Threat Modeling of ICS Incidents/Failure Scenarios (Cyber) using ATT&CK for ICS

Harry Perper

Chief Engineer, National Cybersecurity FFRDC

The MITRE Corporation

harry@mitre.org

MITRE

ATT&CK ??? (its spelled wrong?)

Why did MITRE spend time researching?
and
What is it?

Tough Questions for ICS Defenders

- How effective are my defenses?
- Do I have a chance at detecting an APT?
- Is the data I'm collecting useful?
- Do I have overlapping tool coverage?
- Will a new product help my organization's defenses?

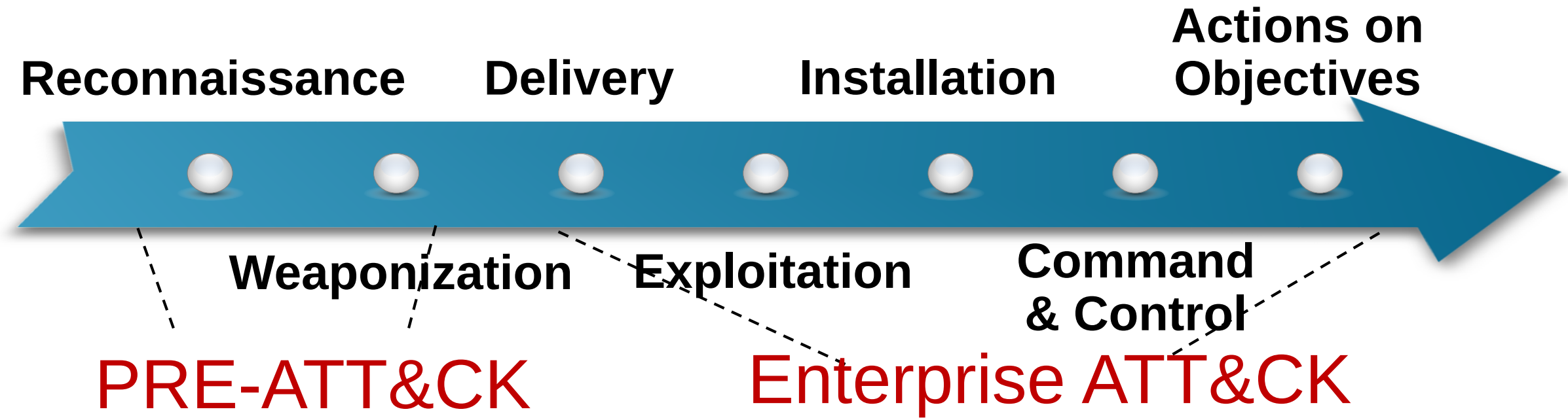
Tactics: the adversary's technical goals

Techniques: how the goals are achieved

Initial Access	Execution	Persistence	Privilege Escalation	Defense Evasion	Credential Access	Discovery	Lateral Movement	Collection	Command And	Exfiltration	Impact
Drive-by Compromise	AppleScript	.bash_profile and .bashrc	Access Token Manipulatio	Access Token Manipulatio	Account Manipulation	Account Discovery	AppleScript	Audio Capture	Commonly Used Port	Automated Exfiltration	Data Destruction
Exploit Public-Facing Application	CMSTP	Accessibility Features	Accessibility Features	Binary Padding	Bash History	Application Window Discovery	Application Deployment Software	Automated Collection	Communication Through Removable Media	Data Compressed	Data Encrypted for Impact
External Remote Services	Command-Line Interface	Account Manipulation	AppCert DLLs	BITS Jobs	Brute Force	Browser Bookmark Discovery	Distributed Component Object Model	Clipboard Data	Connection Proxy	Data Encrypted	Defacement
Hardware Additions	Compiled HTML File	AppCert DLLs	AppInit DLLs	Bypass User Account Control	Credential Dumping	Domain Trust Discovery	Exploitation of Remote Services	Data from Information Repositories	Custom Command and Control Protocol	Data Transfer Size Limits	Disk Content Wipe
Replication Through Removable Media	Control Panel Items	AppInit DLLs	Application Shimming	Clear Command History	Credentials in Files	File and Directory Discovery	Logon Scripts	Data from Local System	Custom Cryptographic Protocol	Exfiltration Over Alternativ Protocol	Disk Structure Wipe
Spearphishing Attachmen	Dynamic Data Exchange	Application Shimming	Bypass User Account Control	CMSTP	Credentials in Registry	Network Service Scanning	Pass the Hash	Data from Network Shared Drive	Data Encoding	Exfiltration Over Comman and Control Channel	Endpoint Denial of Service
Spearphishing Link	Execution through API	Authentication Package	DLL Search Order Hijacking	Code Signing	Exploitation for Credential Access	Network Share Discovery	Pass the Ticket	Data from Removable Media	Data Obfuscation	Exfiltration Over Other Network Medium	Firmware Corruption
Spearphishing via Service	Execution through Module Load	BITS Jobs	Dylib Hijacking	Compile After Delivery	Forced Authentication	Network Sniffing	Remote Desktop Protocol	Data Staged	Domain Fronting	Exfiltration Over Physical Medium	Inhibit System Recovery
Supply Chain Compromis	Exploitation for Client Execution	Bootkit	Exploitation for Privilege Escalation	Compiled HTML File	Hooking	Password Policy Discove	Remote File Copy	Email Collection	Domain Generation Algorithms	Scheduled Transfer	Network Denial of Service
Trusted Relationship	Graphical User Interface	Browser Extensions	Extra Window Memory Injection	Component Firmware	Input Capture	Peripheral Device Discovery	Remote Services	Input Capture	Fallback Channels		Resource Hijacking
Valid Accounts	InstallUtil	Change Default File Association	File System Permissions Weakness	Component Object Model Hijacking	Input Prompt	Permission Groups Discovery	Replication Through Removable Media	Man in the Browser	Multi-hop Proxy		Runtime Data Manipulation
	Launchctl	Component Firmware	Hooking	Control Panel Items	Kerberoasting	Process Discovery	Shared Webroot	Screen Capture	Multi-Stage Channels		Service Stop
	Local Job Scheduling	Component Object Model Hijacking	Image File Execution Options Injection	DCShadow	Keychain	Query Registry	SSH Hijacking	Video Capture	Multiband Communication		Stored Data Manipulation
	LSASS Driver	Create Account	Launch Daemon	Deobfuscate/Decode Files or Information	LLMNR/NBT-NS Poisonin and Relay	Remote System Discover	Taint Shared Content		Multilayer Encryption		Transmitted Data Manipulation
	Mshta	DLL Search Order Hijacking	New Service	Disabling Security Tools	Network Sniffing	Security Software Discovery	Third-party Software		Port Knocking		
	PowerShell	Dylib Hijacking	Path Interception	DLL Search Order Hijacking	Password Filter DLL	System Information Discovery	Windows Admin Shares		Remote Access Tools		
	Regsvcs/Regasm	External Remote Services	Plist Modification	DLL Side-Loading	Private Keys	System Network Configuration Discovery	Windows Remote Management		Remote File Copy		
	Regsvr32	File System Permissions Weakness	Port Monitors	Execution Guardrails	Securityd Memory	System Network Connections Discovery			Standard Application Layer Protocol		
	Rundll32	Hidden Files and Directories	Process Injection	Exploitation for Defense Evasion	Two-Factor Authentication Interception	System Owner/User Discovery			Standard Cryptographic Protocol		
	Scheduled Task	Hooking	Scheduled Task	Extra Window Memory Injection		System Service Discovery			Standard Non-Application Layer Protocol		
	Scripting	Hypervisor	Service Registry Permissions Weakness	File Deletion		System Time Discovery			Uncommonly Used Port		
	Service Execution	Image File Execution Options Injection	Setuid and Setgid	File Permissions Modification		Virtualization/Sandbox Evasion			Web Service		
	Signed Binary Proxy Execution	Kernel Modules and Extensions	SID-History Injection	File System Logical Offsets							
	Signed Script Proxy Execution	Launch Agent	Startup Items	Gatekeeper Bypass							
	Source	Launch Daemon	Sudo	Group Policy Modification							
	Space after Filename	Launchctl	Sudo Caching	Hidden Files and Directories							
	Third-party Software	LC_LOAD_DYLIB Addition	Valid Accounts	Hidden Users							
	Trap	Local Job Scheduling	Web Shell	Hidden Window							
	Trusted Developer Utilities	Login Item		HISTCONTROL							
	User Execution	Logon Scripts		Image File Execution Options Injection							
	Windows Management Instrumentation	LSASS Driver		Indicator Blocking							
	Windows Remote Management	Modify Existing Service		Indicator Removal from Tools							
	XSL Script Processing	Netsh Helper DLL		Indicator Removal on Host							
		New Service		Indirect Command Execution							
		Office Application Startup		Install Root Certificate							
		Path Interception		InstallUtil							

MITRE

Zooming in on the Adversary Lifecycle



PRE-ATT&CK

Enterprise ATT&CK

Mobile ATT&CK

https://www.lockheedmartin.com/en-us/capabilities/cyber/cyber-kill-chain.html

MITRE

Breaking Down ATT&CK

Techniques: how the goals are achieved

Tactics: the adversary's technical goals

Initial Access	Execution	Persistence	Privilege Escalation	Defense Evasion	Credential Access	Discovery	Lateral Movement	Collection	Command And	Exfiltration	Impact
Drive-by Compromise	AppleScript	.bash_profile and .bashrc	Access Token Manipulati	Access Token Manipulati	Account Manipulation	Account Discovery	AppleScript	Audio Capture	Commonly Used Port	Automated Exfiltration	Data Destruction
Exploit Public-Facing Application	CMSTP	Accessibility Features	Accessibility Features	Binary Padding	Bash History	Application Window Discovery	Application Deployment Software	Automated Collection	Communication Through Removable Media	Data Compressed	Data Encrypted for Impact
External Remote Services	Command-Line Interface	Account Manipulation	AppCert DLLs	BITS Jobs	Brute Force	Browser Bookmark Discovery	Distributed Component Object Model	Clipboard Data	Connection Proxy	Data Encrypted	Defacement
Hardware Additions	Compiled HTML File	AppCert DLLs	AppInit DLLs	Bypass User Account Control	Credential Dumping	Domain Trust Discovery	Exploitation of Remote Services	Data from Information Repositories	Custom Command and Control Protocol	Data Transfer Size Limits	Disk Content Wipe
Replication Through Removable Media	Control Panel Items	AppInit DLLs	Application Shimming	Clear Command History	Credentials in Files	File and Directory Discovery	Logon Scripts	Data from Local System	Custom Cryptographic Protocol	Exfiltration Over Alternativ Protocol	Disk Structure Wipe
Spearphishing Attachmen	Dynamic Data Exchange	Application Shimming	Bypass User Account Control	CMSTP	Credentials in Registry	Network Service Scanning	Pass the Hash	Data from Network Shared Drive	Data Encoding	Exfiltration Over Comman and Control Channel	Endpoint Denial of Service
Spearphishing Link	Execution through API	Authentication Package	DLL Search Order Hijacking	Code Signing	Exploitation for Credential Access	Network Share Discovery	Pass the Ticket	Data from Removable Media	Data Obfuscation	Exfiltration Over Other Network Medium	Firmware Corruption
Spearphishing via Service	Execution through Module Load	BITS Jobs	Dylib Hijacking	Compile After Delivery	Forced Authentication	Network Sniffing	Remote Desktop Protocol	Data Staged	Domain Fronting	Exfiltration Over Physical Medium	Inhibit System Recovery
Supply Chain Compromis	Exploitation for Client Execution	Bootkit	Exploitation for Privilege Escalation	Compiled HTML File	Hooking	Password Policy Discove	Remote File Copy	Email Collection	Domain Generation Algorithms	Scheduled Transfer	Network Denial of Service
Trusted Relationship	Graphical User Interface	Browser Extensions	Extra Window Memory Injection	Component Firmware	Input Capture	Peripheral Device Discovery	Remote Services	Input Capture	Fallback Channels		Resource Hijacking
Valid Accounts	InstallUtil	Change Default File Association	File System Permissions Weakness	Component Object Model Hijacking	Input Prompt	Permission Groups Discovery	Replication Through Removable Media	Man in the Browser	Multi-hop Proxy		Runtime Data Manipulation
	Launchctl	Component Firmware	Hooking	Control Panel Items	Kerberoasting	Process Discovery	Shared Webroot	Screen Capture	Multi-Stage Channels		Service Stop
	Local Job Scheduling	Component Object Model Hijacking	Image File Execution Options Injection	DCShadow	Keychain	Query Registry	SSH Hijacking	Video Capture	Multiband Communication		Stored Data Manipulation
	LSASS Driver	Create Account	Launch Daemon	Deobfuscate/Decode Files or Information	LLMNR/NBT-NS Poisonin and Relay	Remote System Discover	Taint Shared Content		Multilayer Encryption		Transmitted Data Manipulation
	Mshta	DLL Search Order Hijacking	New Service	Disabling Security Tools	Network Sniffing	Security Software Discovery	Third-party Software		Port Knocking		
	PowerShell	Dylib Hijacking	Path Interception	DLL Search Order Hijacking	Password Filter DLL	System Information Discovery	Windows Admin Shares		Remote Access Tools		
	Regsvcs/Regasm	External Remote Services	Plist Modification	DLL Side-Loading	Private Keys	System Network Configuration Discovery	Windows Remote Management		Remote File Copy		
	Regsvr32	File System Permissions Weakness	Port Monitors	Exploitation for Defense Evasion	Securityd Memory	System Network Connections Discovery			Standard Application Layer Protocol		
	Rundll32	Hidden Files and Directories	Process Injection	Extra Window Memory Injection	Two-Factor Authentication Interception	System Owner/User Discovery			Standard Cryptographic Protocol		
	Scheduled Task	Hooking	Scheduled Task	File Deletion		System Service Discovery			Standard Non-Application Layer Protocol		
	Scripting	Hypervisor	Service Execution	File System Logical Offsets		System Time Discovery			Uncommonly Used Port		
	Service Execution	Image File Execution Options Injection	Setuid and Setgid	Gatekeeper Bypass		Virtualization/Sandbox Evasion			Web Service		
	Signed Binary Proxy Execution	Kernel Modules and Extensions	SID-History Injection	Hidden Files and Directories							
	Signed Script Proxy Execution	Launch Agent	Startup Items	Hidden Window							
	Source	Launch Daemon	Sudo	Image File Execution Options Injection							
	Space after Filename	Launchctl	Sudo Caching	Indicator Blocking							
	Third-party Software	LC_LOAD_DYLIB Addition	Valid Accounts	Indicator Removal from Tools							
	Trap	Local Job Scheduling	Web Shell	Indicator Removal on Host							
	Trusted Developer Utilities	Login Item		Indirect Command Execution							
	User Execution	Logon Scripts		Install Root Certificate							
	Windows Management Instrumentation	LSASS Driver		InstallUtil							
	Windows Remote Management	Modify Existing Service									
	XSL Script Processing	Netsh Helper DLL									
		New Service									
		Office Application Startup									
		Path Interception									

Procedures: Specific technique implementation

Spearphishing Attachment

Examples

Name	Description
APT19	APT19 sent spearphishing emails with malicious attachments in RTF and XLSM formats to deliver initial exploits.[1]
APT28	APT28 sent spearphishing emails containing malicious Microsoft Office attachments.[2][3][4][5][6]

MITRE

Who's Contributing to ATT&CK?

89 individuals and orgs!

- Alain Homewood, Insomnia Security
- Alan Neville, @abnev
- Anastasios Pingios
- Andrew Smith, @jakx_
- Barry Shteiman, Exabeam
- Bartosz Jerzman
- Bryan Lee
- Carlos Borges, CIP
- Casey Smith
- Christiaan Beek, @ChristiaanBeek
- Cody Thomas, SpecterOps
- Craig Aitchison
- Daniel Oakley
- Darren Spruell
- Dave Westgard
- David Ferguson, CyberSponse
- David Lu, Tripwire
- David Routin
- Ed Williams, Trustwave, SpiderLabs
- Edward Millington
- Elger Vinicius S. Rodrigues, @elgervinicius, CYBINT Centre
- Elia Florio, Microsoft
- Emily Ratliff, IBM
- ENDGAME
- Eric Kuehn, Secure Ideas
- Erye Hernandez, Palo Alto Networks
- Felipe Espósito, @Pr0teus
- FS-ISAC
- Hans Christoffer Gaardløs
- Itamar Mizrahi
- Itzik Kotler, SafeBreach
- Jacob Wilkin, Trustwave, SpiderLabs
- Jan Miller, CrowdStrike
- Jared Atkinson, @jaredcatkinson
- Jeremy Galloway
- John Lambert, Microsoft Threat Intelligence Center
- John Strand
- Josh Abraham
- Justin Warner, ICEBRG
- Leo Loobeek, @leoloobeek
- Loic Jaquemet
- Marc-Etienne M.Léveillé, ESET
- Mark Wee
- Matt Graeber, @mattifestation, SpecterOps
- Matt Kelly, @breakersall
- Matthew Demaske, Adaptforward
- Matthew Molyett, @s1air
- McAfee
- Michael Cox
- Mike Kemmerer
- Milos Stojadinovic
- Mnemonic
- Nick Carr, FireEye
- Nik Seetharaman, Palantir
- Nishan Maharjan, @loki248
- Oddvar Moe, @oddvarmoe
- Omkar Gudhate
- Patrick Campbell, @pjcampbe11
- Paul Speulstra, AECOM Global Security Operations Center
- Pedro Harrison
- Praetorian
- Rahmat Nurfauzi, @infosecn1nja, PT Xynexis International
- Red Canary
- RedHuntLabs (@redhuntlabs)
- Ricardo Dias
- Richard Gold, Digital Shadows
- Richie Cyrus, SpecterOps
- Robby Winchester, @robwinchester3
- Robert Falcone
- Romain Dumont, ESET
- Ryan Becwar
- Ryan Benson, Exabeam
- Scott Lundgren, @5twenty9, Carbon Black
- Stefan Kanthak
- Sudhanshu Chauhan, @Sudhanshu_C
- Sunny Neo
- Sylvain Gil, Exabeam
- Teodor Cimpoesu
- Tim MalcomVetter
- Tom Ueltschi @c_APT_ure
- Tony Lambert, Red Canary
- Travis Smith, Tripwire
- Tristan Bennett, Seamless Intelligence
- Valerii Marchuk, Cybersecurity Help s.r.o.
- Veeral Patel
- Vincent Le Toux
- Walker Johnson
- Ye Yint Min Thu Htut, Offensive Security Team, DBS Bank
- Yonatan Gotlib, Deep Instinct

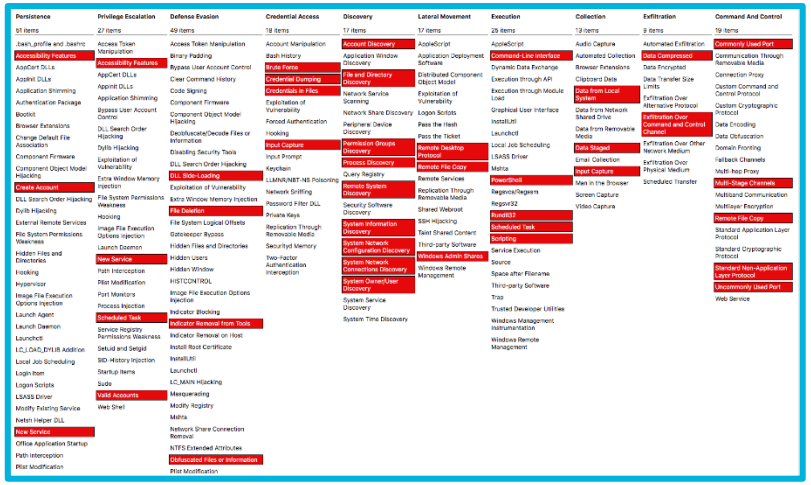
MITRE

ATT&CK Use Cases

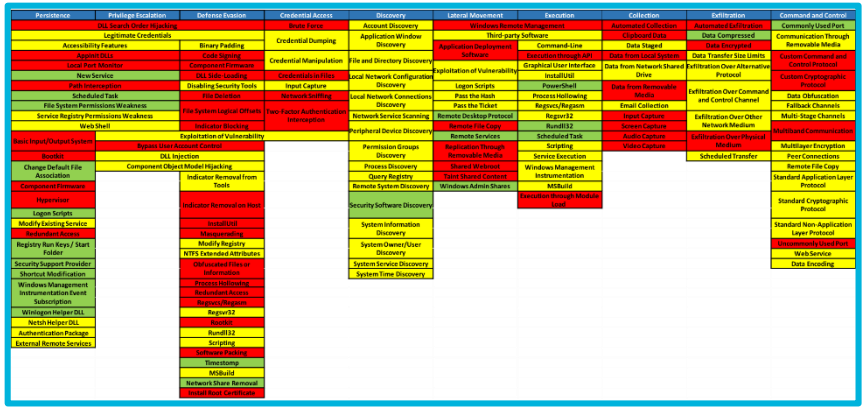
Detection

```
processes = search Process:Create
reg = filter processes where (exe == "reg.exe" and parent_exe
== "cmd.exe")
cmd = filter processes where (exe == "cmd.exe" and
parent_exe != "explorer.exe"")
reg_and_cmd = join (reg, cmd) where (reg.ppid == cmd.pid and
reg.hostname == cmd.hostname)
output reg_and_cmd
```

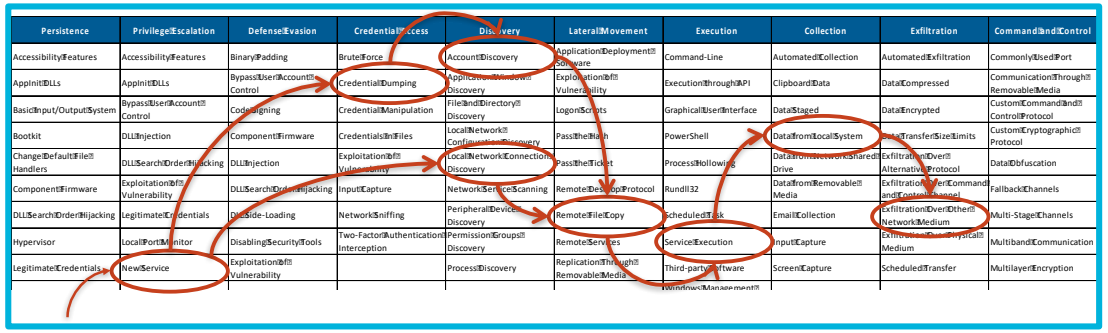
Threat Intelligence



Assessment and Engineering



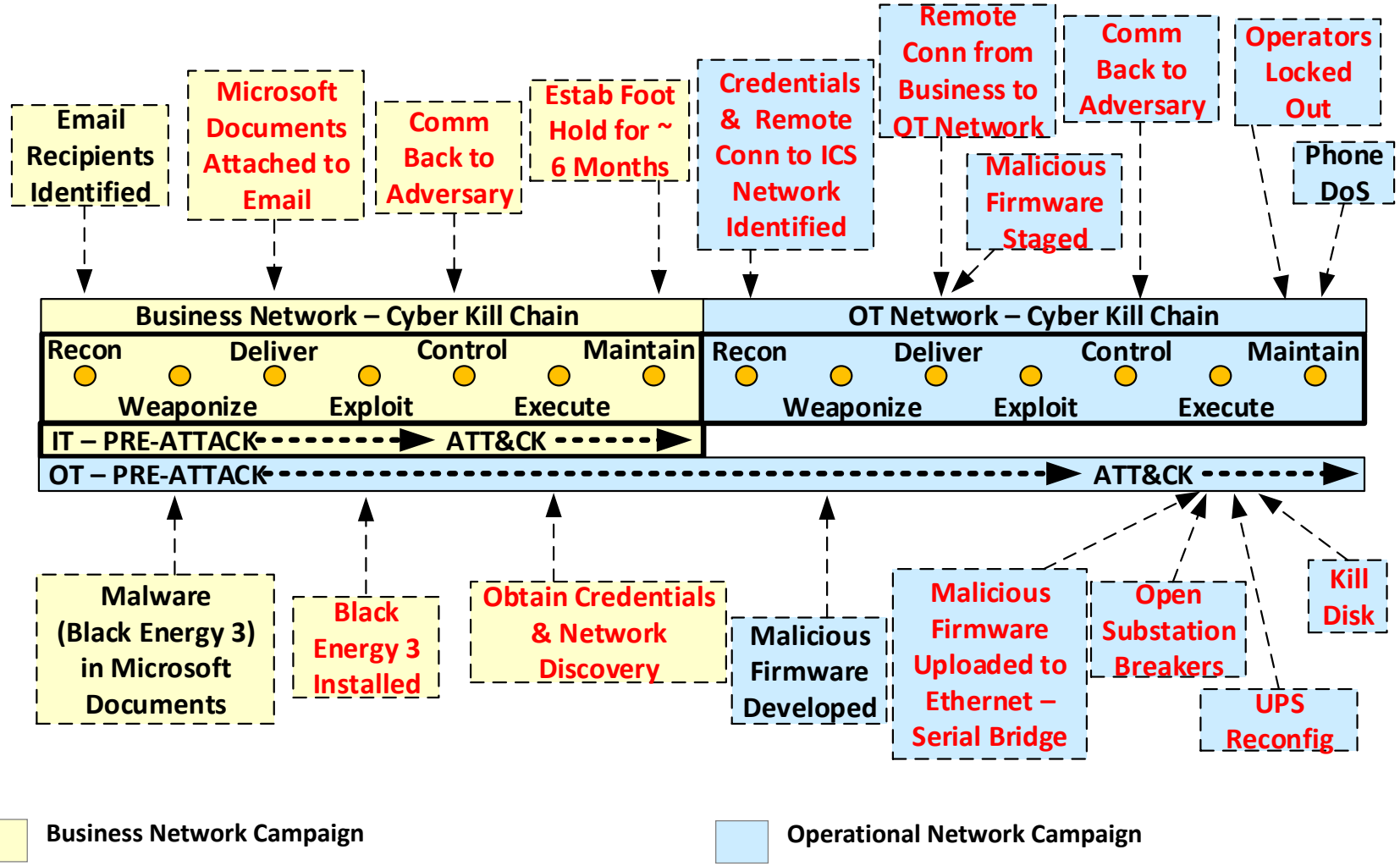
Adversary Emulation



MITRE

Lets apply those lessons to the industrial control system environments

Ukraine Power Grid (Substation) ICS Cyber Attack

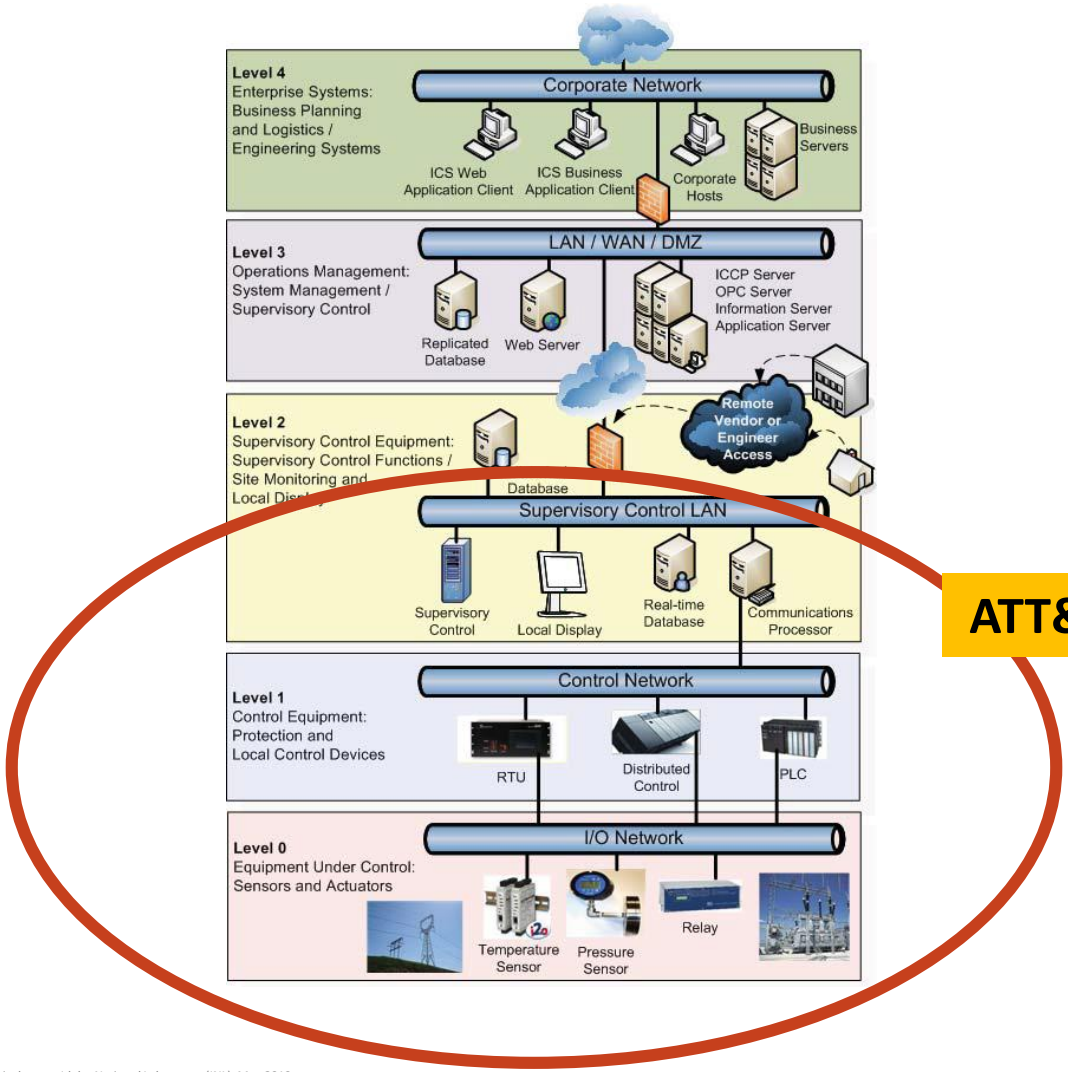


MITRE

ATT&CK for ICS: Why Different Models?

- **Adversary motivations are different**
  - Gaining access, accomplishing an objective depends on the target and what the objective is
    - Enterprise and cyber physical differences
  - Different phases in the lifecycle mean different choices
    - Pre/post compromise differences
- **Technologies are different**
  - How an adversary interacts with systems depends on that system
    - Enterprise systems and embedded devices differences
  - Very different ways of defending them
    - Platform dependencies
    - Data collection
    - Mitigation tradeoffs

ICS Reference Architecture (purdue)



ATT&CK for ICS focus

"NSTB Assessments Summary Report: Common Industrial Control System Cyber Security Weaknesses", Technical report Idaho National Laboratory (INL), May 2010.

MITRE

ATT&CK for ICS – Technique Matrix

Persistence	Privilege Escalation	Defense Evasion	Operator Evasion	Credential Access	Discovery	Lateral Movement	Execution	Command and Control	Compromise Integrity	Physical Impact
External Remote Services	Exploitation for Privilege Escalation	Alternate Modes of Operation	Block Reporting Message	Brute Force	Control Device Discovery	Default Credentials	Alternate Modes of Operation	Commonly Used Port	Alternate Modes of Operation	Block Command Message
Modify Control Logic	Valid Accounts	Exploitation for Defense Evasion	Block Serial Comm Port	Credential Dumping	Control Process	External Remote Services	Command-Line Interface	Connection Proxy	Block Serial Comm Port	Block Reporting Message
Module Firmware		File Deletion	Modify Control Logic	Default Credentials	I/O Module Enumeration	Modify Control Logic	Execution through API		Device Shutdown	DoS Service
System Firmware		Masquerading	Modify HMI/Historian Reporting	Network Sniffing	Location Identification	Valid Accounts	Graphical User Interface		DoS Service	Exploitation for Denial of Service
Valid Accounts		Modify Event Log	Modify I/O Image		Network Connection Enumeration		Man in the Middle		Modify Control Logic	Masquerading
		Modify System Settings	Modify Parameter		Network Service Scanning		Modify Control Logic		System Firmware	Modify Command Message
		Rootkit	Modify Physical Device Display		Network Sniffing		Modify System Settings			Modify Control Logic
			Modify Reporting Message		Remote System Discovery		Scripting			Modify Parameter
			Modify Reporting Settings		Role Identification					Modify Reporting Settings
			Modify Tag		Serial Connection Enumeration					Modify Tag
			Rootkit							Module Firmware
			Spoof Reporting Message							Spoof Command Message
										Spoof Reporting Message

Operator Evasion
- How can we fool the operator into thinking everything is OK
- How can we fool the operator to take the wrong action

Compromise Integrity
- How can we make changes to cause future physical impacts

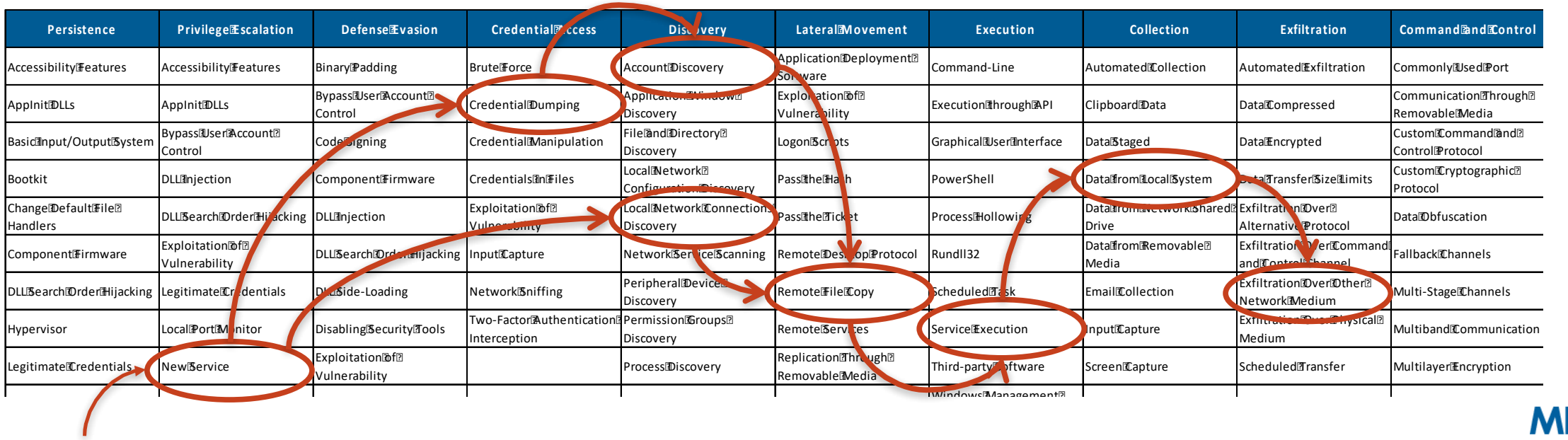
Physical Impact
- How can we stop/degrade the process
- How can we cause catastrophic failure

MITRE

Adversary Emulation with ATT&CK for ICS

Adversary Emulation

- **AKA: Threat-based Red Teaming**
- **Adversary Emulation**
  - Emulate the techniques of an adversary that's most likely to target your environment
  - Focus on the behaviors of those techniques instead of specific implementations



Persistence	Privilege Escalation	Defense Evasion	Credential Access	Discovery	Lateral Movement	Execution	Collection	Exfiltration	Command and Control
Accessibility Features	Accessibility Features	Binary Padding	Brute Force	Account Discovery	Application Deployment Software	Command-Line	Automated Collection	Automated Exfiltration	Commonly Used Port
AppInit DLLs	AppInit DLLs	Bypass User Account Control	Credential Dumping	Application Window Discovery	Exploitation of Vulnerability	Execution through API	Clipboard Data	Data Compressed	Communication Through Removable Media
Basic Input/Output System	Bypass User Account Control	Code Signing	Credential Manipulation	File and Directory Discovery	Logon Scripts	Graphical User Interface	Data Staged	Data Encrypted	Custom Command and Control Protocol
Bootkit	DLL Injection	Component Firmware	Credentials in Files	Local Network Configuration Discovery	Pass the Hash	PowerShell	Data from Local System	Data Transfer Size Limits	Custom Cryptographic Protocol
Change Default File Handlers	DLL Search Order Hijacking	DLL Injection	Exploitation of Vulnerability	Local Network Connections Discovery	Pass the Ticket	Process Hollowing	Data from Network Shared Drive	Exfiltration Over Alternative Protocol	Data Obfuscation
Component Firmware	Exploitation of Vulnerability	DLL Search Order Hijacking	Input Capture	Network Service Scanning	Remote Desktop Protocol	Rundll32	Data from Removable Media	Exfiltration Over Command and Control channel	Fallback Channels
DLL Search Order Hijacking	Legitimate Credentials	DLL Side-Loading	Network Sniffing	Peripheral Device Discovery	Remote File Copy	Scheduled Task	Email Collection	Exfiltration Over Other Network Medium	Multi-Stage Channels
Hypervisor	Local Port Monitor	Disabling Security Tools	Two-Factor Authentication Interception	Permission Groups Discovery	Remote Services	Service Execution	Input Capture	Exfiltration Over Physical Medium	Multiband Communication
Legitimate Credentials	New Service	Exploitation of Vulnerability		Process Discovery	Replication Through Removable Media	Third-party Software	Screen Capture	Scheduled Transfer	Multilayer Encryption
						Windows Management			

MITRE

Use Case – Decompose CrashOverride

- **Using ATT&CK for ICS, the payloads of CrashOverride can be decomposed into adversarial tactics and techniques.**
- **This decomposition provides a means to implement the techniques in a different way.**
- **In this case, to make the attack relevant to US substations, we can implement using Opendnp3.**
- **Decomposition enables effective "purple teaming"**
  - Blue team can effectively assess their defenses associated with the techniques used by the red team

DNP3: Distributed Network Protocol

ICS ATT&CK: Industrial Control System – Adversary Tactics, Techniques & Common Knowledge

Create ICS ATT&CK Coverage Matrix (NOTIONAL)

Persistence	Privilege Escalation	Defense Evasion	Operator Evasion	Credential Access	Discovery	Lateral Movement	Execution	Command and Control	Compromise Integrity	Physical Impact
External Remote Services	Exploitation for Privilege Escalation	Alternate Modes of Operation	Block Reporting Message	Brute Force	Control Device Discovery	Default Credentials	Alternate Modes of Operation	Commonly Used Port	Alternate Modes of Operation	Block Command Message
Modify Control Logic	Valid Accounts	Exploitation for Defense Evasion	Block Serial Comm Port	Credential Dumping	Control Process	External Remote Services	Command-Line Interface	Connection Proxy	Block Serial Comm Port	Block Reporting Message
Module Firmware		File Deletion	Modify Control Logic	Default Credentials	I/O Module Enumeration	Modify Control Logic	Execution through API		Device Shutdown	DoS Service
System Firmware		Masquerading	Modify HMI/Historian Reporting	Network Sniffing	Location Identification	Valid Accounts	Graphical User Interface		DoS Service	Exploitation for Denial of Service
Valid Accounts		Modify Event Log	Modify I/O Image		Network Connection Enumeration		Man in the Middle		Modify Control Logic	Masquerading
		Modify System Settings	Modify Parameter		Network Service Scanning		Modify Control Logic		System Firmware	Modify Command Message
		Rootkit	Modify Physical Device Display		Network Sniffing		Modify System Settings			Modify Control Logic
			Modify Reporting Message		Remote System Discovery		Scripting			Modify Parameter
			Modify Reporting Settings		Role Identification					Modify Reporting Settings
			Modify Tag		Serial Connection Enumeration					Modify Tag
			Rootkit							Module Firmware
			Spoof Reporting Message							Spoof Command Message
										Spoof Reporting Message

Legend

- High Confidence of Detection
- Moderate Confidence of Detection
- Low Confidence of Detection

MITRE

Failure Scenarios

Lack of Open Source Cyber Incidents

- **Solely using an incident-driven approach to defend control systems against physical impacts may not be sufficient**
  - This approach relies on knowledge of adversary activities
- **The lack of incidents about successful attacks (causing physical impact) against control systems puts defenders at a disadvantage**
- **Credible failure scenarios can be used to augment the available incidents about attacks that can cause physical impacts on control systems**

Failure Scenarios

- **Failure scenarios include malicious and non-malicious events such as**:
  - Failures due to compromising equipment functionality,
  - Failures due to data integrity attacks,
  - Communications failures,
  - Human error,
  - Interference with the equipment lifecycle, and
  - Natural disasters that impact cyber security posture.
- **Useful to utilities for risk assessment, planning, procurement, training, tabletop exercises and security testing**

Example Sources of Failure Scenarios

- EPRI NESCOR Failure Scenarios
- OT personnel/SME
- Incident Reporting
- Failure or Safety Analysis
- System Analysis

EPRI NESCOR Failure Scenarios

National Electric Sector Cybersecurity Organization Resource (NESCOR) Failure Scenarios

- NESCOR failure scenarios are developed by EPRI for the US Department of Energy as a part of National Electric Sector Cybersecurity Organization Resource initiatives.
- NESCOR Failure Scenarios are a library of scenarios describing the impact of a cyber-attack on the electric sector, related vulnerabilities, and possible mitigations
- http://smartgrid.epri.com/NESCOR.aspx

NESCOR Failure Scenario Description Decomposition

DER.12 Modified Management Settings for Substation FDEMS Impact Power Quality

- A malicious individual accesses a utility FDEMS that manages DER generation and storage systems within a substation, and modifies the energy output, the volt-var curves, or other DER management settings. When the utility requests the FDEMS to control the DER systems to provide more vars, the FDEMS causes the DER systems to behave erratically and cause the substation to have power quality problems, including tripping of the transmission line breaker.
  - **Target** - A utility FDEMS
  - **Entry point** – N/A
  - **Attack Scenario** - Modifies the energy output, the volt-var curves, or other DER management settings
  - **System Function** - Manages DER generation and storage systems within a substation
  - **Potential Effect** - When the utility requests the FDEMS to control the DER systems to provide more vars, the FDEMS causes the DER systems to behave erratically and causes the substation to have power quality problems, including tripping of the transmission line breaker.

DER **Distributed Energy Resource**

FDEMS **Facilities DER Energy Management System**

MITRE

Attack Scenario to ATT&CK for ICS

Attack Scenario - Modifies the energy output, the volt-var curves, or other DER management settings

- **Persistence – External Remote Service**
- **Discovery – Control Process, Role Identification**
- **Credential Access – Default Credentials**
- **Execution – Command-Line Interface**
- **Physical Impact – Modify Parameter**

OT Subject Matter Experts

Example Failure Scenarios

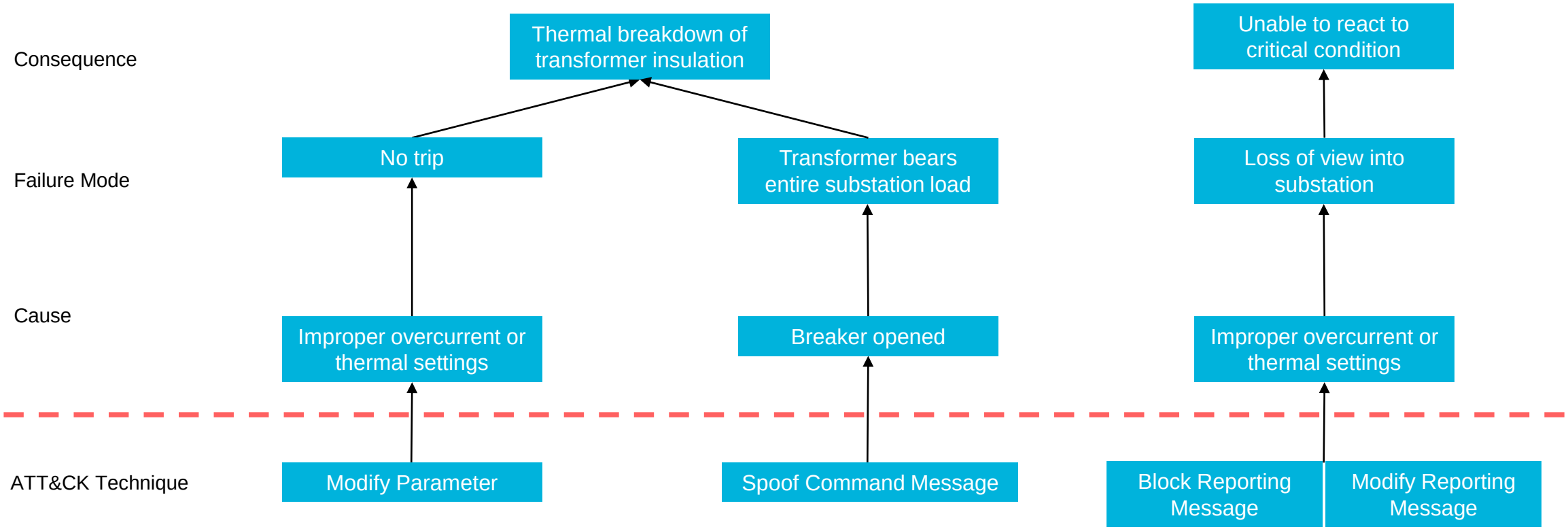
- **Scenario 1:** Transformer Overloading
  - Objective: Rapidly deteriorate transformer insulation
  - Technique: Modify trip settings of overcurrent and thermal protection relays, block communications (alarms, etc.) and open a breaker to force one transformer to bear load. Transformer will rapidly heat up and degrade insulation.

- **Scenario 2:** Disrupting Switching Executions for Circuit Breaker and Isolators
  - Objective: Cause dielectric breakdown of a breaker and isolator
  - Technique: Execute continuous switching actions to take one or more pieces of equipment out of service. Block communications (alarms, etc.)

- **Scenario 3:** Entire Substation Outage
  - Objective: Cause entire substage outage and contingencies
  - Technique: Execute command to open one or more breakers

Ten, Chee-Wooi, Koji Yamashita, Zhiyuan Yang, Athanasios Vasilakos, and Andrew Ginter. "Impact assessment of hypothesized cyberattacks on interconnected bulk power systems." *IEEE Transactions on Smart Grid* (2017).

Scenario 1: Transformer Overloading



MITRE

ICS Data Sources

Problem

- **Maintaining visibility into Operational Technology (OT) networks is essential for quickly detecting and remediating cyber threats.**
- **Understanding the various data sources that are available in OT networks is key to this endeavor. Network traffic is a popular source of data in OT networks but there are other valuable sources of data that are often overlooked.**
  - Host based logs housed on embedded OT devices such as Intelligent Electronic Devices (IED)
  - Asset management data associated with equipment under control.
- **Contextualizing how these data sources can be used for the identification of cyber threats**
- **Exploring the potential negative impacts that collection of data can have on operations.**

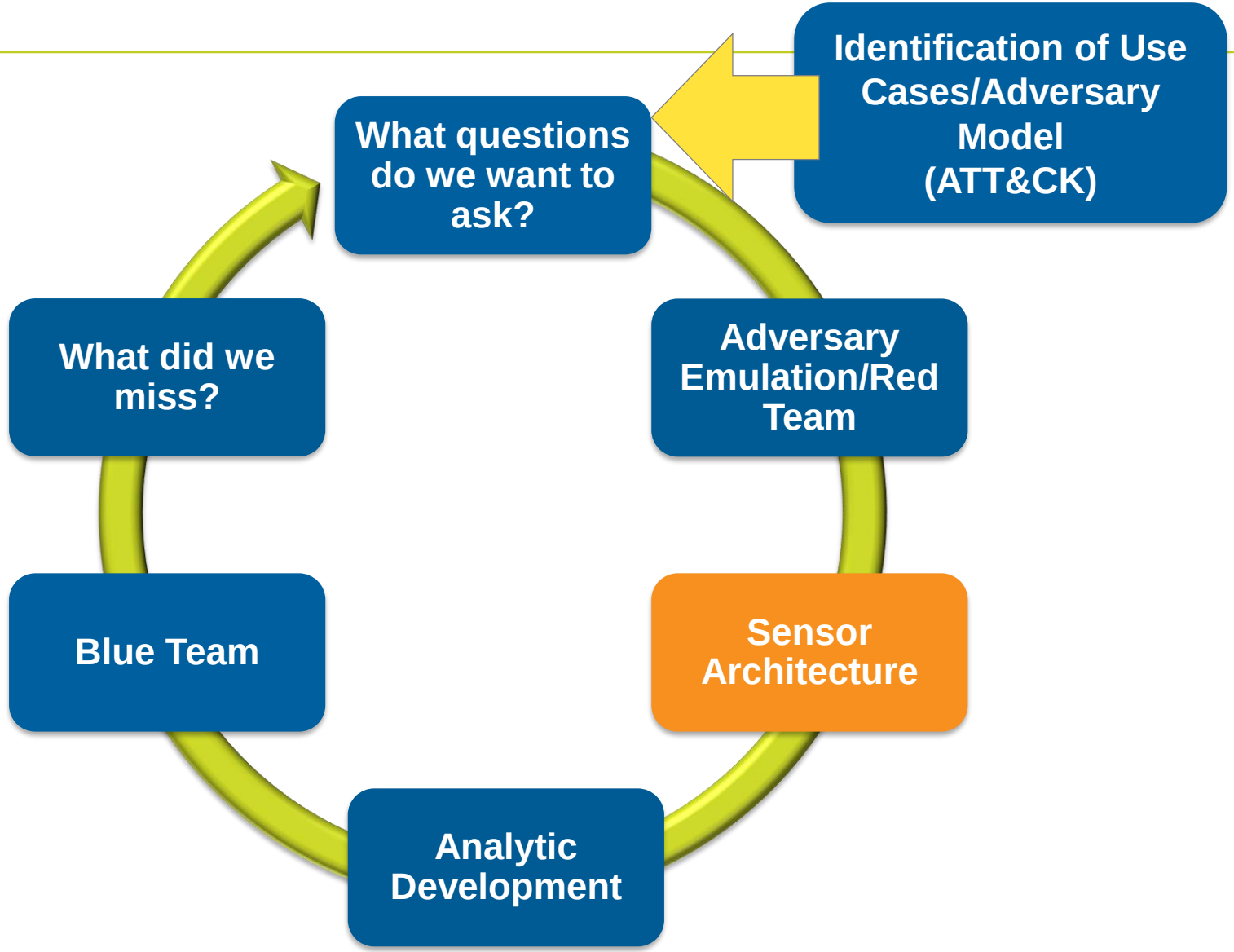
© 2019 The MITRE Corporation. All rights reserved.

Incident Response

- **If an incident occurred:**
  - What data is needed to conduct an investigation
  - Are there mechanism to pull data while a device is in operation?
    - Custom collectors
    - Vendor solutions
  - When does this data need to be collected
    - Realtime
    - Actively polled when needed
    - Roll a truck to the site to collect

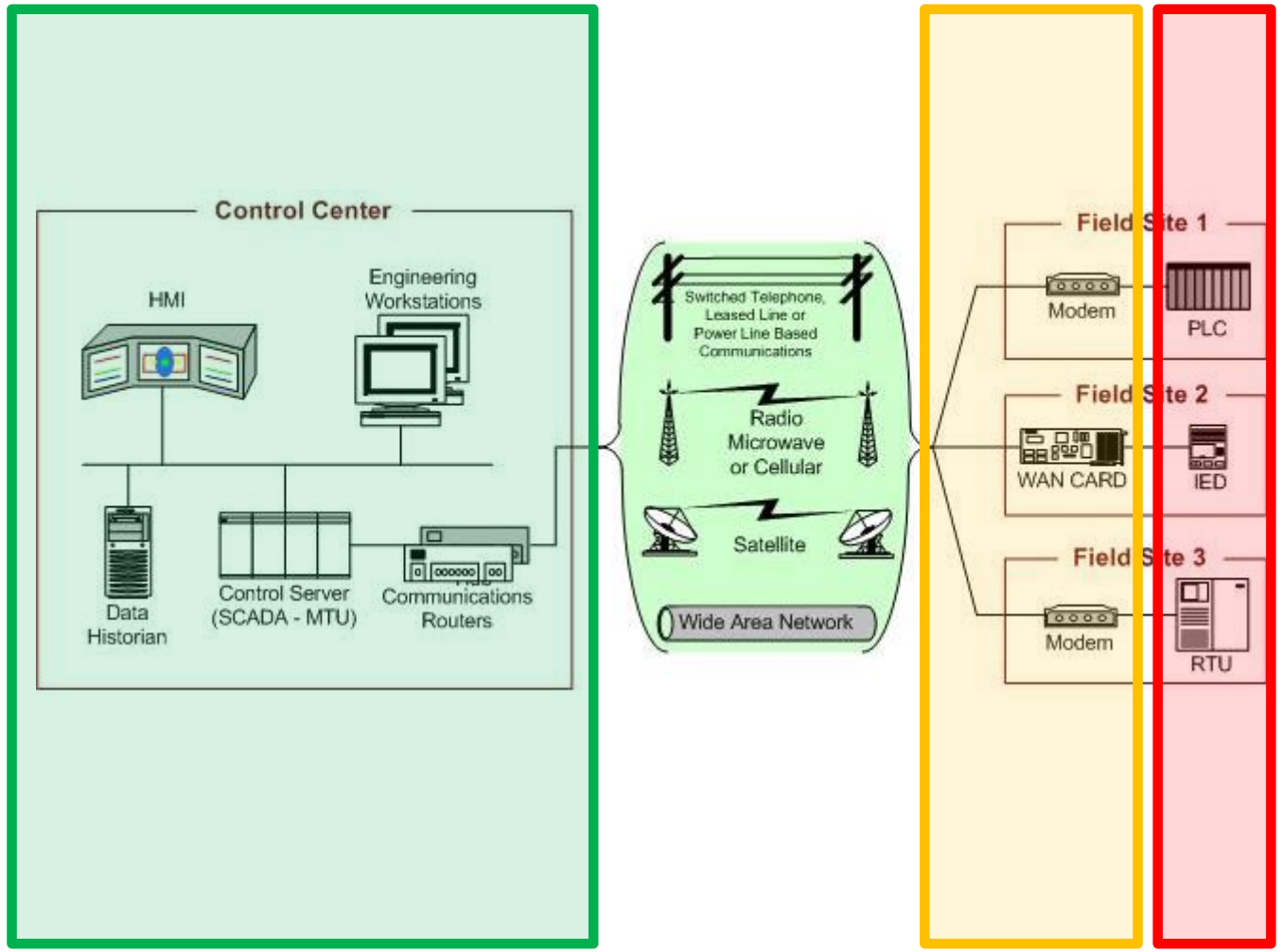
© 2019 The MITRE Corporation. All rights reserved.

Analytic Development Cycle



© 2019 The MITRE Corporation. All rights reserved.

Sensor Architecture - Data Source Collection



Typically collected	
Collected sometimes	
Typically not collected	

© 2019 The MITRE Corporation. All rights reserved.

https://csrc.nist.gov/publications/detail/sp/800-82/rev-2/final

MITRE

Identifying Host-based Data Sources

Data Sources

- **Configuration**
  - Firmware version
  - System settings
  - Control logic
  - Parameters
- **Performance and Statistics**
  - CPU, Memory, Disk, Ethernet, etc.
  - Network connection information
- **Process Information**
  - I/O values associated with tags
  - Alarms and Faults (e.g., Digital Fault Recorder)
  - Process quality (e.g., Phasor Measurement Unit)
- **Asset Management**
  - Condition-Based Monitoring
  - Predictive Maintenance
- **Physical**
  - Physical sensors (e.g., tamper detection)

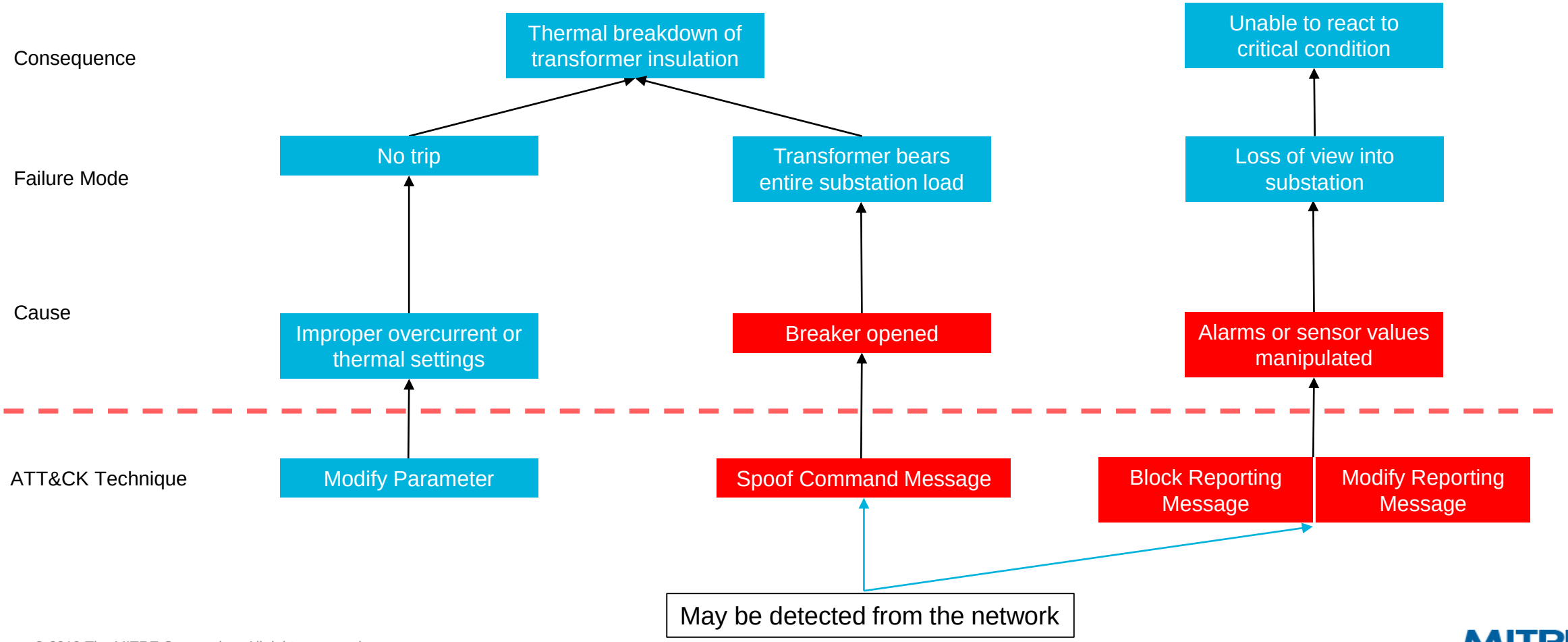
© 2019 The MITRE Corporation. All rights reserved.

Example Attack Scenario

- **Scenario: Transformer Overloading**
  - Objective: Rapidly deteriorate transformer insulation
  - Techniques:
    1. Modify trip settings of overcurrent and thermal protection relays
    2. Block communications (alarms, etc.)
    3. Open a breaker to force one transformer to bear load. Transformer will rapidly heat up and degrade insulation.

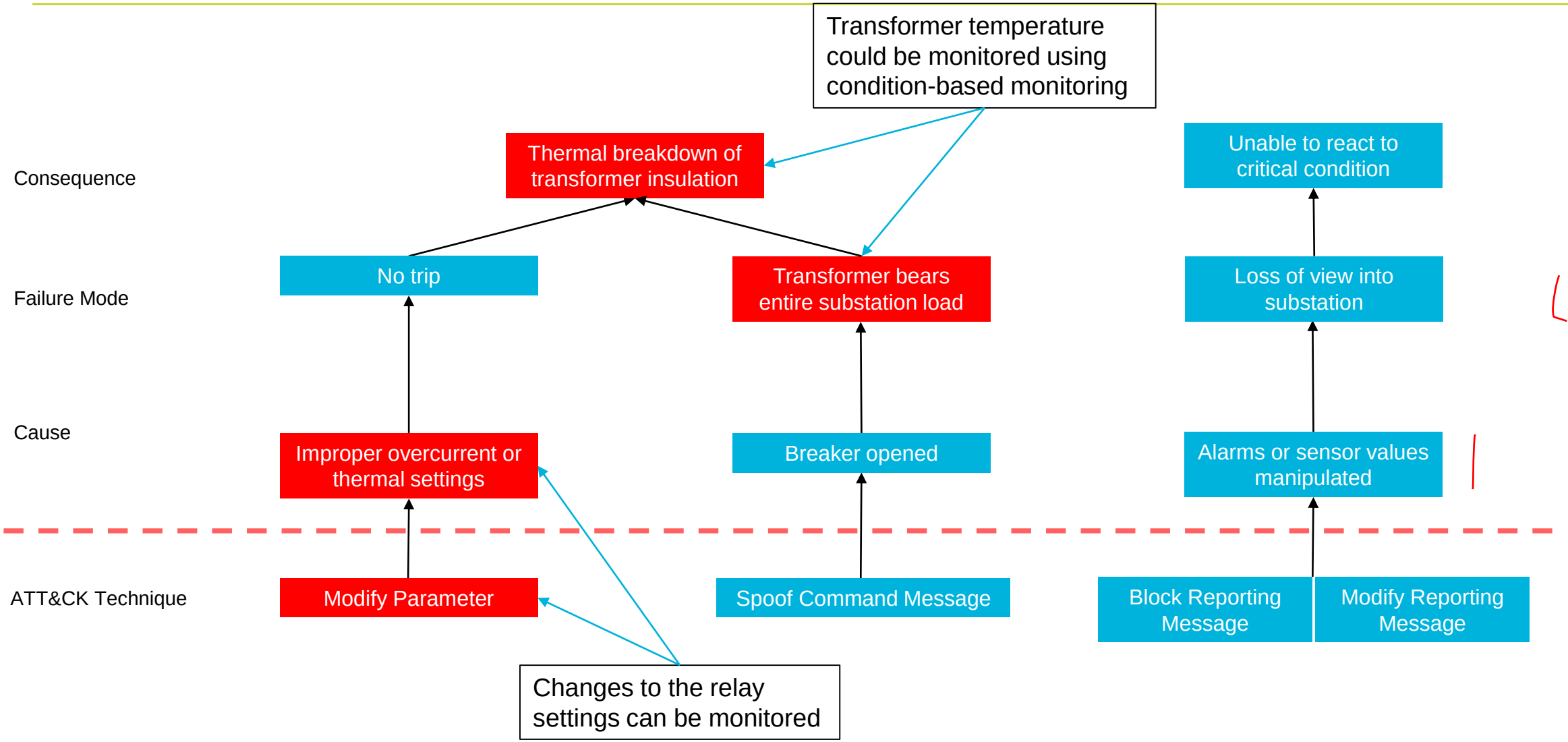
Ten, Chee-Wooi, Koji Yamashita, Zhiyuan Yang, Athanasios Vasilakos, and Andrew Ginter. "Impact assessment of hypothesized cyberattacks on interconnected bulk power systems." *IEEE Transactions on Smart Grid* (2017).

Data Sources - Attack Scenario – Network Data



MITRE

Data Sources - Attack Scenario – Host Data



MITRE

Devices being Evaluated

Vendor	Model	Function
SEL	351, 421, 487, 751	Protection Relay
SEL	3505, 3530	Automation Controller
SEL	3620	Security Gateway
GE	D60, T60	Protection Relay
AB	Logix5581E	Controller
AB	FlexIO	Ethernet I/O
Emerson	ROC800	Controller
Emerson	ControlWave	Controller, Ethernet I/O
Emerson	FloBoss	Sensor

© 2019 The MITRE Corporation. All rights reserved.

Identifying Data Sources - Approach

- **Easier**
  - Identify built-in collection mechanisms
  - Identify vendor aggregation points
- **More Effort**
  - Access device using vendor engineering software
  - Explore available data that can be used for threat detection
  - Collect data with engineering software
  - Analyze PCAPs to understand methods of access
    - Communication protocol (Telnet etc. vs Industrial Protocol)
    - Commands
  - Develop collector to replicate access

© 2019 The MITRE Corporation. All rights reserved.

Data Sources – SEL-751

- **Interfaces**
  - Telnet, FTP
- **Sequential Event Recorder**
  - Data - Firmware version, restarts, parameter changes, commands, etc.
  - Collection - Telnet Stream/CLI or FTP
- **Configuration**
  - Data - Firmware version, system settings, control logic, parameters, etc.
  - Collection - ymodem over Telnet or FTP

© 2019 The MITRE Corporation. All rights reserved.

Data Sources – SEL-RTAC

- **Interfaces**
  - Syslog, Postgresql, HTTP
- **Configuration**
  - Data - Firmware version, system settings, control logic, parameters, etc.
  - Collection – SQL queries and HTTP
- **Process Information**
  - Data – I/O values associated with tags, alarms and faults
  - Collection – SQL queries and Syslog

© 2019 The MITRE Corporation. All rights reserved.

Data Sources – SEL-3620

- **Interfaces**
  - Syslog, Postgresql, FTP, HTTP, Telnet, SSH
- **Performance and Statistics**
  - Data - Network connection information and performance
    - All established, closed, rejected, and dropped ICMP, UDP, or TCP connections
    - Information about the protocol of the packet, and, if applicable, the source and/or destination IP and port
    - What action was taken (dropped, rejected, established, or closed)
    - Performance reports
  - Collection – Syslog, Telnet and ymodem over Telnet/SSH

© 2019 The MITRE Corporation. All rights reserved.

Data Sources – SEL-3620

- **Process Information**
  - Data - Input alarm contact information
  - Collection - Syslog
- **Physical**
  - Data - Motion and light sensor can be collected here
  - Collection - Syslog
- **Configuration**
  - Data - Firmware version, system settings, control logic, parameters, etc. stored on supported connected devices
  - Collection - FTP

© 2019 The MITRE Corporation. All rights reserved.

Data Sources – Allen Bradley Logix5581E

- **Performance and Statistics**
  - Data - CPU, Networking, and Industrial Protocols
  - Collection – HTTP (Webpage scraping required)
- **Process Information**
  - Data - Read tags from the PLC
    - Can be used to collect OT state information
    - PLC has a function called Get System Value(GSV)
  - Collection - Ethernet/IP CIP

© 2019 The MITRE Corporation. All rights reserved.

Some Gaps in Data Offerings

- **Many devices do not have built-in logging interfaces. Collectors will need to be written or specialty software will be required to collect data.**
  - Some vendors have their own software to aggregate data from these devices
- **Most of the devices are missing easy access to traditional IT information, SEL devices being the exception**
- **Most of these devices are missing an easy way to monitor or collect deeper information, for example, mechanisms to dump memory are not prevalent.**

© 2019 The MITRE Corporation. All rights reserved.

ATT&CK for ICS Review Process

Review Process – The approach

1. Reach out to government, national labs, vendors, red teams, and utilities to review ATT&CK for ICS and provide feedback and content
2. Give an introductory walk through of the ATT&CK for ICS wiki to familiarize participants with wiki content
3. Provide secure access to the wiki to participants during the review period
4. Collect and incorporate feedback and content from participants
5. Begin the public release process

Review Process – What are we looking for?

- **Sharable incident data to help mature the model**
- **Feedback about technique groupings (e.g. Asset, Level)**
  - Suggestions about additional tactic categories
- **Feedback about technique names**
  - Which technique names seem too broad
  - Suggestions about naming convention
  - Additions to techniques
- **Errors and omissions**
  - Tactic and technique descriptions
  - Does the mapping of incident data match the adversary's TTP in incident reports
  - Was any information about adversary TTP omitted
- **Envisioned use cases in your organization**

ATT&CK

https://attack.mitre.org

attack@mitre.org

@MITREattack

MITRE