity, OT Cybersecurity, and Support Staff personnel may have been able to observe anomalous network traffic, vulnerability announcements, and intermittent application failures.

A total of five observables were identified with the use of the Exploit Public Facing Application technique (T0819). This technique is important for investigation because it provides both network and host-based evidence of adversarial behavior in both the IT and OT environments. This technique represents the initial access to the OT environment and responding to it will prevent adversarial behavior from impacting any control systems. Terminating the chain of techniques at this point would isolate adversarial behavior to the IT environment.

Of the five observables associated with this technique, four are assessed to be highly perceivable (Local EWS RTU Application Allows Anomalous Module to Execute Code (CVE 2008-2639); Inbound Network Connections Over TCP Port 20222 from External IP Host; Anomalous Code Executed Over MS SQL ODBC Port 20222 to Local EWS RTU Application from Remote External IP; Local EWS Application Intermittently Crashing).

Please see Appendix A for the list of observables.

CyOTE Capabilities for Technique Perception and Comprehension	
Artifacts **(See Appendix B)**	A total of 55 artifacts could be generated by the Exploit Public Facing Application technique
Technique Observers	IT Cybersecurity, OT Cybersecurity, Support Staff

3.7. DENIAL OF SERVICE TECHNIQUE (T0814) FOR INHIBIT RESPONSE FUNCTION

The adversary tested the capabilities of the vulnerability to cause intermittent DoS by executing the Metasploit module over TCP Port 20222.[27] This DoS caused the CitectSCADA application to crash. The module sent anomalous 400-byte strings of data over TCP Port 20222 to the identified EWS. The adversary executed this technique from a remote external host to the internal target Windows XP EWS using the CiExceptionMailer.dll. This caused an exception error on the EWS because the application buffer size is 376 bytes and the 400-byte strings resulted in a bad memory read. The adversary used this public exploit to test its ability to cause an impact to the EWS, likely first on 16 June 2008 (D-50) and last on 5 August (D-0)**.**

OT Staff, OT Cybersecurity, Engineering, and Support Staff personnel may have been able to observe the CitectSCADA application on the EWS intermittently crashing.

A total of six observables were identified with the use of the Denial of Service technique (T0814). This technique is important for investigation because the use of this technique creates the first impact on the OT control environment. This technique appears in the middle of the attack sequence and responding to it will preclude the existence of software-based problems, instead suggesting adversarial behavior in the OT environment. Terminating the chain of techniques at this point would disrupt further adversarial movement toward more sensitive control systems.

Of the six observables associated with this technique, five are assessed to be highly perceivable (Inbound Network Connections over TCP Port 20222 from External IP Host; Local EWS Application Intermittently Crashing; Local EWS Application Reports Exception Error Due to Bad Memory Read; Local EWS Application Receiving Calls from Anomalous .dll; Local EWS Application Receiving Calls from CiExceptionMailer.dll).

Please see Appendix A for the list of observables.

CyOTE Capabilities for Technique Perception and Comprehension	
Artifacts **(See Appendix B)**	A total of 14 artifacts could be generated by the Denial of Service technique
Technique Observers	OT Staff, OT Cybersecurity, Engineering, Support Staff

3.8. DATA FROM INFORMATION REPOSITORIES TECHNIQUE (T0811) FOR COLLECTION

The adversary began collecting credentials on the EWS to gain persistent access to the CitectSCADA application from an external host IP. A Metasploit module created a reverse command shell through the CVE 2008-2639 exploit over TCP Port 20222.[28] The adversary captured EWS host information and operator keystrokes during logons, enumerated all applications, and identified the full path to the RTU operators' CitectSCADA application account (Document and Settings/{USER}/Application Data/Citect/CitectSCADA7.1/).[29] This activity took place between 16 June (D-50) and 1 August 2008 (D-4).

IT Cybersecurity and OT Cybersecurity personnel may have been able to observe anomalous network connections to the EWS.

A total of two observables were identified with the use of the Data from Information Repositories technique (T0811). This technique is important for investigation because the adversary has not gained persistence on a device that controls an OT system. This technique appears in the middle stages of the attack and responding to it will deny the adversary continued access to devices that can manipulate the RTU settings. Terminating the chain of techniques at this point would deny the adversary the capability to cause catastrophic physical damage to the pipeline.

Of the two observables associated with this technique, one is assessed to be highly perceivable (Inbound Network Connections over TCP Port 20222 from External IP Host).

Please see Appendix A for the list of observables.

CyOTE Capabilities for Technique Perception and Comprehension	
Artifacts **(See Appendix B)**	A total of 35 artifacts could be generated by the Data from Information Repositories technique
Technique Observers	IT Staff, IT Cybersecurity, OT Staff, OT Cybersecurity, Support Staff

3.9. VALID ACCOUNTS TECHNIQUE (T0859) FOR PERSISTENCE

Once the adversary gathered the logon credentials of the RTU operators, the adversary was able to maintain access on the EWS. The adversary's logon sessions would create application events, Event ID 4624, and timestamps associated with a valid RTU operator's account. The adversary compromised the RTU operator's user account from 30 June (D-36) until 11:45 PM on 5 August 2008 (M+42).

IT Cybersecurity and OT Cybersecurity personnel may have been able to observe the use of the EWS RTU application at anomalous times.

A total of eight observables were identified with the use of the Valid Accounts technique (T0859). This technique is important for investigation because at this point the adversary can dwell within the OT environment with the RTU operators' credentials. The adversary can research how the RTU operator and the EWS RTU application function day to day. This technique appears in a transition from the middle stage to the late stage and responding to it will degrade the adversary's access to the EWS. Terminating the chain of techniques at this point would delay the adversary's progress but would require the victim organization to make significant configuration changes to prevent catastrophic damage.

Of the eight observables associated with this technique, one is assessed to be highly perceivable (Local Engineering Workstation (EWS) Successful Logon (Windows Event ID 4624) with Anomalous Timestamp Outside the User's Normal Working Hours).

Please see Appendix A for the list of observables.

CyOTE Capabilities for Technique Perception and Comprehension	
Artifacts (See Appendix B)	A total of 16 artifacts could be generated by the Valid Accounts technique
Technique Observers	IT Staff, IT Cybersecurity, OT Staff, OT Cybersecurity, Engineering, Support Staff

3.10. MODIFY ALARM SETTINGS TECHNIQUE (T0838) FOR INHIBIT RESPONSE FUNCTION

The adversary used the compromised RTU operator's account to modify alarm settings in the CitectSCADA application. This activity resulted in successful logon, application events, and anomalous timestamps associated with the RTU operator's user account. The RTU Operator's account executed two functions: AlarmDisable and AlarmDisableRec.[30] These function commands disable all alarms and remove all alarms from record. This activity took place on 1 August 2008 (D-4).

OT Staff, OT Cybersecurity, Engineering, and Support Staff personnel may have been able to observe the anomalous logon timestamps and modified alarm functions.

A total of 11 observables were identified with the use of the Modify Alarm Settings technique (T0838). This technique is important for investigation because the adversary can adjust the OT systems with valid credentials that will be difficult to detect. This technique appears late in the attack sequence and responding to it will temporarily delay the adversary's activity. Terminating the chain of techniques at this point would delay the adversary but would not prevent recurring impacts to the OT environment.

Of the 11 observables associated with this technique, four are assessed to be highly perceivable (Local EWS Successful Logon (Windows Event ID 4624) with Anomalous Timestamp Outside the User's Normal Working Hours; User Account Executes an Anomalous Function; RTU Operator User Account Anomalously Executes AlarmDisable Function on RTU Application; RTU Operator User Account Anomalously Executes AlarmDisableRec Function on RTU Application).

Please see Appendix A for the list of observables.

CyOTE Capabilities for Technique Perception and Comprehension	
Artifacts **(See Appendix B)**	A total of 16 artifacts could be generated by the Modify Alarm Settings technique
Technique Observers	OT Staff, OT Cybersecurity, Engineering, Support Staff

3.11. BLOCK REPORTING MESSAGE TECHNIQUE (T0804) FOR INHIBIT RESPONSE FUNCTION

The adversary modified the report parameters using the same EWS RTU operator's user account. The RTU operator's compromised account specified that the block 30 RTU client cluster would not connect to the EWS. The specific command within the EWS application was [Alarm.Block30cluster.Block30server]DisableConnection.[31] The RTU operator account executed this command on 1 August 2008 (D-4).

OT Staff, OT Cybersecurity, Engineering, and Support Staff personnel may have been able to observe the anomalous logon timestamps and modified reporting parameters.

A total of 11 observables were identified with the use of the Block Reporting Message technique (T0804). This technique is important for investigation because the adversary can adjust the OT system's configuration with valid credentials that will be difficult to detect. This technique appears late in the attack sequence and responding to it will temporarily delay the adversary's activity. Terminating the chain of techniques at this point would delay the adversary but would not prevent recurring impacts to the OT environment.

Of the 11 observables associated with this technique, three are assessed to be highly perceivable (Local EWS Successful Logon (Windows Event ID 4624) with Anomalous Timestamp Outside the User's Normal Working Hours; RTU Operator User Account Anomalously Disables Reporting Parameter for RTU from the RTU application; RTU Operator User Account Anomalously Disables Reporting Parameter for RTU from the RTU Application Using the [Alarm.Block30cluster.Block30server]DisableConnection Command).

Please see Appendix A for the list of observables.

CyOTE Capabilities for Technique Perception and Comprehension	
Artifacts **(See Appendix B)**	A total of 18 artifacts could be generated by the Block Reporting Message technique
Technique Observers	OT Staff, OT Cybersecurity, Engineering, Support Staff

3.12. UNAUTHORIZED COMMAND MESSAGE TECHNIQUE (T0855) FOR IMPAIR PROCESS CONTROL

The adversary used the compromised RTU Operator user account to log on to the EWS at 10:00 PM on 5 August (M-57), creating logon events and application log events with timestamps not normally associated with the operator's normal working hours. The adversary used the account to modify the block30runtime.ctz backup project file to run with block valve 30 in a sustained closed position.[32] The block30runtime.ctz project file anomalously executed the command for the RTU to close block valve 30. The EWS file metadata showed that the RTU operator user account modified the project file at 10:15 PM on 5 August (M-48).

OT Staff, OT Cybersecurity, and Engineering personnel may have been able to observe the logon events with anomalous timestamps.

A total of 12 observables were identified with the use of the Unauthorized Command Message technique (T0855). This technique is important for investigation because this modification would have been difficult to perceive given that it was a valid account executing a backup project file. This technique appears late in the attack and responding to it will temporarily delay the effects of the adversarial behavior. Terminating the chain of techniques at this point would deny the project file communication with the RTU but the adversary would still be able to make changes from the RTU application to cause an impact on the OT system.

Of the 12 observables associated with this technique, three are assessed to be highly perceivable (Local EWS Successful Logon (Windows Event ID 4624) with Anomalous Timestamp Outside the User's Normal Working Hours; RTU Operator User Account Modifies Run Time Project File from RTU Application; RTU Operator User Account Anomalously Executes Command for RTU to Close Valve).

Please see Appendix A for the list of observables.

CyOTE Capabilities for Technique Perception and Comprehension	
Artifacts (See Appendix B)	A total of 16 artifacts could be generated by the Unauthorized Command Message technique
Technique Observers	OT Staff, OT Cybersecurity, Engineering

3.13. MANIPULATION OF CONTROL TECHNIQUE (T0831) FOR IMPACT

The adversary remained logged in to the EWS to monitor the project file executing the command to close block valve 30. The block valve remained in the sustained closed position from 10:15 PM (M-48) until 11:53 PM on 5 August (M+50), causing an increase in flow pressure. The operators did not notice the change in flow pressure due to the modified alarm settings.

OT Staff, OT Cybersecurity, Engineering, and Support Staff personnel may have been able to observe the change in valve position at block valve 30, but the modified alarm settings impeded the operators' understanding of the true status of the pipeline.

A total of 11 observables were identified with the use of the Manipulation of Control technique (T0831). This technique is important for investigation because the adversary created an unstable state within the OT system, disabled the alarms, and blocked reporting messages from the block valve cluster. This technique appears late in the attack sequence and responding to it will delay the adversary's coordinated activities to cause catastrophic damage. Terminating the chain of techniques at this point would delay the damage to property but not prevent future adversarial attempts to create an impact.

Of the 11 observables associated with this technique, four are assessed to be highly perceivable (Local EWS Successful Logon (Windows Event ID 4624) with Anomalous Timestamp Outside the User's Normal Working Hours; RTU Operator User Account Anomalously Executes Command for RTU to Close Valve; RTU Operator User Account Anomalously Moves Valve to Closed Position; Anomalous Increase in Flow Pressure at Closed Valve Location).

Please see Appendix A for the list of observables.

CyOTE Capabilities for Technique Perception and Comprehension	
Artifacts **(See Appendix B)**	A total of 16 artifacts could be generated by the Manipulation of Control technique
Technique Observers	OT Staff, OT Cybersecurity, Engineering, Support Staff

3.14. ALARM SUPPRESION TECHNIQUE (T0878) FOR INHIBIT RESPONSE FUNCTION

The pressure at block valve 30 began to increase and the RTU's alarms were disabled.[33] The flow rate reporting messages from the RTU were not accurate from 10:15 PM (M-48) until 11:43 PM (M+40) on 5 August when people that live near block valve 30 notified the fire department and pipeline operators that there was a fire along highway E80.[34]

OT Staff, OT Cybersecurity, Engineering, and Support Staff personnel may have been able to observe inconsistencies in pipeline telemetry data.

A total of three observables were identified with the use of the Alarm Suppression technique (T0878). This technique is important for investigation because it enabled the adversary to coordinate both network-based and physical sabotage. This technique appears late in the attack sequence and responding to it will reduce the damage caused to physical property. Terminating the chain of techniques at this point would enable operators to monitor the state of the block valve but would not prevent the adversary from causing sustained damage.

Of the three observables associated with this technique, none are assessed to be highly perceivable.

Please see Appendix A for the list of observables.

CyOTE Capabilities for Technique Perception and Comprehension	
Artifacts **(See Appendix B)**	A total of 13 artifacts could be generated by the Alarm Suppression technique
Technique Observers	OT Staff, OT Cybersecurity, Engineering, Support Staff

3.15. DAMAGE TO PROPERTY TECHNIQUE (T0879) FOR IMPACT

The block valve began to leak between 10:45 (M-18) and 11:00 PM (M-3) on 5 August. The network-based adversary coordinated with a sabotage team on the ground that initiated the explosion at 11:03 PM (D-0). This resulted in catastrophic destruction of property at block valve 30 and a fire that burned until 9 August (D+4).[35,36]

OT Staff, OT Cybersecurity, Engineering, and Support Staff personnel may have been able to observe the explosion and fire.

A total of four observables were identified with the use of the Damage to Property technique (T0879). This technique is important for investigation because it is the triggering event for the recovery operations that took place. This technique appears late in the timeline and responding to it will enable the operator to recover from damages and understand the contributing causes. This technique is a consequence of the adversary behavior and operators can only limit additional damages at this point.

Of the six observables associated with this technique, five are assessed to be highly perceivable (Anomalous Explosion at Closed Block Valve Location; Anomalous Fire along Midstream Pipeline at Block Valve Location; Destroyed Remote Terminal Unit (RTU); Destroyed Block Valve; Damaged Midstream Pipeline).

Please see Appendix A for the list of observables.

CyOTE Capabilities for Technique Perception and Comprehension	
Artifacts **(See Appendix B)**	A total of 18 artifacts could be generated by the Damage to Property technique
Technique Observers	OT Staff, OT Cybersecurity, Engineering, Support Staff

3.16. DATA DESTRUCTION TECHNIQUE (T0809) FOR INHIBIT RESPONSE FUNCTION

The adversary logged on from an external IP to the MS SQL Server that stored camera footage and deleted 60 hours of footage from the Pelco IP-Based camera overlooking block valve 30.[37] The adversary deleted all file extensions with timestamps between 12:45 PM on 2 August (D-3) to 11:45 PM on 5 August (M+42), including evidence from the Recycle Bin. The adversary then successfully logged off the database server which created a log event at 11:50 PM on 5 August (M+50).

IT Staff, IT Cybersecurity and Support Staff personnel may have been able to observe the user account activity from an external IP and the anomalously missing video footage.

A total of 22 observables were identified with the use of the Data Destruction technique (T0809). This technique is important for investigation because it reveals the adversary's intentions to destroy evidence. This technique necessitates the unplanned restoration of data from backups and can result in unexpected expenses related to data recovery efforts. This technique appears late in the attack sequence and responding to it will support the contributing cause analysis. This technique appears after the triggering event but may assist pipeline operators and owners to comprehend the presence of adversarial behavior.

All 22 observables are assessed to be highly perceivable.

Please see Appendix A for the list of observables.

CyOTE Capabilities for Technique Perception and Comprehension	
Artifacts (See Appendix B)	A total of 27 artifacts could be generated by the Data Destruction technique
Technique Observers	IT Staff, IT Cybersecurity, Support Staff

3.17. LOSS OF SAFETY TECHNIQUE (T0880) FOR IMPACT

The operators experienced a loss of safety event due to the failure of the RTU to report and sound an alarm for the overpressure, rupture, and subsequent fire from 10:15 PM (M-48) to 11:43 PM (M+40) on 5 August. Operators returned the pipeline to a safe configuration at approximately 11:53 PM (M+50) by closing block valve 29 and 31 to isolate the damaged pipeline segment.[38]

OT Staff, OT Cybersecurity, Engineering, and Support Staff personnel may have been able to observe the misrepresentation of the state of the pipeline and the reported state.

A total of three observables were identified with the use of the Loss of Safety technique (T0880). This technique is important for investigation because it represents the adversary creating impacts that could put human lives in danger. This technique appears late in the attack sequence and responding to it will return the configuration to safe operations. There are no preventative measures for the operators at this stage of the attack.

Of the three observables associated with this technique, none are assessed to be highly perceivable.

Please see Appendix A for the list of observables.

CyOTE Capabilities for Technique Perception and Comprehension	
Artifacts **(See Appendix B)**	A total of 3 artifacts could be generated by the Loss of Safety technique
Technique Observers	OT Staff, OT Cybersecurity, Engineering, Support Staff

3.18. LOSS OF PRODUCTIVITY AND REVENUE TECHNIQUE (T0828) FOR IMPACT

The operating company initiated recovery operations at 11:53 PM on 5 August (M+50) and held a press conference to report the incident at 1:08 AM on 6 August (H+2).[39] The pipeline operators shut down the pipeline for repairs and did not return to normal operations until 25 August (D+20). The owners lost about 30,000 barrels of oil, $100 million in transit tariff fees, and $3 to $4 billion in export revenue.[40]

IT Staff, IT Cybersecurity, OT Staff, OT Cybersecurity, Engineering, Support Staff, and Management personnel may have been able to observe the many financial losses over the 20 days of recovery.

A total of four observables were identified with the use of the Loss of Productivity and Revenue technique (T0828). This technique is important for investigation because it reveals the financial exposure to cyber-physical adversary behavior. Additionally, this technique presents an impact for the end users or consumers of products and services, and responding to it will recover damages lost during the incident.

All four observables are assessed to be highly perceivable.

Please see Appendix A for the list of observables.

CyOTE Capabilities for Technique Perception and Comprehension	
Artifacts (See Appendix B)	A total of 5 artifacts could be generated by the Loss of Productivity and Revenue technique
Technique Observers	IT Staff, IT Cybersecurity, OT Staff, OT Cybersecurity, Engineering, Support Staff, Management

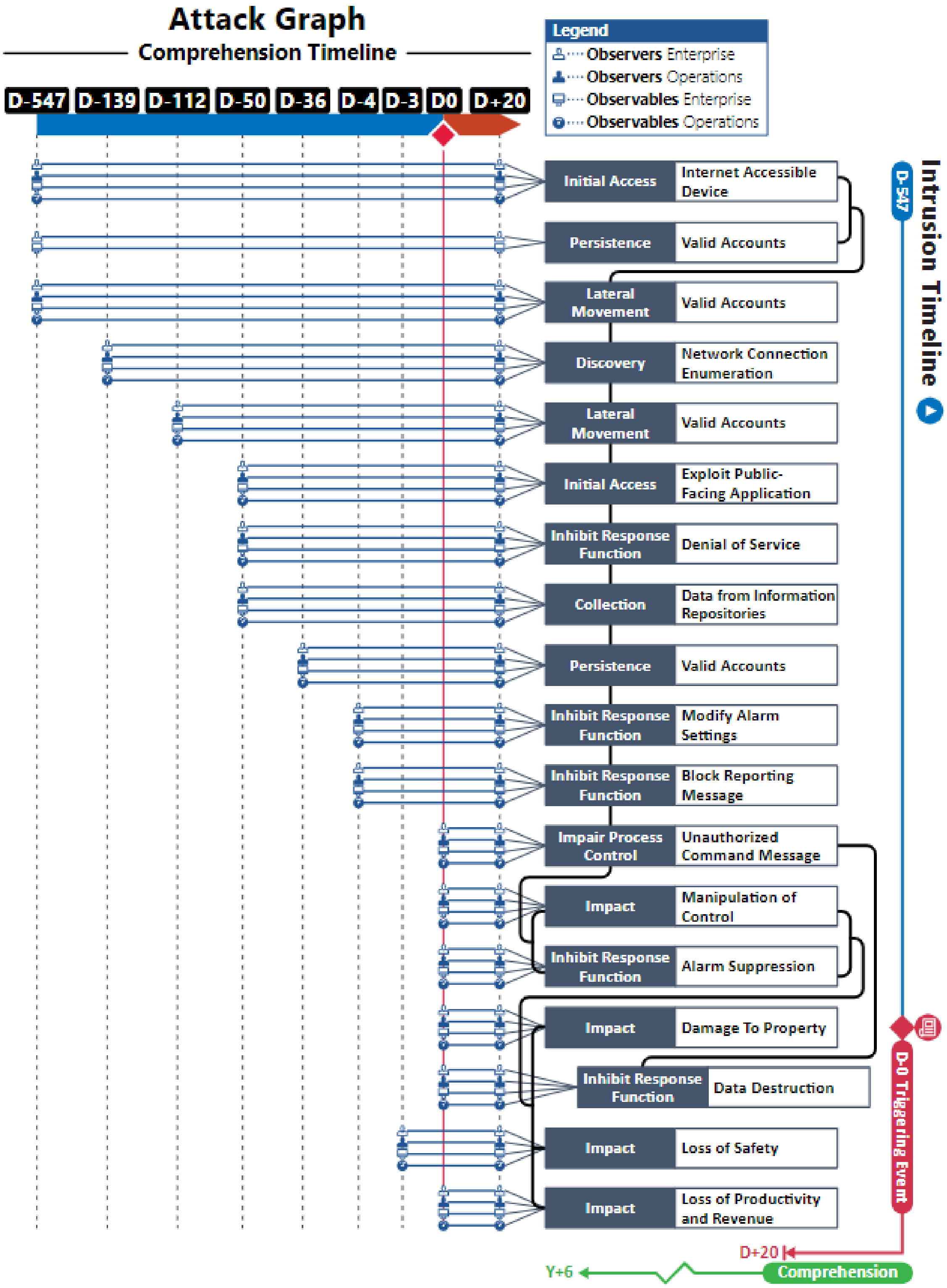


Figure 3. Attack Graph

APPENDIX A: OBSERVABLES LIBRARY

NOTE: Highly perceivable observables are highlighted in italics

Observables Associated with Internet Accessible Device Technique (T0883)	
Observable 1	*Inbound Real Time Streaming Protocol (RTSP) Network Traffic Over TCP Port 554 From Anomalous External IP Host*
Observable 2	*Network Session Created Over Real Time Streaming Protocol (RTSP) TCP Port 554 with Anomalous External IP Host*

Observables Associated with Valid Accounts Technique (T0859)	
Observable 1	Inbound Real Time Streaming Protocol (RTSP) Network Traffic Over TCP Port 554 From Anomalous External IP Host
Observable 2	Default Administrator Credentials Used to Logon to Devices with Public IP Address
Observable 3	*Successful Logon to Device with Public IP Address (Windows Event ID 4624)*
Observable 4	*Network Traffic Over RTSP TCP 554 POST Request Using Default Administrator Credentials with Logon from Anomalous External IP Host*
Observable 5	*Network Session Created Over RTSP TCP Port 554 with Anomalous External IP Host*

Observables Associated with Valid Accounts Technique (T0859)	
Observable 1	*User Successfully Logs On to Local IP-Based Security Camera from Anomalous External IP Host*
Observable 2	Local IP-Based Security Camera Successful Logon Event (Windows Log Event ID 4624)
Observable 3	Local IP-Based Security Camera Successful Logon with Explicit Credentials (Windows Log Event ID 4648)
Observable 4	*Local IP-Based Security Camera Special Privileged Assigned to New Logon (Windows Log Event ID 4672)*
Observable 5	*User Successfully Logs On to Local Security Camera Control Server from Anomalous External IP Host*
Observable 6	Local Camera Command Server Successful Logon Event (Windows Log Event ID 4624)
Observable 7	Local Camera Command Server Successful Logon with Explicit Credentials (Windows Log Event ID 4648)
Observable 8	*User Successfully Logs On to Local MS SQL Server Camera Storage Database from Anomalous External IP Host*
Observable 9	Local MS SQL Server Camera Storage Database Successful Logon Event (Windows Log Event ID 4624)
Observable 10	Local MS SQL Server Camera Storage Database Successful Logon with Explicit Credentials (Windows Log Event ID 4648)

Observables Associated with Valid Accounts Technique (T0859)	
Observable 11	*Local MS SQL Server Camera Storage Database Special Privileged Assigned to New Logon (Windows Log Event ID 4672)*

Observables Associated with Network Connection Enumeration Technique (T0840)	
Observable 1	*Valid User Account Logons to IP-Based Camera Control Server from Anomalous External Host IP*
Observable 2	Internal IP-Based Camera Control Server Makes Inbound Connection to MS SQL Server Over TCP Port 1433
Observable 3	Internal IP-Based Camera Control Server Makes Inbound Connection to MS SQL Server Over TCP Port 1434
Observable 4	Internal IP-Based Camera Control Server Makes Outbound Connection to 63 IP-Based Security Cameras Over TCP Port 554
Observable 5	*Valid User Account Logons to Internal Camera MS SQL Server from Anomalous External Host IP*
Observable 6	Internal MS SQL Server Makes Outbound Connections to 200 Internal Devices over TCP Port 1433
Observable 7	Internal MS SQL Server Makes Outbound Connections to Local Engineering Workstation (EWS) over TCP Port 1433
Observable 8	Internal MS SQL Server Makes Outbound Connection to 63 Remote Terminal Units (RTUs) over TCP Port 1433

Observables Associated with Valid Accounts Technique (T0859)	
Observable 1	*Valid User Account Logons to Internal Camera MS SQL Server from Anomalous External Host IP*
Observable 2	*Local MS SQL Server Camera Storage Database Successful Logon Event (Windows Log Event ID 4624)*
Observable 3	*Local MS SQL Server Camera Storage Database Successful Logon with Explicit Credentials (Windows Log Event ID 4648)*
Observable 4	*Local MS SQL Server Camera Storage Database Special Privileged Assigned to New Logon (Windows Log Event ID 4672)*

Observables Associated with Exploit Public-Facing Application Technique (T0819)	
Observable 1	*Local Engineering Workstation (EWS) Remote Terminal Unit (RTU) Application Allows Anomalous Module to Execute Code (CVE 2008-2639)*
Observable 2	*Inbound Network Connections Over TCP Port 20222 from External IP Host*
Observable 3	*Anomalous Code Executed Over MS SQL ODBC port 20222 to Local Engineering Workstation (EWS) Remote Terminal Unit (RTU) Application from Remote External IP*
Observable 4	Execution of 400-byte strings on the Local Engineering Workstation (EWS) from Remote External Host

Observables Associated with Exploit Public-Facing Application Technique (T0819)	
Observable 5	*Local Engineering Workstation (EWS) Application Intermittently Crashing*

Observables Associated with Denial of Service Technique (T0814)	
Observable 1	*Inbound Network Connections over TCP Port 20222 from External IP Host*
Observable 2	Execution of 400-byte strings on the Local Engineering Workstation (EWS) from Remote External Host
Observable 3	*Local Engineering Workstation (EWS) Application Intermittently Crashing*
Observable 4	*Local Engineering Workstation (EWS) Application Reports Exception Error Due to Bad Memory Read*
Observable 5	*Local Engineering Workstation (EWS) Application Receiving Calls from Anomalous (.dll)*
Observable 6	*Local Engineering Workstation (EWS) Application Receiving Calls from CiExceptionMailer.dll*

Observables Associated with Data from Information Repositories Technique (T0811)	
Observable 1	*Inbound Network Connections over TCP Port 20222 from External IP Host*
Observable 2	Reverse Shell Established between Local Engineering Workstation (EWS) and External IP Host

Observables Associated with Valid Accounts Technique (T0859)	
Observable 1	Local Engineering Workstation (EWS) Successful Logon (Windows Event ID 4624)
Observable 2	Local Engineering Workstation (EWS) Application Log Events
Observable 3	Local Engineering Workstation (EWS) CitectSCADA Log Events
Observable 4	CitectSCADA File-based Logs from (C:\ProgramData\SchneiderElectric\Citect_SCADA_2008\Logs)
Observable 5	CitectSCADA File-based Logs Changelog from (C:\ProgramData\SchneiderElectric\Citect_SCADA_2008\Logs)
Observable 6	CitectSCADA File-based Logs Syslog from (C:\ProgramData\SchneiderElectric\Citect_SCADA_2008\Logs)
Observable 7	CitectSCADA File-based Logs Tracelog from (C:\ProgramData\SchneiderElectric\Citect_SCADA_2008\Logs)
Observable 8	*Local Engineering Workstation (EWS) Successful Logon (Windows Event ID 4624) with Anomalous Timestamp Outside the User’s Normal Working Hours*

Observables Associated with Modify Alarm Settings Technique (T0838)	
Observable 1	Local Engineering Workstation (EWS) Successful Logon (Windows Event ID 4624)
Observable 2	Local Engineering Workstation (EWS) Application Log Events
Observable 3	Local Engineering Workstation (EWS) CitectSCADA Log Events
Observable 4	CitectSCADA File-based Logs from (C:\ProgramData\SchneiderElectric\Citect_SCADA_2008\Logs)
Observable 5	CitectSCADA File-based Logs Changelog from (C:\ProgramData\SchneiderElectric\Citect_SCADA_2008\Logs)
Observable 6	CitectSCADA File-based Logs Syslog from (C:\ProgramData\SchneiderElectric\Citect_SCADA_2008\Logs)
Observable 7	CitectSCADA File-based Logs Tracelog from (C:\ProgramData\SchneiderElectric\Citect_SCADA_2008\Logs)
Observable 8	*Local Engineering Workstation (EWS) Successful Logon (Windows Event ID 4624) with Anomalous Timestamp Outside the User's Normal Working Hours*
Observable 9	*User Account Executes an Anomalous Function*
Observable 10	*Remote Terminal Unit (RTU) Operator User Account Anomalously Executes AlarmDisable Function on Remote Terminal Unit (RTU) Application*
Observable 11	*Remote Terminal Unit (RTU) Operator User Account Anomalously Executes AlarmDisableRec Function on Remote Terminal Unit (RTU) Application*

Observables Associated with Block Reporting Message Technique (T0804)	
Observable 1	Local Engineering Workstation (EWS) Successful Logon (Windows Event ID 4624)
Observable 2	Local Engineering Workstation (EWS) Application Log Events
Observable 3	Local Engineering Workstation (EWS) CitectSCADA Log Events
Observable 4	CitectSCADA File-based Logs from (C:\ProgramData\SchneiderElectric\Citect_SCADA_2008\Logs)
Observable 5	CitectSCADA File-based Logs Changelog from (C:\ProgramData\SchneiderElectric\Citect_SCADA_2008\Logs)
Observable 6	CitectSCADA File-based Logs Syslog from (C:\ProgramData\SchneiderElectric\Citect_SCADA_2008\Logs)
Observable 7	CitectSCADA File-based Logs Tracelog from (C:\ProgramData\SchneiderElectric\Citect_SCADA_2008\Logs)
Observable 8	*Local Engineering Workstation (EWS) Successful Logon (Windows Event ID 4624) with Anomalous Timestamp Outside the User's Normal Working Hours*
Observable 9	User Account Anomalously Disables Reporting Parameter
Observable 10	*Remote Terminal Unit (RTU) Operator User Account Anomalously Disables Reporting Parameter for Remote Terminal Unit (RTU) from the Remote Terminal Unit (RTU) Application*

Observables Associated with Block Reporting Message Technique (T0804)	
Observable 11	*Remote Terminal Unit (RTU) Operator User Account Anomalously Disables Reporting Parameter for Remote Terminal Unit (RTU) From the Remote Terminal Unit (RTU) Application Using the '[Alarm.Block30cluster.Block30server]DisableConnection' Command*

Observables Associated with Unauthorized Command Message Technique (T0855)	
Observable 1	Local Engineering Workstation (EWS) Successful Logon (Windows Event ID 4624)
Observable 2	Local Engineering Workstation (EWS) Application Log Events
Observable 3	Local Engineering Workstation (EWS) CitectSCADA Log Events
Observable 4	CitectSCADA File-based Logs from (C:\ProgramData\SchneiderElectric\Citect_SCADA_2008\Logs)
Observable 5	CitectSCADA File-based Logs Changelog from (C:\ProgramData\SchneiderElectric\Citect_SCADA_2008\Logs)
Observable 6	CitectSCADA File-based Logs Syslog from (C:\ProgramData\SchneiderElectric\Citect_SCADA_2008\Logs)
Observable 7	CitectSCADA File-based Logs Tracelog from (C:\ProgramData\SchneiderElectric\Citect_SCADA_2008\Logs)
Observable 8	*Local Engineering Workstation Engineering Workstation (EWS) Successful Logon (Windows Event ID 4624) with Anomalous Timestamp Outside the User's Normal Working Hours*
Observable 9	User Account Anomalously Modifies Project File on Local Engineering Workstation Engineering Workstation (EWS)
Observable 10	*Remote Terminal Unit (RTU) Operator User Account Anomalously Modifies Run Time Project File from Remote Terminal Unit (RTU) Application*
Observable 11	Remote Terminal Unit (RTU) Operator User Account Anomalously Modifies block30runtime.ctz to Execute with Block Valve Moved to Sustained Closed Position
Observable 12	*Remote Terminal Unit (RTU) Operator User Account Anomalously Executes Command for Remote Terminal Unit (RTU) to Close Valve*

Observables Associated with Manipulation of Control Technique (T0831)	
Observable 1	Local Engineering Workstation (EWS) Successful Logon (Windows Event ID 4624)
Observable 2	Local Engineering Workstation (EWS) Application Log Events
Observable 3	Local Engineering Workstation (EWS) CitectSCADA Log Events
Observable 4	CitectSCADA File-based Logs from (C:\ProgramData\SchneiderElectric\Citect_SCADA_2008\Logs)

Observables Associated with Manipulation of Control Technique (T0831)	
Observable 5	CitectSCADA File-based Logs Changelog from (C:\ProgramData\SchneiderElectric\Citect_SCADA_2008\Logs)
Observable 6	CitectSCADA File-based Logs Syslog from (C:\ProgramData\SchneiderElectric\Citect_SCADA_2008\Logs)
Observable 7	CitectSCADA File-based Logs Tracelog from (C:\ProgramData\SchneiderElectric\Citect_SCADA_2008\Logs)
Observable 8	*Local Engineering Workstation (EWS) Successful Logon (Windows Event ID 4624) with Anomalous Timestamp Outside the User's Normal Working Hours*
Observable 9	*Remote Terminal Unit (RTU) Operator User Account Anomalously Executes Command for Remote Terminal Unit (RTU) to Close Valve*
Observable 10	*Remote Terminal Unit (RTU) Operator User Account Anomalously Moves Valve to Closed Position*
Observable 11	*Anomalous Increase in Flow Pressure at Closed Valve Location*

Observables Associated with Alarm Suppression Technique (T0878)	
Observable 1	Anomalous Increase in Flow Pressure at Closed Valve Location
Observable 2	Remote Terminal Unit (RTU) Application Anomalously Muted Alarms from Remote Terminal Unit (RTU)
Observable 3	Remote Terminal Unit (RTU) Application Anomalously Failed to Report Messages from Remote Terminal Unit (RTU)

Observables Associated with Damage to Property Technique (T0879)	
Observable 1	Anomalous Leak at Closed Block Valve Location
Observable 2	*Anomalous Explosion at Closed Block Valve Location*
Observable 3	*Anomalous Fire along Midstream Pipeline at Block Valve Location*
Observable 4	*Destroyed Remote Terminal Unit (RTU)*
Observable 5	*Destroyed Block Valve*
Observable 6	*Damaged Midstream Pipeline*

Observables Associated with Data Destruction Technique (T0809)	
Observable 1	*Valid User Account Logon to Internal Camera MS SQL Server from Anomalous External Host IP*
Observable 2	*Local MS SQL Server Camera Storage Database Successful Logon Event (Windows Log Event ID 4624)*
Observable 3	*Local MS SQL Server Camera Storage Database Successful Logon with Explicit Credentials (Windows Log Event ID 4648)*
Observable 4	*Local MS SQL Server Camera Storage Database Special Privileged Assigned to New Logon (Windows Log Event ID 4672)*

Observables Associated with Data Destruction Technique (T0809)	
Observable 5	*Valid User Account Anomalously Deletes an Hour of Camera Footage*
Observable 6	*Anomalously Missing Files with Extensions Associated with Pelco Camera from Database*
Observable 7	*Anomalously Missing Files with Extension Associated with Pelco Camera from Database (.avi)*
Observable 8	*Anomalously Missing Files with Extension Associated with Pelco Camera from Database (.asf)*
Observable 9	*Anomalously Missing Files with Extension Associated with Pelco Camera from Database (.pns)*
Observable 10	*Anomalously Missing Files with Extension Associated with Pelco Camera from Database (.bmp)*
Observable 11	*Anomalously Missing Files with Extension Associated with Pelco Camera from Database (.jpeg)*
Observable 12	*Anomalously Missing Files with Extension Associated with Pelco Camera from Database (.tif)*
Observable 13	*Anomalously Missing Files with Extension Associated with Pelco Camera from Database (.pev)*
Observable 14	*Anomalously Missing Files with Extension Associated with Pelco Camera from Database (.pck)*
Observable 15	*Anomalously Missing Files with Extension Associated with Pelco Camera from Database (.pix)*
Observable 16	*Anomalously Missing Files with Extensions Associated with Pelco Camera from Database Backup Folder*
Observable 17	*Anomalously Missing Files with Extension Associated with Pelco Camera from Database (.pev)*
Observable 18	*Anomalously Missing Files with Extension Associated with Pelco Camera from Database (.pck)*
Observable 19	*Anomalously Missing Files with Extension Associated with Pelco Camera from Database (.pix)*
Observable 20	*User Account Anomalously Empties Recycle Bin*
Observable 21	*User Account Initiated Logoff (Windows Event ID 4647)*
Observable 22	*User Account Successfully Logged Off (Windows Event ID 4634)*

Observables Associated with Loss of Safety Technique (T0880)	
Observable 1	Anomalous Failure of Remote Terminal Unit (RTU) Application to Alert Operators of Overpressure for approximately 30 minutes
Observable 2	Anomalous Failure of Remote Terminal Unit (RTU) Application to Alert Operators of Rupture at Valve Location
Observable 3	Anomalous Failure of Remote Terminal Unit (RTU) Application to Alert Operators of Explosion for 40 minutes

Observables Associated with Loss of Productivity and Revenue Technique (T0828)	
Observable 1	*Pipeline Anomalously Shut Down for Repairs for 20 days*
Observable 2	*Anomalous Loss of 30,000 Barrels of Oil*
Observable 3	*Anomalous Loss of $5 Million a Day in Transit Tariff Fees for 20 Days*
Observable 4	*Anomalous Loss of $3 to $4 Billion in Export Revenue Over 20 Days*

APPENDIX B: ARTIFACTS LIBRARY

Artifacts Associated with Internet Accessible Device Technique (T0883)	
Artifact 1	Host Registry Entries
Artifact 2	HTTPS Traffic
Artifact 3	Suspicious Connections in Proxy Logs
Artifact 4	Timestamps
Artifact 5	VPN Logoff Events
Artifact 6	Suspicious Connections in Firewall Logs
Artifact 7	VPN Logon Events
Artifact 8	SAP Traffic
Artifact 9	Host Registry Entries HKEY_LOCAL_MACHINE\SYSTEM
Artifact 10	SQL Traffic
Artifact 11	Host Information in External Data Store or Website (SHODAN)
Artifact 12	HTTP 80
Artifact 13	VNC Traffic Port 5800 or
Artifact 14	Dialog Boxes Opened on HMI or
Artifact 15	Application Authentication Events
Artifact 16	Internet Address in Memory Socket Data
Artifact 17	Remote Logins in OS Logs (Windows Event)
Artifact 18	Operational Database Connection to External Addresses
Artifact 19	Industrial Traffic from Internet Address
Artifact 20	Standard Traffic from Internet Address
Artifact 21	Internet Address in Application Logs
Artifact 22	Internet Address in OS Logs
Artifact 23	Internet Address in Command Line Record Data (netstat)

Artifacts Associated with Valid Accounts Technique (T0859)	
Artifact 1	Logon Session Creation
Artifact 2	User Account Creation
Artifact 3	Logon Type Entry
Artifact 4	Logon Timestamp
Artifact 5	Failed Logon Event
Artifact 6	Successful Logon Event
Artifact 7	System Logs
Artifact 8	Default Credential Use

Artifacts Associated with Valid Accounts Technique (T0859)	
Artifact 9	Authentication Creation
Artifact 10	Prefetch Files Created After Execution
Artifact 11	Logons
Artifact 12	Application Log
Artifact 13	Domain Permission Requests
Artifact 14	Permission Elevation Requests
Artifact 15	Application Use Times
Artifact 16	Configuration Changes

Artifacts Associated with Network Connection Enumeration Technique (T0840)	
Artifact 1	Device Failure
Artifact 2	Protocol Header Enumeration
Artifact 3	Protocol Content Enumeration
Artifact 4	Sequential Protocol SYN Traffic
Artifact 5	Statistical Anomalies in Network Traffic
Artifact 6	Echo Port 8 Traffic
Artifact 7	DNS Port 53 Zone Transfers
Artifact 8	Device Reboot
Artifact 9	Bandwidth Degradation
Artifact 10	Host Recent Connection Logs
Artifact 11	ICMP Port 7 Traffic
Artifact 12	SNMP Port 162 Traffic
Artifact 13	SNMP Port 161 Traffic
Artifact 14	Command Line Dialog Box Open
Artifact 15	VNC Port 5900 Calls
Artifact 16	Operating System Queries
Artifact 17	Email Server Calls
Artifact 18	Recurring Protocol SYN Traffic
Artifact 19	TCP ACK Scan
Artifact 20	Common Network Traffic
Artifact 21	Polling Network Traffic from Abnormal IP Sender Addresses
Artifact 22	NETBIOS Name Services Port
Artifact 23	Active Directory Calls
Artifact 24	SMTP Port 25 Traffic

Artifacts Associated with Network Connection Enumeration Technique (T0840)	
Artifact 25	DNS Lookup Queries
Artifact 26	ARP Scans
Artifact 27	TCP Connect Scan
Artifact 28	TCP SYN Scans
Artifact 29	Industrial Network Traffic
Artifact 30	TCP FIN Scans
Artifact 31	TCP Reverse Ident Scan
Artifact 32	TCP XMAS Scan
Artifact 33	LDAP Port

Artifacts Associated with Exploit Public-Facing Application (T0819)	
Artifact 1	Logon Security Event
Artifact 2	Logon Timestamp
Artifact 3	Process Failure
Artifact 4	Process State Change
Artifact 5	Operational Data Modification
Artifact 6	Operational Data Corruption
Artifact 7	OPC COM Objects
Artifact 8	Remote Connections
Artifact 9	External Network Connections
Artifact 10	Logon Event
Artifact 11	Prefetch
Artifact 12	Logon Event
Artifact 13	Administrator Logon
Artifact 14	External Network Connections
Artifact 15	Remote Connections
Artifact 16	Ransom Note
Artifact 17	Logon Timestamp After Hours
Artifact 18	MAC Address
Artifact 19	IP Address
Artifact 20	Process Ending
Artifact 21	HTTP Traffic Port
Artifact 22	External Industrial Protocol Connections
Artifact 23	Web Server Log

Artifacts Associated with Exploit Public-Facing Application (T0819)	
Artifact 24	VNC Traffic Port
Artifact 25	SSH Traffic Port
Artifact 26	Logon Security Event
Artifact 27	Telnet Traffic
Artifact 28	Increase Number of Logon Attempts
Artifact 29	TFTP Port
Artifact 30	FTP Port
Artifact 31	Application Failure
Artifact 32	HTTPS Port
Artifact 33	User Account
Artifact 34	Web Proxy Logs
Artifact 35	Application Log
Artifact 36	Process Creation
Artifact 37	Process Ending
Artifact 38	Source IP Address
Artifact 39	MAC Address
Artifact 40	Firewall Logs
Artifact 41	TLS Certificate
Artifact 42	.lnk Files
Artifact 43	FTPS Port
Artifact 44	Logon Alert for Default Password
Artifact 45	Process Creation
Artifact 46	Vendor Jump Host Logon
Artifact 47	Configuration Alert for Default Password
Artifact 48	Remote Connections
Artifact 49	RDP Traffic Port
Artifact 50	VNC Traffic Port
Artifact 51	SSH Traffic Port
Artifact 52	Telnet Traffic
Artifact 53	HTTP Traffic
Artifact 54	Application Log
Artifact 55	RDP Traffic Port

Artifacts Associated with Denial of Service Technique (T0814)	
Artifact 1	MAC Addresses
Artifact 2	ICMP Echo Port 7 Traffic Increase
Artifact 3	Application Failure
Artifact 4	Operational Data Corruption
Artifact 5	Application Log
Artifact 6	External Network Connections
Artifact 7	IP Addresses
Artifact 8	Network Traffic Connection Increase
Artifact 9	Services Failure
Artifact 10	Ransom Notice
Artifact 11	Low Resources Warning
Artifact 12	Increase Industrial Protocol Exceptions
Artifact 13	TDS Traffic Increase Port
Artifact 14	Process Performance Degrades

Artifacts Associated with Data from Information Repositories Technique (T0811)	
Artifact 1	SFTP Traffic Port
Artifact 2	Share Drive Access
Artifact 3	Operational Database Logons
Artifact 4	Engineering Workstation Application Log
Artifact 5	HTTP Traffic Port
Artifact 6	HTTPS Traffic Port
Artifact 7	FTPS Traffic Port
Artifact 8	File Access
Artifact 9	Telnet Traffic Port
Artifact 10	File Modification
Artifact 11	FTP Traffic Port
Artifact 12	VNC Traffic Port
Artifact 13	RDP Traffic Port
Artifact 14	Authentication Success
Artifact 15	Authentication Attempts
Artifact 16	MSSQL Traffic
Artifact 17	Traffic Timestamps
Artifact 18	SMB Traffic

Artifacts Associated with Data from Information Repositories Technique (T0811)	
Artifact 19	Project File Modification
Artifact 20	Data Bytes Sent
Artifact 21	User Session Creation
Artifact 22	Application Logon
Artifact 23	TDS Port
Artifact 24	Operational Database Data Modification
Artifact 25	Design Documentation Manipulation
Artifact 26	Authentication Failure
Artifact 27	Personnel List Files Accessed
Artifact 28	Jump Host Credentials Accessed
Artifact 29	Vendor Documentation Accessed
Artifact 30	Remote Procedure Calls
Artifact 31	Recent Search List
Artifact 32	MRU List Change
Artifact 33	Design Documentation Access
Artifact 34	Database Request
Artifact 35	SSH Traffic Port

Artifacts Associated with Modify Alarm Settings Technique (T0838)	
Artifact 1	User Logs
Artifact 2	Network Traffic
Artifact 3	Mismatch Between System Status and Physical Process
Artifact 4	Alarm Failures
Artifact 5	Alert Failures
Artifact 6	Application Logs
Artifact 7	Dialog Box Creation
Artifact 8	Configuration Changes
Artifact 9	False Positive Reporting
Artifact 10	System Operating Outside of Parameters
Artifact 11	Increase In Vendor Support Sessions
Artifact 12	Increase In Maintenance Reports
Artifact 13	Device Failure
Artifact 14	False Negative Reporting
Artifact 15	Dangerous Physical Changes

Artifacts Associated with Modify Alarm Settings Technique (T0838)	
Artifact 16	Operational Data Performance Degradation

Artifacts Associated with Block Reporting Message Technique (T0804)	
Artifact 1	Application Log Event Absent
Artifact 2	Application Modification
Artifact 3	Physical Process Changes Without Data Received
Artifact 4	Conflicting Device Status Reports
Artifact 5	Delayed Operational Process Status Change
Artifact 6	Operational Database Data Modification
Artifact 7	Historian Database Missing Data
Artifact 8	I/O Server Nonresponsive
Artifact 9	Real-Time Operational Data Missing
Artifact 10	Supervisory Application Logs Mismatch Current State
Artifact 11	Process Status Modification
Artifact 12	Network Traffic Changes
Artifact 13	Network Connections Creation
Artifact 14	Operational Device Failure
Artifact 15	Operational Database Configuration Change
Artifact 16	Operational Process Alarm Failures
Artifact 17	I/O Values Mismatched with Process Current State
Artifact 18	Operational Process Termination

Artifacts Associated with Unauthorized Command Message Technique (T0855)	
Artifact 1	MAC Addresses
Artifact 2	Application Level I/O Manipulation
Artifact 3	Process Alarm Event
Artifact 4	Process Alarm
Artifact 5	Operational Data Created
Artifact 6	OS Level I/O Manipulation
Artifact 7	IP Addresses
Artifact 8	Operational Application Log
Artifact 9	Process Logic Change
Artifact 10	Protocol Specific Command Packet
Artifact 11	Machine State Change

Artifacts Associated with Unauthorized Command Message Technique (T0855)	
Artifact 12	Process Restart
Artifact 13	Process Failure
Artifact 14	Network Resets
Artifact 15	Protocol Metadata Change
Artifact 16	Process Timing Change

Artifacts Associated with Manipulation of Control Technique (T0831)	
Artifact 1	Controller Set Point Change
Artifact 2	Event Log Creation
Artifact 3	Process Restart
Artifact 4	Process Shutdown
Artifact 5	Process State Change
Artifact 6	Process Initiated
Artifact 7	Controller Tag Change
Artifact 8	Controller Parameter Change
Artifact 9	I/O Modification
Artifact 10	Operational Data Modification
Artifact 11	Application File Modification
Artifact 12	Application Log Event
Artifact 13	Command Execution
Artifact 14	HMI Input Manipulation
Artifact 15	Altered Command Sequences
Artifact 16	Engineering Workstation Mouse Movement

Artifacts Associated with Alarm Suppression Technique (T0878)	
Artifact 1	Change In Process Output
Artifact 2	Modification of Alarm Set Points
Artifact 3	Runaway Process State
Artifact 4	Catastrophic Failures
Artifact 5	Configuration Change Logs
Artifact 6	Increased Number of Output Quality Assurance Failures
Artifact 7	Insertion of Malicious Industrial Protocol to Suppress True Process Values
Artifact 8	Modification of SQL Database Inputs
Artifact 9	SQL Protocol Network Traffic

Artifacts Associated with Alarm Suppression Technique (T0878)	
Artifact 10	Mismatch Between Sensor Reporting and Physical Process
Artifact 11	Increased Maintenance Issues
Artifact 12	Control System Degradation
Artifact 13	External Connection to Operational Database

Artifacts Associated with Damage to Property Technique (T0879)	
Artifact 1	Pressure Relief
Artifact 2	Reduction In Traffic Volume to Device
Artifact 3	Frequent Maintenance Failures
Artifact 4	Damage to Property Due to Equipment Degradation
Artifact 5	Damage to Property Due to Malicious Network Traffic
Artifact 6	Breakers Closing and Opening Rapidly
Artifact 7	Safety Systems Engaged
Artifact 8	Increase In Connecting Errors to Device
Artifact 9	Loud Vibrations
Artifact 10	Liquid Spills
Artifact 11	Damage to Property Due to Equipment Malfunction
Artifact 12	Catastrophic Failure
Artifact 13	Surges In Power
Artifact 14	Ladder Logic Configuration Changes
Artifact 15	Industrial Network Traffic
Artifact 16	Smoke
Artifact 17	Process Trip
Artifact 18	Alarms

Artifacts Associated with Data Destruction Technique (T0809)	
Artifact 1	Command Line Arguments
Artifact 2	Files Moved to Recycle Bin
Artifact 3	Missing Files
Artifact 4	Host System Reboot Failure
Artifact 5	Process Logic Failure
Artifact 6	Event Log Creation
Artifact 7	System Call
Artifact 8	System Application Interruption

Artifacts Associated with Data Destruction Technique (T0809)	
Artifact 9	Device Failure
Artifact 10	Recovery Attempt Failure
Artifact 11	TFTP Port
Artifact 12	SFTP Port
Artifact 13	Memory Corruption
Artifact 14	Use of File Transfer Protocols
Artifact 15	SCP Port
Artifact 16	File Encryptions
Artifact 17	Non-Native Files
Artifact 18	External Network Connections
Artifact 19	Transient Device Connections
Artifact 20	Program Execution
Artifact 21	Telnet Port
Artifact 22	FTPS Port
Artifact 23	HTTP Port
Artifact 24	HTTPS Port
Artifact 25	Local Network Connections
Artifact 26	FTP Port
Artifact 27	SMB Port

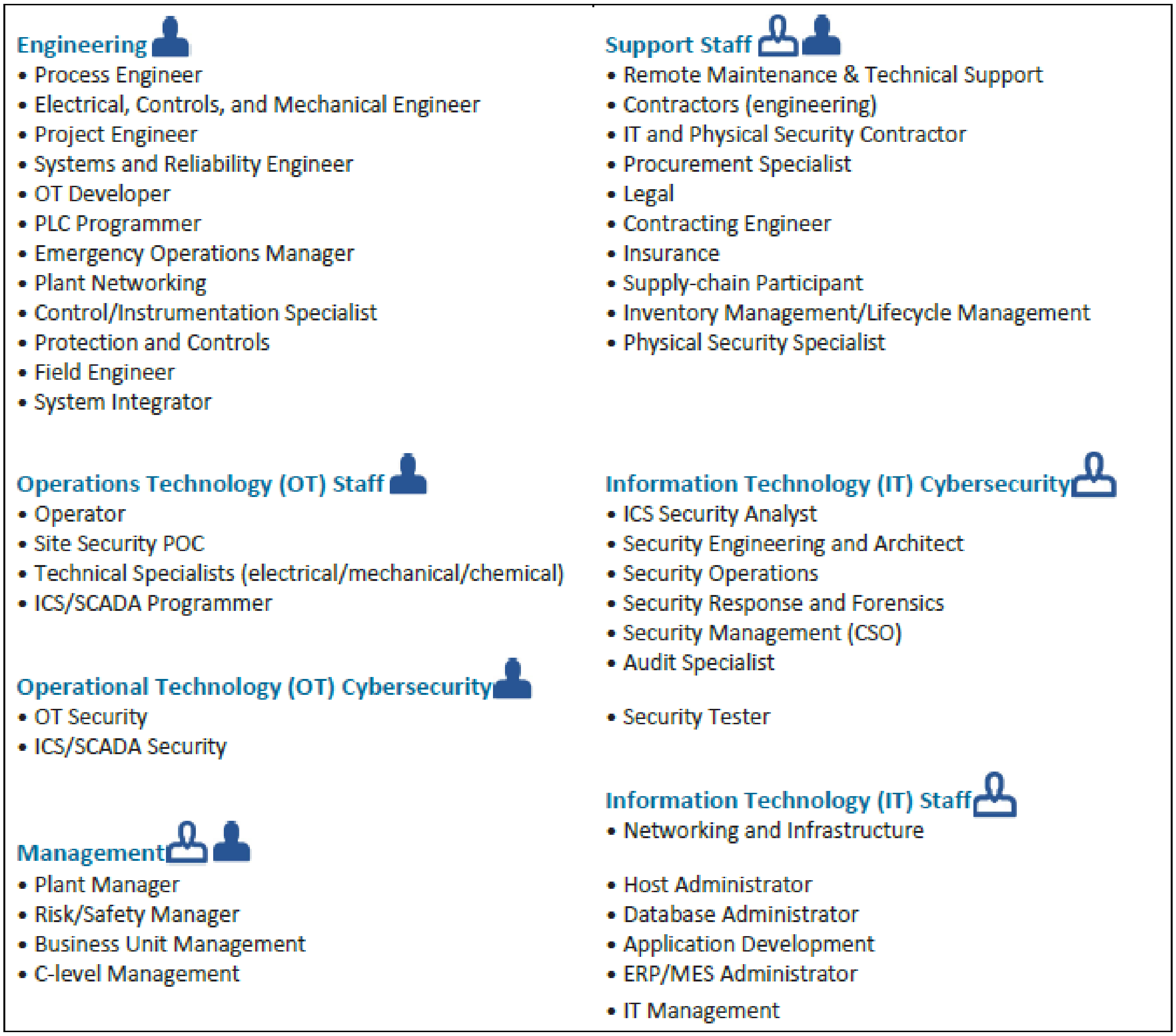
Artifacts Associated with Loss of Safety Technique (T0880)	
Artifact 1	Malicious Firmware Update to a Safety System
Artifact 2	Loss of Control of a Safety System
Artifact 3	Loss of Access to a Safety System

Artifacts Associated with Loss of Productivity and Revenue Technique (T0828)	
Artifact 1	Loss of Confidence in a Safety System Due to Unreliability Might Result in a Risk Management Driven Shutdown of a Plant
Artifact 2	Wormable or Other Highly Propagating Malware Might Result in The Shutdown of a Plant to Prevent Ransomware or Other Destructive Attacks
Artifact 3	Extortion Attempts Might Lead to Reduced Operations Due to Potential Presence of Malicious Attackers
Artifact 4	Loss of Control of Critical Systems Due to Ransomware or Loss of Confidence Might Lead to a Degraded Productivity or Revenue Operating State

Artifacts Associated with Loss of Productivity and Revenue Technique (T0828)	
Artifact 5	File System Modification Artifacts Might Be Associated with The Loss of Productivity and Revenue Attack Might Be Present on Disk

APPENDIX C: OBSERVERS

This is a collection of standardized potential observers that work in operational technology organizations. It has been slightly modified by the CyOTE team from the Job Role Groupings listed in the SANS ICS Job Role to Competency Level Poster to communicate the categories of potential observers during cyber events.



Engineering

- Process Engineer
- Electrical, Controls, and Mechanical Engineer
- Project Engineer
- Systems and Reliability Engineer
- OT Developer
- PLC Programmer
- Emergency Operations Manager
- Plant Networking
- Control/Instrumentation Specialist
- Protection and Controls
- Field Engineer
- System Integrator

Operations Technology (OT) Staff

- Operator
- Site Security POC
- Technical Specialists (electrical/mechanical/chemical)
- ICS/SCADA Programmer

Operational Technology (OT) Cybersecurity

- OT Security
- ICS/SCADA Security

Management

- Plant Manager
- Risk/Safety Manager
- Business Unit Management
- C-level Management

Support Staff

- Remote Maintenance & Technical Support
- Contractors (engineering)
- IT and Physical Security Contractor
- Procurement Specialist
- Legal
- Contracting Engineer
- Insurance
- Supply-chain Participant
- Inventory Management/Lifecycle Management
- Physical Security Specialist

Information Technology (IT) Cybersecurity

- ICS Security Analyst
- Security Engineering and Architect
- Security Operations
- Security Response and Forensics
- Security Management (CSO)
- Audit Specialist
- Security Tester

Information Technology (IT) Staff

- Networking and Infrastructure
- Host Administrator
- Database Administrator
- Application Development
- ERP/MES Administrator
- IT Management

REFERENCES

[1] [Bloomberg | Jordan Robertson and Michael Riley | “Mysterious ’08 Turkey Pipeline Blast Opened New Cyberwar” | https://www.bloomberg.com/news/articles/2014-12-10/mysterious-08-turkey-pipeline-blast-opened-new-cyberwar | 10 December 2014 | Accessed on 15 August 2022 | The source is publicly available information and does not contain classification markings]

[2] [The Sydney Morning Herald | Jordan Robertson and Michael Riley | “Before Stuxnet, Refahiye pipeline blast in Turkey opened new cyberwar era” | https://www.smh.com.au/world/before-stuxnet-refahiye-pipeline-blast-in-turkey-opened-new-cyberwar-era-20141212-125nvy.html | 12 December 2014 | Accessed on 15 August 2022 | The source is publicly available information and does not contain classification markings]

[3] [Verso Books | James Marriott and Mike Minio-Puello | “The Oil Road: Journeys from The Caspian Sea to The City of London” | Chapter 14, pp 207-211 | 10 September 2013 | London, UK | Accessed on 17 August 2022 | The source is publicly available information and does not contain classification markings]

[4] [Bloomberg | Jordan Robertson and Michael Riley | “Mysterious ’08 Turkey Pipeline Blast Opened New Cyberwar” | https://www.bloomberg.com/news/articles/2014-12-10/mysterious-08-turkey-pipeline-blast-opened-new-cyberwar#xj4y7vzkg | 10 December 2014 | Accessed on 6 June 2022 | The source is publicly available information and does not contain classification markings]

[5] [Verso Books | James Marriott and Mike Minio-Puello | “The Oil Road: Journeys from The Caspian Sea to The City of London” | Chapter 14, pp 207-211 | 10 September 2013 | London, UK | Accessed on 17 August 2022 | The source is publicly available information and does not contain classification markings]

[6] [Reuters | Orhan Coskun and Lada Yevgrashina | “Blast halts Azeri oil pipeline through Turkey” | https://www.reuters.com/article/us-turkey-pipeline-explosion/blast-halts-azeri-oil-pipeline-through-turkey-idUSSP31722720080806 | 5 August 2008 | Accessed on 17 August 2022 | The source is publicly available information and does not contain classification markings]

[7] [Bloomberg | Jordan Robertson and Michael Riley | “Mysterious ’08 Turkey Pipeline Blast Opened New Cyberwar” | https://www.bloomberg.com/news/articles/2014-12-10/mysterious-08-turkey-pipeline-blast-opened-new-cyberwar#xj4y7vzkg | 10 December 2014 | Accessed on 6 June 2022 | The source is publicly available information and does not contain classification markings]

[8] [Hurriyet | Hurriyet Staff | “Baku-Tbilisi-Ceyhan oil pipeline back to normal operations, BP says” | https://www.hurriyet.com.tr/gundem/baku-tbilisi-ceyhan-oil-pipeline-back-to-normal-operations-bp-says-9741262 | 25 August 2008 | Accessed on 17 August 2022 | The source is publicly available information and does not contain classification markings]

[9] [Verso Books | James Marriott and Mike Minio-Puello | “The Oil Road: Journeys from The Caspian Sea to The City of London” | Chapter 14, pp 207-211 | 10 September 2013 | London, UK | Accessed on 17 August 2022 | The source is publicly available information and does not contain classification markings]

[10] [Bloomberg | Jordan Robertson and Michael Riley | “Mysterious ’08 Turkey Pipeline Blast Opened New Cyberwar” | https://www.bloomberg.com/news/articles/2014-12-10/mysterious-08-turkey-pipeline-blast-opened-new-cyberwar#xj4y7vzkg | 10 December 2014 | Accessed on 6 June 2022 | The source is publicly available information and does not contain classification markings]

[11] [Bloomberg | Jordan Robertson and Michael Riley | “Mysterious ’08 Turkey Pipeline Blast Opened New Cyberwar” | https://www.bloomberg.com/news/articles/2014-12-10/mysterious-08-turkey-pipeline-blast-opened-new-cyberwar#xj4y7vzkg | 10 December 2014 | Accessed on 6 June 2022 | The source is publicly available information and does not contain classification markings]

[12] [Microsoft | “netstat” | https://learn.microsoft.com/en-us/windows-server/administration/windows-commands/netstat | 29 July 2021 | Accessed on 15 August 2022 | The source is publicly available information and does not contain classification markings]

[13] [CitectSCADA | Schneider Electric | “CitectSCADA User Guide | https://www.koningenhartman.nl/UserFiles/Product/Datasheet/CitectSCADA%20User%20Guide.pdf |

October 2010 | Accessed on 31 August 2022 | The source is publicly available information and does not contain classification markings]

[14] [National Institute of Standards and Technology | Kevin Finisterre | “The Five W’s of Citect ODBC Vulnerability CVE-2008-2639” | https://nvd.nist.gov/vuln/detail/CVE-2008-2639 | 16 June 2008 | Accessed on 31 August 2022 | The source is publicly available information and does not contain classification markings]

[15] [National Institute of Standards and Technology | Kevin Finisterre | “The Five W’s of Citect ODBC Vulnerability CVE-2008-2639” | https://nvd.nist.gov/vuln/detail/CVE-2008-2639 | 16 June 2008 | Accessed on 31 August 2022 | The source is publicly available information and does not contain classification markings]

[16] [Bloomberg| Jordan Robertson and Michael Riley | “Mysterious ’08 Turkey Pipeline Blast Opened New Cyberwar” | https://www.bloomberg.com/news/articles/2014-12-10/mysterious-08-turkey-pipeline-blast-opened-new-cyberwar | 10 December 2014 | Accessed on 15 August 2022 | The source is publicly available information and does not contain classification markings]

[17] [Bloomberg | Jordan Robertson and Michael Riley | “Mysterious ’08 Turkey Pipeline Blast Opened New Cyberwar” | https://www.bloomberg.com/news/articles/2014-12-10/mysterious-08-turkey-pipeline-blast-opened-new-cyberwar#xj4y7vzkg | 10 December 2014 | Accessed on 6 June 2022 | The source is publicly available information and does not contain classification markings]

[18] [The Internet Society | “Real Time Streaming Protocol (RTSP): Request for Comment: 2326” | https://www.rfc-editor.org/rfc/rfc2326 | April 1998 | Accessed on 15 August 2022 | The source is publicly available information and does not contain classification markings]

[19] [SANS | Robert Lee, Tim Conway, and Michael Assante | “ICS Defense Use Case” | https://assets.contentstack.io/v3/assets/blt36c2e63521272fdc/bltae3dda4993b8c720/607f23571cac355a10f6bdc9/Media-report-of-the-BTC-pipeline-Cyber-Attack.pdf | 20 December 2014 | Accessed on 6 June 2022 | The source is publicly available information and does not contain classification markings]

[20] [Bloomberg | Jordan Robertson and Michael Riley | “Mysterious ’08 Turkey Pipeline Blast Opened New Cyberwar” | https://www.bloomberg.com/news/articles/2014-12-10/mysterious-08-turkey-pipeline-blast-opened-new-cyberwar#xj4y7vzkg | 10 December 2014 | Accessed on 6 June 2022 | The source is publicly available information and does not contain classification markings]

[21] [CitectSCADA | Schneider Electric | “CitectSCADA User Guide | https://www.koningenhartman.nl/UserFiles/Product/Datasheet/CitectSCADA%20User%20Guide.pdf | October 2010 | Accessed on 31 August 2022 | The source is publicly available information and does not contain classification markings]

[22] [Microsoft | “netstat” | https://learn.microsoft.com/en-us/windows-server/administration/windows-commands/netstat | 29 July 2021 | Accessed on 15 August 2022 | The source is publicly available information and does not contain classification markings]

[23] [National Institute of Standards and Technology | Kevin Finisterre | “The Five W’s of Citect ODBC Vulnerability CVE-2008-2639” | https://nvd.nist.gov/vuln/detail/CVE-2008-2639 | 16 June 2008 | Accessed on 31 August 2022 | The source is publicly available information and does not contain classification markings]

[24] [Nmap Software LLC | “The Nmap Project” | https://nmap.org/book/man.html | 2005-2022 | Accessed on 17 August 2022 | The source is publicly available information and does not contain classification markings]

[25] [National Institute of Standards and Technology | Kevin Finisterre | “The Five W’s of Citect ODBC Vulnerability CVE-2008-2639” | https://nvd.nist.gov/vuln/detail/CVE-2008-2639 | 16 June 2008 | Accessed on 31 August 2022 | The source is publicly available information and does not contain classification markings]

[26] [National Institute of Standards and Technology | Kevin Finisterre | “The Five W’s of Citect ODBC Vulnerability CVE-2008-2639” | https://nvd.nist.gov/vuln/detail/CVE-2008-2639 | 16 June 2008 | Accessed

on 31 August 2022 | The source is publicly available information and does not contain classification markings]

[27] [National Institute of Standards and Technology | Kevin Finisterre | “The Five W’s of Citect ODBC Vulnerability CVE-2008-2639” | https://nvd.nist.gov/vuln/detail/CVE-2008-2639 | 16 June 2008 | Accessed on 31 August 2022 | The source is publicly available information and does not contain classification markings]

[28] [National Institute of Standards and Technology | Kevin Finisterre | “The Five W’s of Citect ODBC Vulnerability CVE-2008-2639” | https://nvd.nist.gov/vuln/detail/CVE-2008-2639 | 16 June 2008 | Accessed on 31 August 2022 | The source is publicly available information and does not contain classification markings]

[29] [CitectSCADA | Schneider Electric | “CitectSCADA User Guide | https://www.koningenhartman.nl/UserFiles/Product/Datasheet/CitectSCADA%20User%20Guide.pdf | October 2010 | Accessed on 31 August 2022 | The source is publicly available information and does not contain classification markings]

[30] [CitectSCADA | Schneider Electric | “CitectSCADA User Guide | https://www.koningenhartman.nl/UserFiles/Product/Datasheet/CitectSCADA%20User%20Guide.pdf | October 2010 | Accessed on 31 August 2022 | The source is publicly available information and does not contain classification markings]

[31] [CitectSCADA | Schneider Electric | “CitectSCADA User Guide | https://www.koningenhartman.nl/UserFiles/Product/Datasheet/CitectSCADA%20User%20Guide.pdf | October 2010 | Accessed on 31 August 2022 | The source is publicly available information and does not contain classification markings]

[32] [CitectSCADA | Schneider Electric | “CitectSCADA User Guide | https://www.koningenhartman.nl/UserFiles/Product/Datasheet/CitectSCADA%20User%20Guide.pdf | October 2010 | Accessed on 31 August 2022 | The source is publicly available information and does not contain classification markings]

[33] [Bloomberg | Jordan Robertson and Michael Riley | “Mysterious ’08 Turkey Pipeline Blast Opened New Cyberwar” | https://www.bloomberg.com/news/articles/2014-12-10/mysterious-08-turkey-pipeline-blast-opened-new-cyberwar#xj4y7vzkg | 10 December 2014 | Accessed on 6 June 2022 | The source is publicly available information and does not contain classification markings]

[34] [Verso Books | James Marriott and Mike Minio-Puello | “The Oil Road: Journeys from The Caspian Sea to The City of London” | Chapter 14, pp 207-211 | 10 September 2013 | London, UK | Accessed on 17 August 2022 | The source is publicly available information and does not contain classification markings]

[35] [Reuters | Reuters Staff | “BTC oil pipeline damage study may take a week - BP” | https://www.reuters.com/article/turkey-georgia-pipelines/btc-oil-pipeline-damage-study-may-take-a-week-bp-idUSLD04125420080813 | 13 August 2008 | Accessed on 15 August 2022 | The source is publicly available information and does not contain classification markings]

[36] [Bloomberg | Jordan Robertson and Michael Riley | “Mysterious ’08 Turkey Pipeline Blast Opened New Cyberwar” | https://www.bloomberg.com/news/articles/2014-12-10/mysterious-08-turkey-pipeline-blast-opened-new-cyberwar#xj4y7vzkg | 10 December 2014 | Accessed on 6 June 2022 | The source is publicly available information and does not contain classification markings]

[37] [Bloomberg | Jordan Robertson and Michael Riley | “Mysterious ’08 Turkey Pipeline Blast Opened New Cyberwar” | https://www.bloomberg.com/news/articles/2014-12-10/mysterious-08-turkey-pipeline-blast-opened-new-cyberwar#xj4y7vzkg | 10 December 2014 | Accessed on 6 June 2022 | The source is publicly available information and does not contain classification markings]

[38] [Reuters | Orhan Coskun and Lada Yevgrashina | “Blast halts Azeri oil pipeline through Turkey” | https://www.reuters.com/article/us-turkey-pipeline-explosion/blast-halts-azeri-oil-pipeline-through-turkey-idUSSP31722720080806 | 5 August 2008 | Accessed on 17 August 2022 | The source is publicly available information and does not contain classification markings]

[39] [Reuters | Orhan Coskun and Lada Yevgrashina | “Blast halts Azeri oil pipeline through Turkey” | https://www.reuters.com/article/us-turkey-pipeline-explosion/blast-halts-azeri-oil-pipeline-through-turkey-idUSSP31722720080806 | 5 August 2008 | Accessed on 17 August 2022 | The source is publicly available information and does not contain classification markings]

[40] [The Sydney Morning Herald | Jordan Robertson and Michael Riley | “Before Stuxnet, Refahiye pipeline blast in Turkey opened new cyberwar era” | https://www.smh.com.au/world/before-stuxnet-refahiye-pipeline-blast-in-turkey-opened-new-cyberwar-era-20141212-125nvy.html | 12 December 2014 | Accessed on 15 August 2022 | The source is publicly available information and does not contain classification markings]