



MIDWEST
RELIABILITY
ORGANIZATION

2022 Annual Security Conference

October 5, 2022

CLARITY

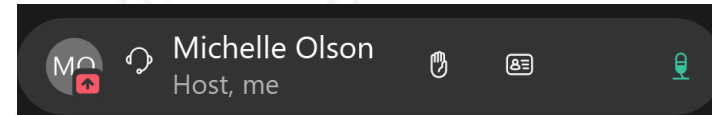
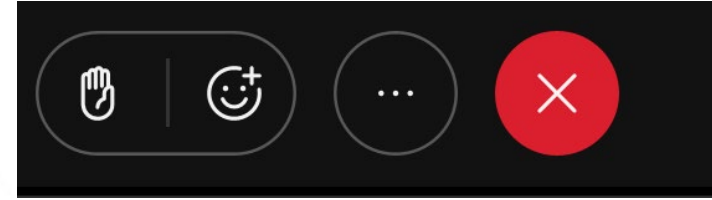
ASSURANCE

RESULTS

WebEx Chat Feature

Please hold questions until the end of each presentation unless speakers recommend otherwise.

If you would like to submit questions as the speakers are presenting, please submit them via the chat.



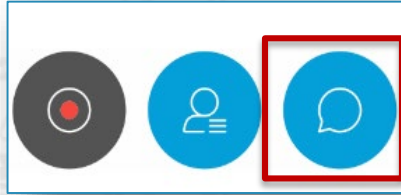
CLARITY

ASSURANCE

RESULTS

WebEx Chat Feature

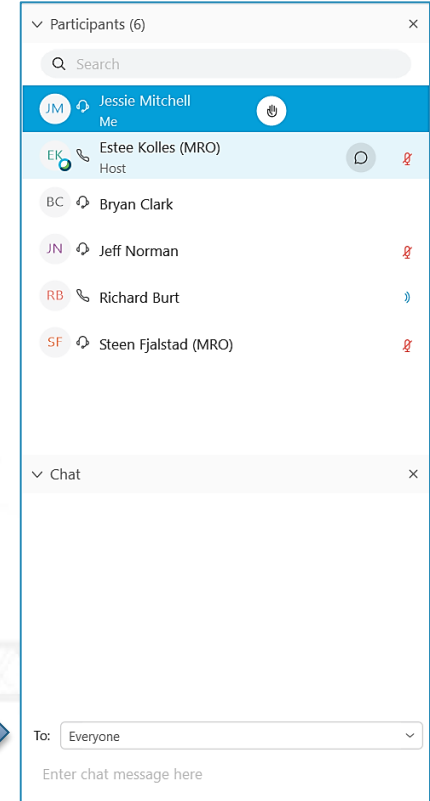
Open the Chat Feature:



The chat feature will appear to the right of the WebEx window.

Attendees should chat their questions to: “MRO Host”.

Select MRO Host by using the drop down arrow in the “To” field.



CLARITY

ASSURANCE

RESULTS

Disclaimer

The Midwest Reliability Organization (MRO) Security Advisory Council (SAC) is committed to providing training and non-binding guidance to industry stakeholders regarding existing and emerging security topics. Subject Matter Experts (SMEs) developed any materials, including presentations, through the MRO SAC from member organizations within the MRO Region and other government and industry security experts. The views in this presentation are presented by these MRO SAC SMEs, government, and industry experts, and do not express the opinions and views of MRO.





MIDWEST
RELIABILITY
ORGANIZATION

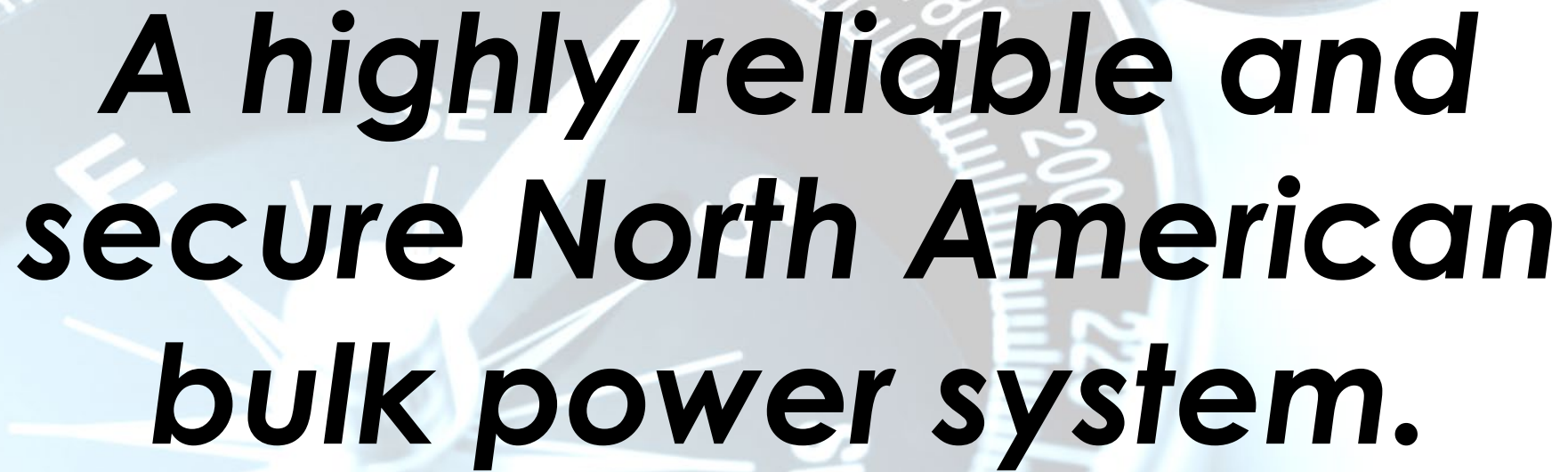
Assessing and Mitigating Regional BPS Risk

Security Conference, October 5, 2022

CLARITY

ASSURANCE

RESULTS



***A highly reliable and
secure North American
bulk power system.***

Our Shared Vision

The ERO Enterprise

- **The ERO Enterprise offers a unique, wide-area view of risk across North America**
 - Rapidly evolving resource mix
 - Energy assurance
 - Extreme weather events
 - Cyber and physical security
 - Supply chain vulnerabilities
 - Bulk power system modeling accuracy



MRO's Value Proposition

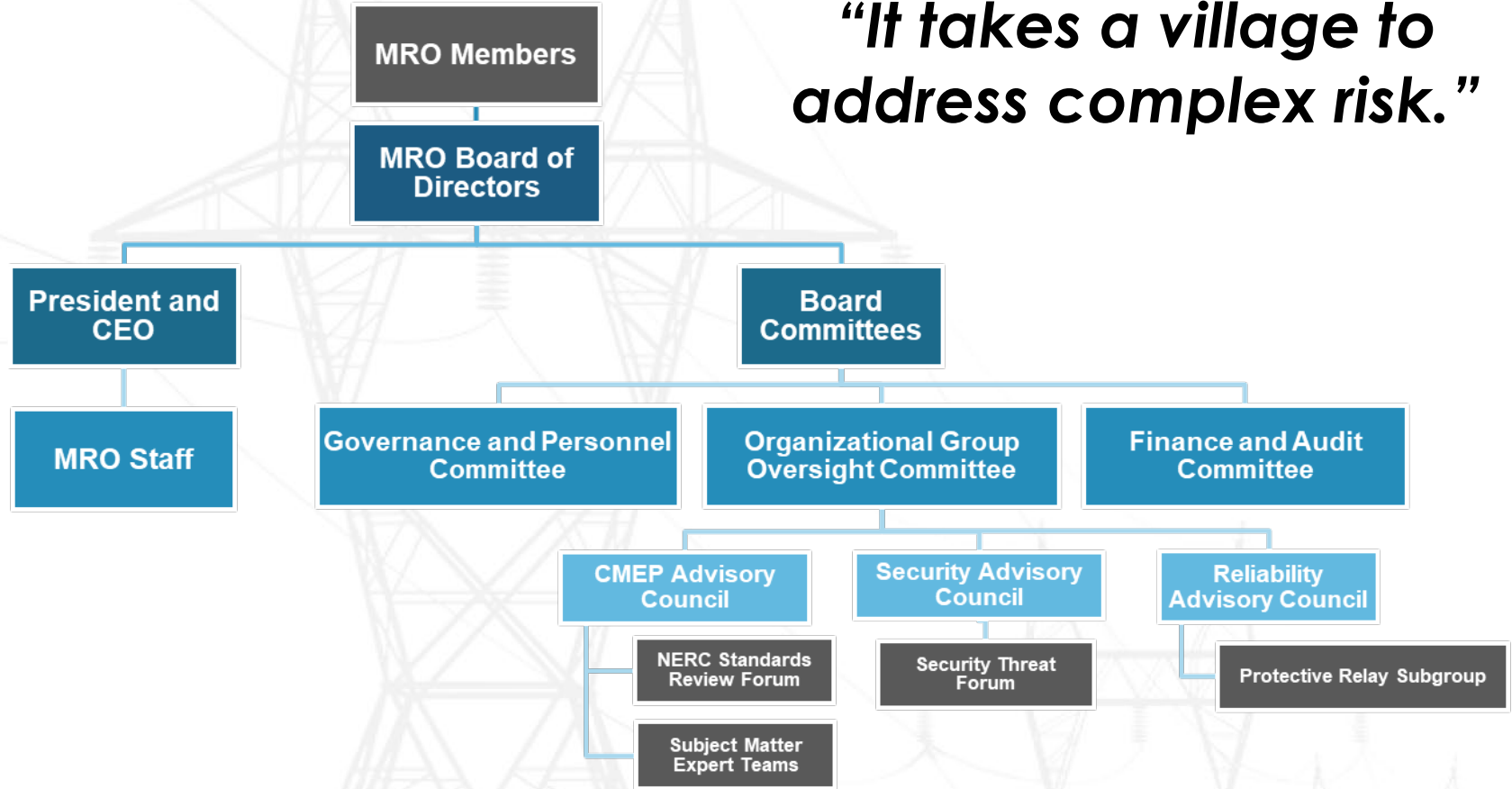
- **As part of the ERO, MRO offers a targeted, regional view of risk**
 - Winter planning reserve margins
 - Generation availability during severe cold weather
 - Lack of energy assurance assessments
 - Supply chain vulnerabilities
 - Insider threats, malware and ransomware
 - Bulk power system modeling accuracy





MRO Value Proposition – Bridging the Gap

“It takes a village to address complex risk.”

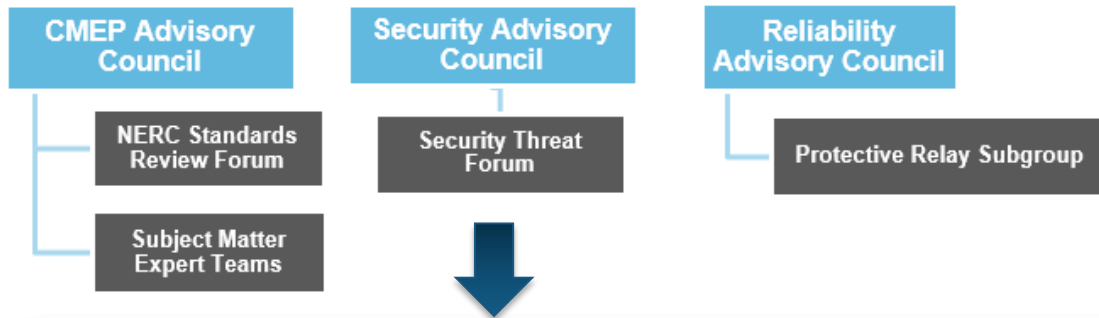




Role of the MRO Board



Role of MRO Leadership and Staff



- **Serve as subject matter experts to MRO's board, members, registered entities, and staff:**
 - Identify, assess and develop mitigation strategies for physical, cyber, and control system security risks within MRO's regional footprint.
 - Facilitate information sharing with regional constituents on emerging threats and vulnerabilities.
 - Provide input to and support the development of MRO's Regional Risk Assessment.
 - Expand outreach efforts to raise awareness of risk and strengthen security of the regional bulk power system.

Role of MRO Org Groups and the SAC

SAC Roster

Our Future Is
BRIGHT!



NAME	ROLE	COMPANY	TERM END
Clayton Whitacre	Chair	Great River Energy	12/31/2022
Michael Meason	Vice Chair	Western Farmers Electric Cooperative	12/31/2023
Brett Lawler	Member	Xcel Energy	12/31/2023
Chad Wasinger	Member	Sunflower Electric Power Cooperative	12/31/2023
Daniel Graham	Member	Basin Electric Power Cooperative	12/31/2024
Douglas Peterchuck	Member	Omaha Public Power District	12/31/2024
Jamey Sample	Member	Xcel Energy	12/31/2022
Jason Nations	Member	Oklahoma Gas and Electric	12/31/2024
Justin Haar	Member	Minnkota Power Cooperative	12/31/2023
Laura Liston	Member	Alliant Energy Corporation	12/31/2022
Matthew Szyda	Member	Manitoba Hydro	12/31/2023
Norma Browne	Member	Ameren	12/31/2024
Sam Ellis	Member	Southwest Power Pool, Inc.	12/31/2022
Tim Anderson	Member	Dairyland Power Cooperative	12/31/2024
Tony Eddleman	Member	Nebraska Public Power District	12/31/2022


Importance of Technology and Security

MRO Security Conference - 10/05/2022
Jeremy Anderson – VP & CIO

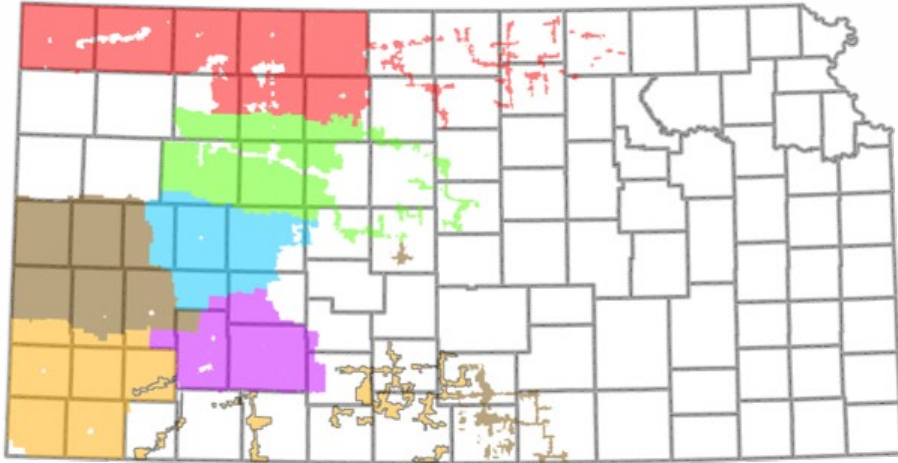
Email: jeremy.anderson@sunflower.net



SUNFLOWER ELECTRIC POWER CORPORATION

A Touchstone Energy® Cooperative 

Sunflower Electric Power Corp – Who We Are.....



- A not-for-profit wholesale electric utility corporation
- Formed in 1957 to provide wholesale generation to 6 member cooperatives
- Provider of wholesale generation and transmission services to Western Kansas
- Headquartered in Hays, Kansas



Importance of Technology & Security – A Reflection of “The Good.....”

- The utility industry has gone through extensive, technical transformation change including:
 - Evolution from mechanical to technical enabled generation and transmission control systems
 - Monitoring and management of generation and transmission assets through wired and wireless connectivity
 - Improved corporate practices (e.g., Finance, HR, Supply Chain, etc.)
 - Improved connectivity, collaboration, and communication capabilities
- With the above technology changes, increased expectations in effectiveness have been established through:
 - Speed of delivery and execution
 - Availability of systems
 - Responsiveness (e.g., break fix resolution timeliness, application response times, etc.)
- Proactive technical solutions exist to protect technology assets and information through:
 - Real time evaluation and monitoring of abnormal systems behavior
 - Isolation/notification of potential unauthorized intrusion attempts
 - Automated handling/remediation of unauthorized attempts to exploit vulnerabilities
 - Filtering capabilities that greatly reduce risk of “phishing” and/or unauthorized access



Importance of Technology & Security – “The Bad and The Ugly”

- Industry players are constantly under attack through a variety of cyber security exposures with the intent of disrupting technical solutions including:
 - Ransomware, encryption, remote control, and phishing.
 - Theft and distribution of credentials and sensitive information
 - Viruses, worms, and other malicious payloads
 - Others.....
- A quick history of business impacts with recent successful hacking/intrusion events:
 - Lawsuits levied with companies exhibiting cyber security risks/exposures
 - Unauthorized distribution of sensitive information impacting corporate credibility
 - Insurance policies have been created for cyber security, but coverages remain unclear
 - Significant costs incurred with ransomware payments made to bad actors to recover systems
 - Decryption efforts (post ransomware payments) have illustrated organic growth of data creating additional capacity issues impacting restoration timeframes
 - Publications in the handling of cyber security/ransomware events has increased momentum within the “bad actor” community



Importance of Technology & Security – Are We Proactively Prepared?

- Has proper investment occurred with proactive technology to successfully identify and prevent an attack?
- Is there a fostering environment of listening in what is needed to mitigate cyber security risks with some level of executive sponsorship?
- Are processes setup to minimize the time between identification and mitigation of a hacking attempt?
 - Real time monitoring tools in place?
 - Systematic notifications to technologists leveraged when hacking attempts occur?
 - Written procedures in place to know who does what and what needs to be done in priority order?
 - Are company cultures championed to openly notify technologists if exposed system behavior is exhibited?
 - Are the above tactics periodically exercised/practiced?
- The industry spends significant amounts of time and resources to proactively prevent a cyber security event but is enough focus applied in preparing reactively for the restoral of systems in the event of a successful attack?



Importance of Technology & Security – Are We Reactively Prepared?

- “Gold Copy” can be a potential solution.....
 - “Gold Copy” is an offline or disconnected backup copy of system data isolated in the event of a successful cyber attack event leveraging CIP-009 rigor
 - Pristine backup copies are encrypted, “air-gapped”, and stored offline from live systems to prevent contamination
 - Scheduled rotation of on-line to “air-gapped” backups defined at regular intervals
 - Purging of old backup data as required by media capacity leads to a robust, historical archive of data spanning multiple months with version control
 - Backup media devices stored in secured “storm cases” inside physical security perimeters to isolate and protect data
- “Gold Copy” data recovery and restoral approach (if required):
 - All impacted hardware and elements are wiped clean of data down to “bare metal” hardware
 - Operating Systems and Systems Software are restored first based on pristine, source data elements (OEM installation files, etc.)
 - Application data evaluated from the “Gold Copy” archive, targeted restoration dates identified, and restoration continues until completion
 - Periodic exercising of the above procedures occur to ensure maximum efficiency in restoral timelines



Importance of Technology & Security – Summary

- Capability enablement, enhancement, and dependance on technology solutions continues to increase across the industry
- With the above comes additional risk to technical infrastructure and business disruption as a result of “bad actor” activity
- Multiple technical solutions exist to proactively mitigate risk
- A reassessment of backup and restoral techniques should be considered
- A multi-layered, comprehensive approach with both proactive and reactive protection measures can improve risk mitigation associated with cyber security events and improve availability of technical systems



Hacking Closed Networks



Ira Winkler, CISSP
ira@securementem.com
+1-443-603-0200

Impossible to Hack

- The network is closed
- It's just a bunch of hype



HOLD MY ~~BEER~~



SECURE
MENTEM



Ignorance is Dangerous, NOT Bliss

- When you don't realize something is a threat, you don't protect against it
- The risk profile must be well understood
- Generally networks are closed, because of the perceived risk
If it's valuable enough to close a network, with all of the costs, it's valuable enough for an attacker to try to find a way in

SECURE
MENTEM

Meet Bandit



SECRET
MENTAL



The Vulnerabilities are Real



- 2008 RSA presentation about hacking the power grid
- 5 federal agents contacted me
 - 2 unannounced
- Lobbying group said they wanted to talk
 - “It’s not like we want to discredit you, or anything like that”
- Brian Krebs called saying the NRC wanted to brief him on why what I described was impossible
 - So he knew I was right

Two Months Later

washingtonpost.com > Technology

TVA Power Plants Vulnerable to Cyber Attacks, GAO Finds

By Brian Krebs

washingtonpost.com Staff Writer

Wednesday, May 21, 2008; 12:01 AM

TOOLBOX



Resize



Print



E-mail



Reprints

SECURE
MENTEM

The Ways Are Almost Infinite

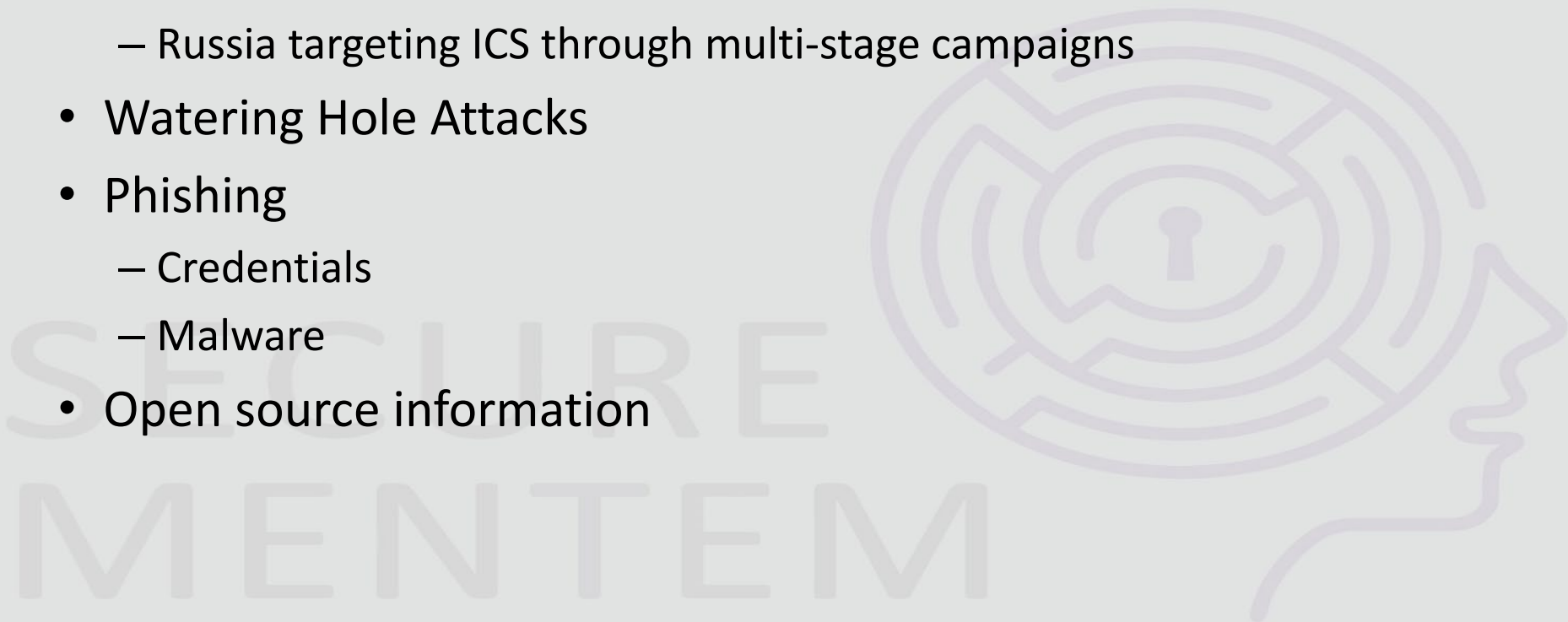


- Limited by creativity
- Many versions of the different scenarios
- Networks aren't really "closed"
- Access points uncontrolled
- Diagnostic equipment
- Insider abuse
- Compromise developers

SI
MENTEM

Targeting “Closed” Networks

- CERT TA18-074A
 - Russia targeting ICS through multi-stage campaigns
- Watering Hole Attacks
- Phishing
 - Credentials
 - Malware
- Open source information

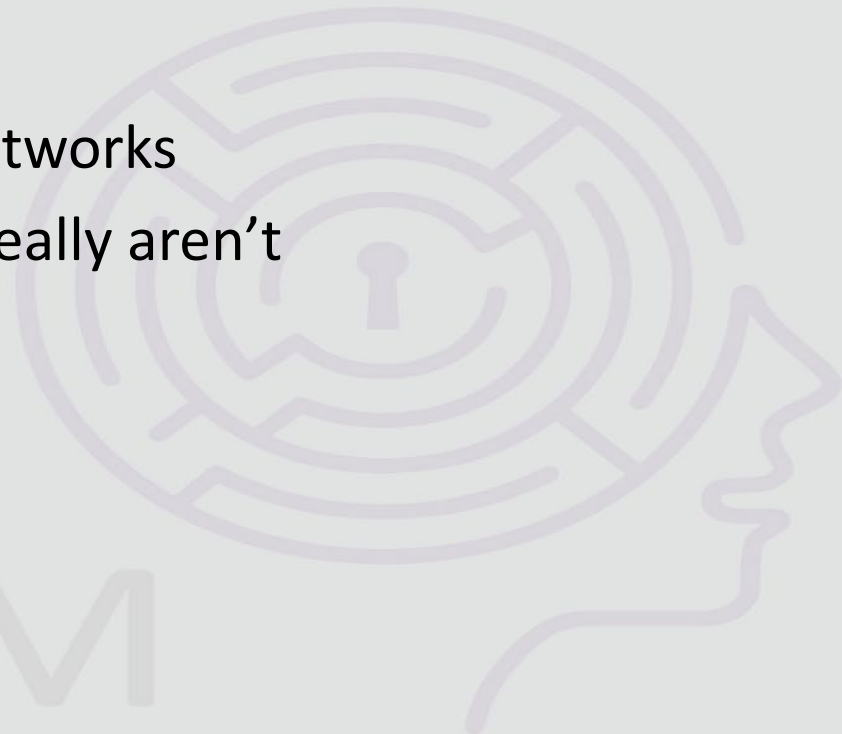


SECURE
MENTEM

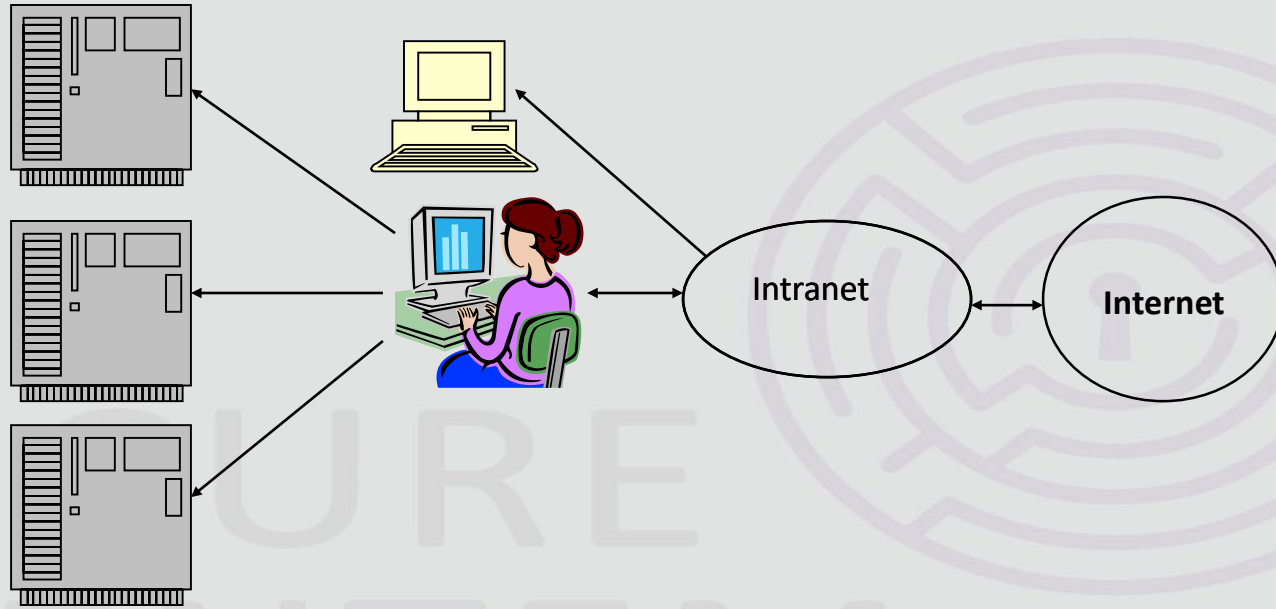
Closed Networks Usually Aren't

- Might have started out closed
- Functionality added periodically
- Don't want expense of multiple networks
- Put in “limited” connections that really aren't
- Bridges are added

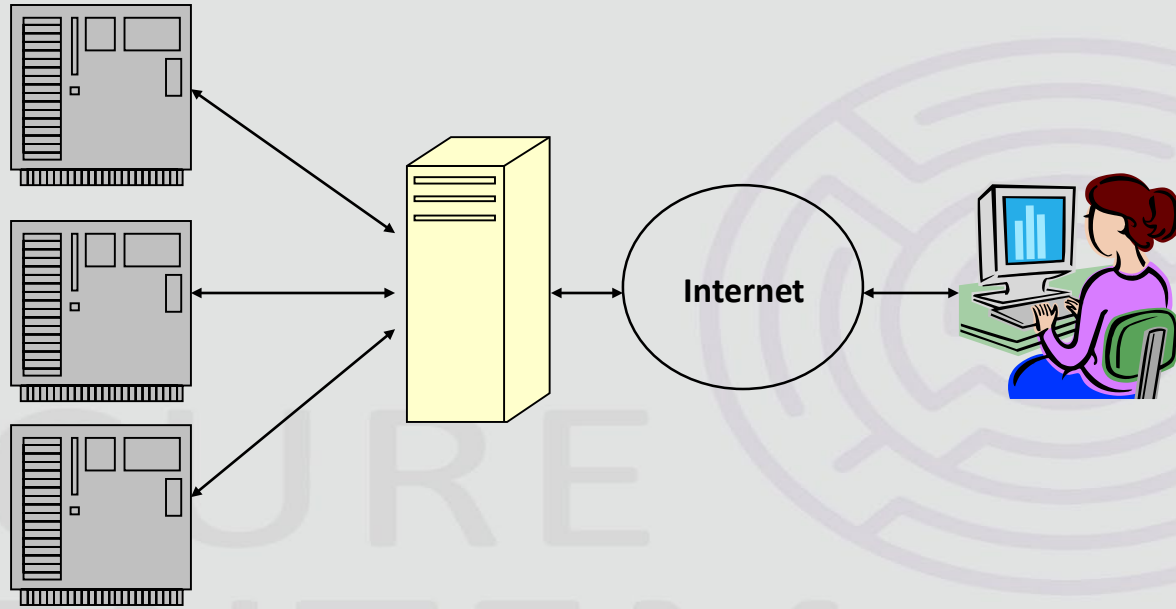
SECURE
MENTEM



The Migration



One Example: Power Capacity Sales



Even Worse

- Doesn't include:
 - Wireless
 - Rogue IT
 - Subcontract connections
 - Etc.

SECURE
MENTEM



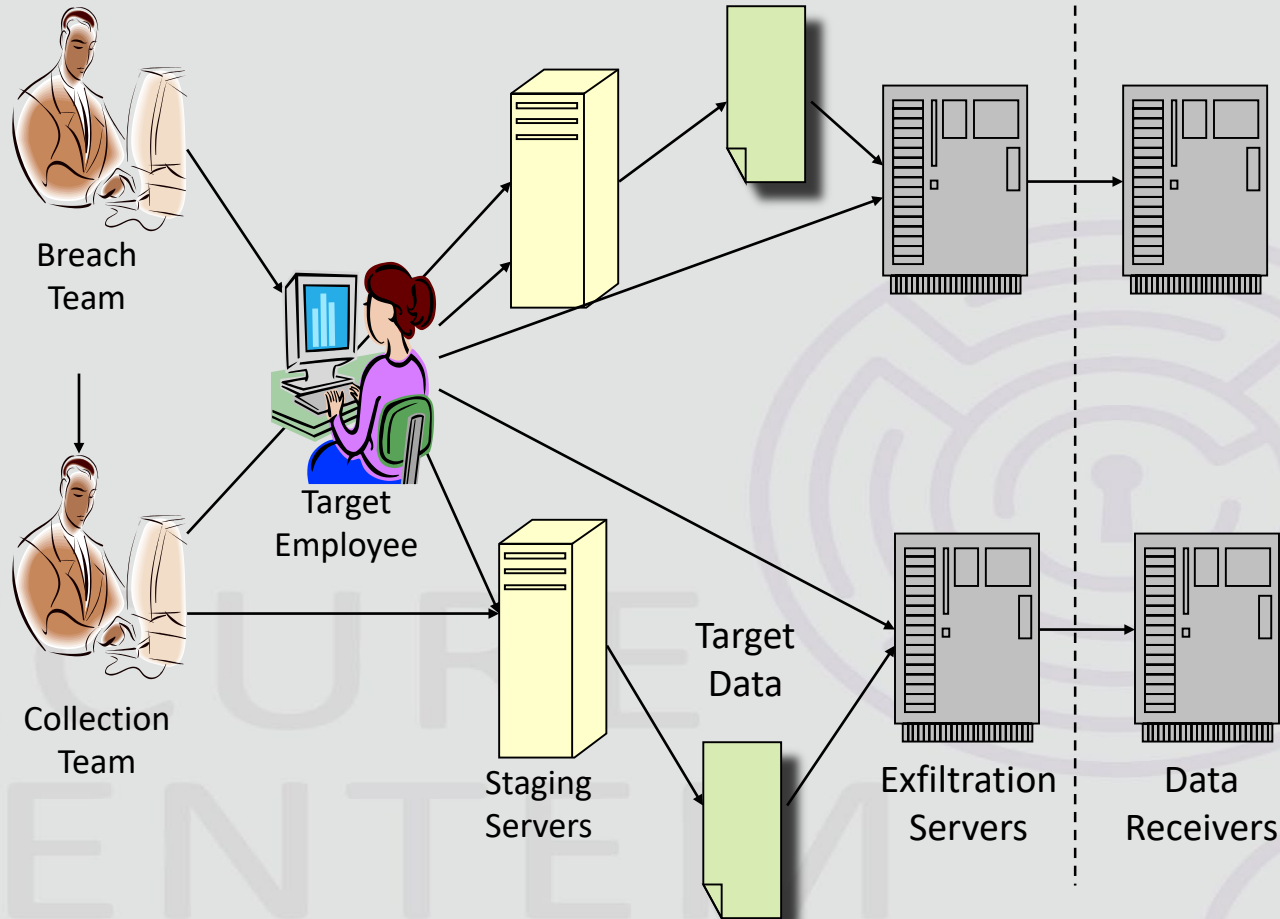
Once In

- Systems are frequently not patched
 - Wannacry for example
- Outdated systems
- Insecure configurations

SECURE
MENTEM



APT Compromise Methodology



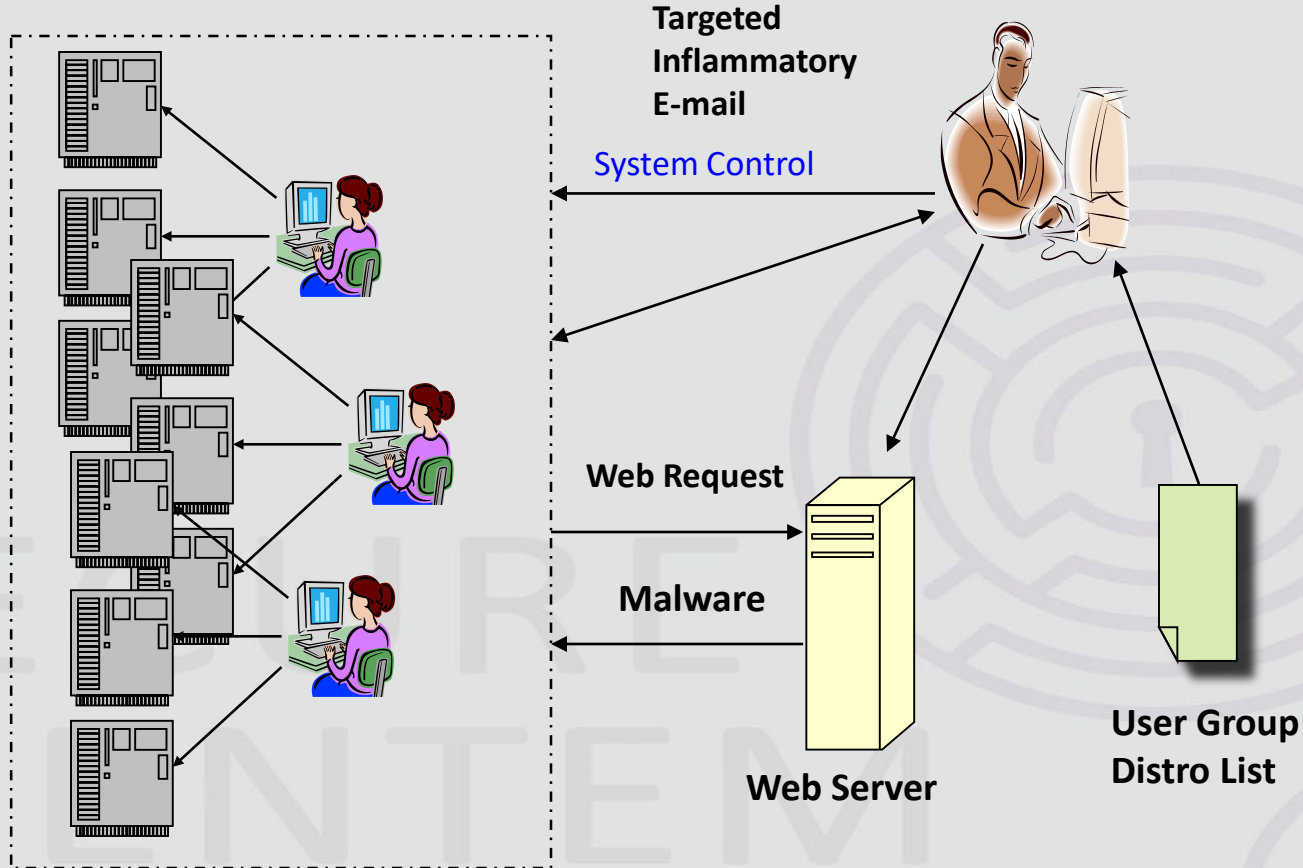
Similar Methodology for Malware

- Colonial Pipeline attack modified
- Generally only one team
- Network searched for maximum impact
- Just no infiltration of data...this time
 - Extortionware

SECURE
MENTEM



Power Grid Example



General Note

- My case study in 2008
- Siobhon Gorman reported Russia and China hacking US power grid in 2009
- Wired reported it as new on September 6, 2017
- New round of stories on March 15, 2018
- New round of stories in another 6 months
- BTW: Russia hacked Ukraine power grid in June 2017

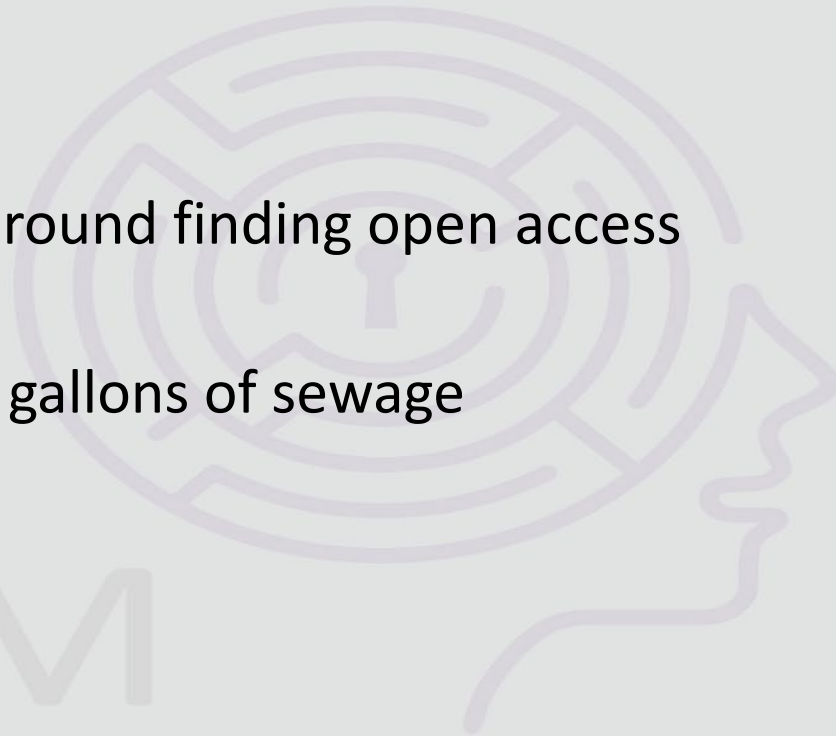
Uncontrolled Access Points

- Closed networks frequently have many access points
- Power grid has many points where diagnostic equipment can plug in
- Critical infrastructures are distributed and have many access points
 - Consider the Air Traffic Control System – radar, transmitters, airport operations, etc.
 - Water systems have controls throughout hundreds of miles
 - Telecom systems have access points all over

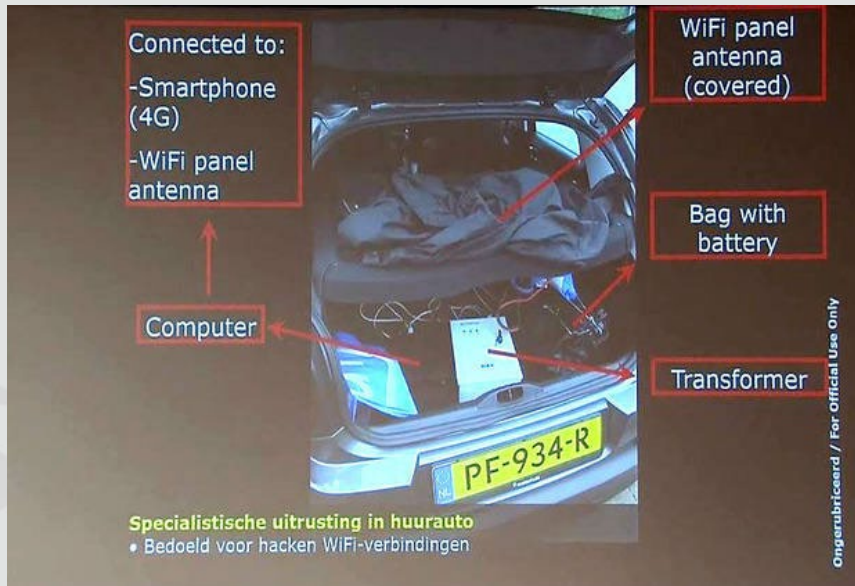
Maroochy Incident

- Vitek Boden worked for a contractor that installed radio controlled SCADA equipment
- Left under bad circumstances
- Stole radio equipment and drove around finding open access points to sewage system
- Released hundred of thousands of gallons of sewage

SECURE
MENTEM



Organization for the Prohibition of Chemical Weapons



- GRU operation to damage the investigation of Sergei Skripal attempted assassination
- Part of worldwide “brazen, close access cyber operations.” – British Ambassador Peter Williams

Diagnostic Equipment



- Can be specialized equipment
- Can be a PC
- Can be a USB device to put in updates
- Plugged into critical systems to perform diagnostics
- Connected to equipment through USB or other connectors

Worldwide Issue

- With naval vessels, they can be at all ports around the world
- Think about the thousands of people who have access to a naval base
 - Local contractors
 - Naval personnel
 - Defense contractors
- Not everyone is cleared
- Diagnostic equipment may not be treated as sensitive

Some Hacks Require Detailed Research

- Might need to know system configuration
 - Such as Stuxnet
- Might require hacking of contractors development facilities
- Might get from insiders
- Might get from documents available to maintenance personnel or elsewhere
- Some information might be available from open sources

Hacking the Developers

- With naval vessels, I mean defense contractors
- Su Bin group hacked 50 TB from 2008-2014
 - Included details of onboard computer systems
- BAE Systems hacked in 2009
- Lockheed Martin hacked in 2011
- Australian contractor reported hacked in 2017
 - F-35, C-130, and P-8 data hacked, along with 30GB of data about smart bombs and naval vessels
- If you can hack it out, you can put it in



SECRET

Compromise the Supply Chain

- Intercept equipment to plant malware/proactively sabotage recipient
- Equation Group supposedly doing it since early 2000s
- China accused of doing this
- Rice size chip for AWS and Apple
- Stuxnet likely delivered via equipment compromised prior to delivery
- Can be for initial delivery or periodic updates

Software Supply Chain Hacks

- SolarWinds
- Crypto wallets
- Most software is just a conglomeration of freeware
- Log4J

SECURE
MENTEM



Insiders

- Many potential insiders
- Insiders at developers
- Insiders on ships
- Insiders at repair facilities
- Insiders have planted time bombs and sabotaged operations elsewhere
- They've taken things out; little stops them from putting things in



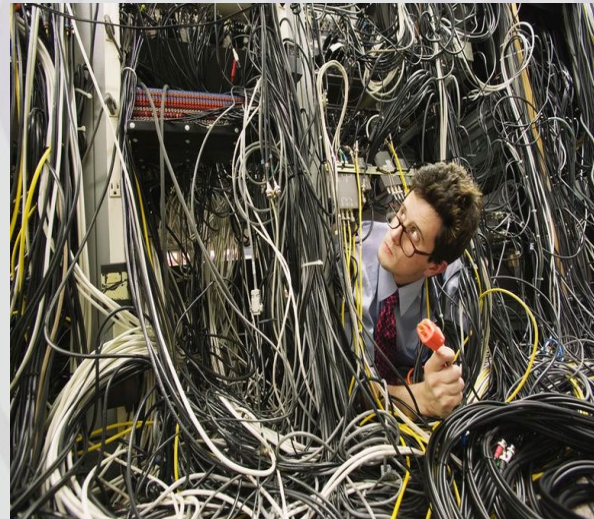
Black Bag Operations



- Outsiders infiltrate an organization
- Can be through pretexts
- Assumed identities
- Get jobs inside targeted organizations
 - Frequently through contractors
- When you don't have or trust insiders
 - Usually a last resort

Making Closed Networks Open

- A simple patch cable between network equipment
 - If equipment is co-located
 - Ships at sea now provide Internet for morale and other purposes
- Attaching routers to the network
 - Wireless or connected to a cellular/satellite device
 - A more permanent Maroochy
 - There are tools that look for rogue WiFi, so don't laugh
- Modems
 - Yes they still exist



Stuxnet Basics

- In theory, US and Israeli assets determined internal architecture
- Identified software in use
- Developed hack
- Created malware laden USB drives, or
- Compromised supply chain and delivered pre-infected equipment to contractor
- Dropped or delivered drives near developers
- Malware worked autonomously as designed
- Able to consistently upgrade attacks

So, Can You Hack a Naval Vessel?

- Yep, but admittedly complicated
- Stuxnet-like attack strategy
 - Probably autonomous attack
- Determine architecture
- Determine attack vectors
- Plant malware through supply chain, maintenance, or hacking
- Or, placing taps or inside sabotage



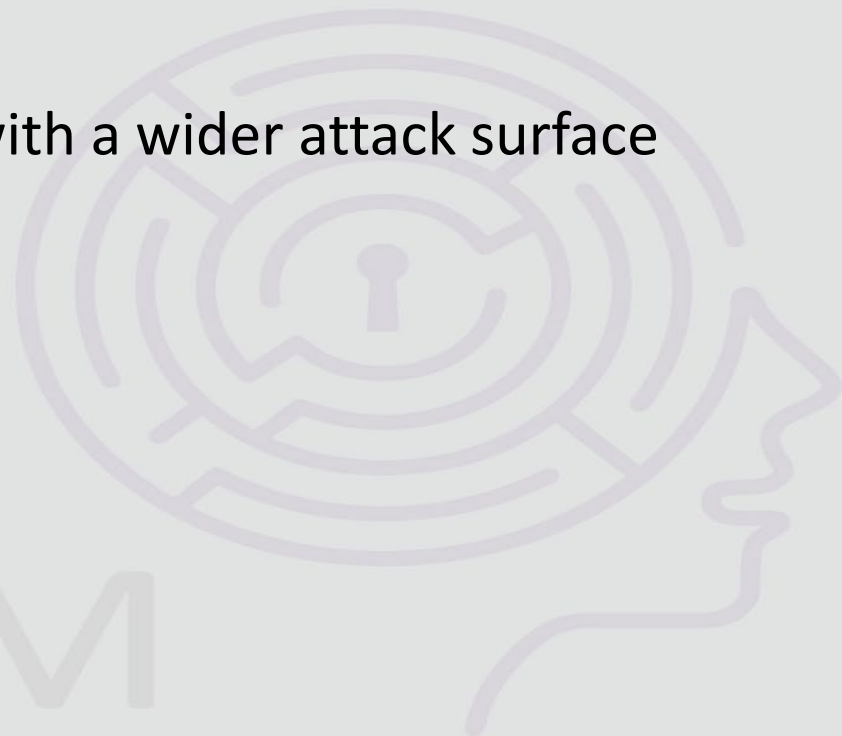
Disclaimer

- Of course, this attack is theoretical
- Similar attacks have been accomplished
- It is more complicated than described, but still possible
 - If anyone said you're going to regularly get malware in an underground Iranian facility, they would have been derided, probably like I will be
- To my terrorist followers, there's not enough here to launch the attacks

Hacking Open Networks Can Use Similar Techniques

- Supply chain, insiders, outsiders, network taps, etc. are still similar threats
- The attack vectors are the same, with a wider attack surface

SECURE
MENTEM



Stopping These Things



- Ignorance of the risk is the greatest threat
- Acknowledge the threat
 - Again, if it is valuable enough to cause the network to be closed, it is valuable enough for an outsider to target you
 - Everything is on the table
- Supply chain security
- Protection needs to be as tight as the most valuable open network
- Detection needs to be constant and pervasive
 - Assume technical and physical compromise

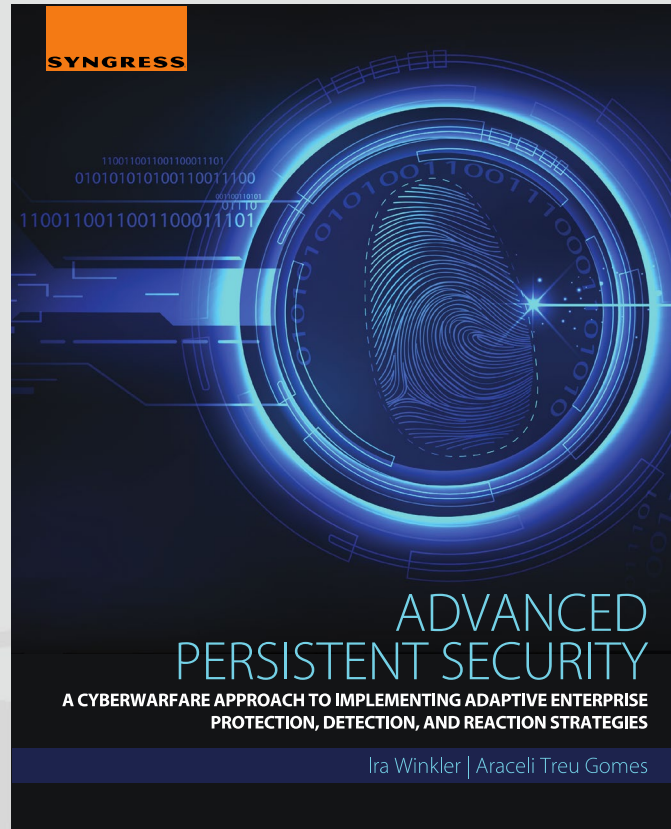
The Big Takeaway

- This can be done
- This has been done
- Saying such an attack is impossible is the greatest threat

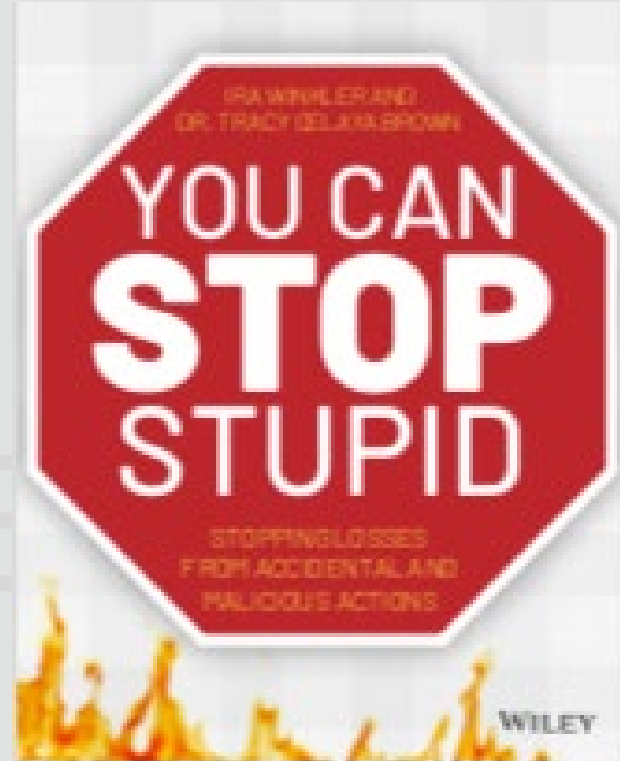
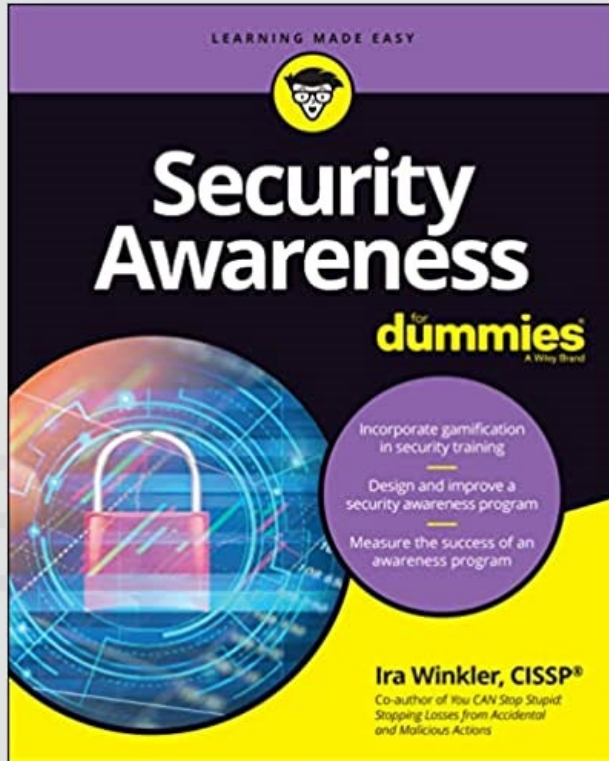
SECURE
MENTEM



The Book, The Myth, The Legend



The Next Legends?



For More Information

ira@securementem.com

+1-443-603-0200

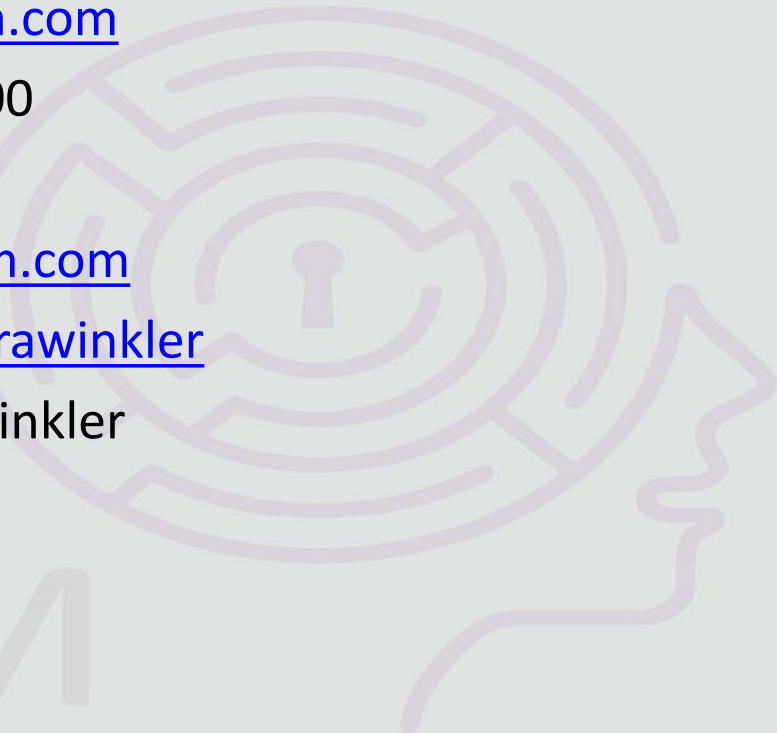
[@irawinkler](#)

www.securementem.com

www.linkedin.com/in/irawinkler

Facebook.com/irawinkler

SECURE
MENTEM





MIDWEST
RELIABILITY
ORGANIZATION

Geopolitical Tensions Overview and SAC

Brett Lawler, Senior Threat Intelligence Consultant, Xcel Energy

Jennifer Flandermeyer, Director, Federal Regulatory Affairs, Evergy

John Rhea, Vice President, Chief Ethics and Compliance Officer, Ameren

Tony Eddleman, Director of NERC Reliability Compliance, NPPD

CLARITY

ASSURANCE

RESULTS



Questions



MIDWEST
RELIABILITY
ORGANIZATION

Adversary Emulation in OT Environments

Ian Anderson | OGE Energy Corp

CLARITY

ASSURANCE

RESULTS

Agenda

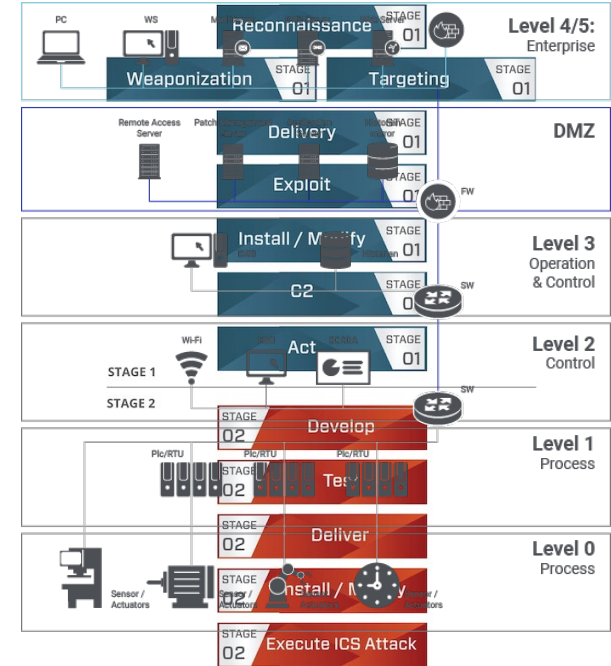
- **Why Adversary Emulation**
- **Operationalizing Adversary Emulation**
- **Adversary Emulation in OT**



Key Terms

- Cyber / ICS Kill Chain
- Purdue Model
- Access vs Impact

Figure 3: ICS Cyber Kill-Chain





What problem are we solving?



CLARITY

ASSURANCE

RESULTS

Application Security

[illegible]

A collage of various cybersecurity and network security logos, including AhnLab, Avecto, Avira, Bkav, Carbon Black, Check Point, Comodo, ESET, Fortinet, H3C, Huawei, ICSA, Inetec, Intel, Kaspersky, McAfee, MikroTik, NetScout, Palo Alto Networks, Panda, Sophos, Symantec, Trend Micro, and Zscaler.

Application Security Testing

ICS + OT

APERIO

BAYSHORE

BELDEN
SENDING ALL THE RIGHT SIGNALS

CLAROTY

CRITIFENCE

CyberX

CYBERBIT
PROTECTING A NEW DIMENSION

DRAGOS

endian

FIRMITAS

HALO ANALYTICS

Indegy

N-dimension solutions

NexDefense

NextNine

NOZOMI NETWORKS

PAS

PFP
CYBERSECURITY

radiflow

Rhebo

##SCADAfence

SECURITY MATTERS

sentryo

MSSP

Traditional MSSP

at&t, BAE SYSTEMS, EY, CenturyLink, Cisco Systems, CSC, IBM, Microsoft, nmap, OPTIV, Secureworks, Symantec

Advanced MSS & MDR

ADI, ARCTIC WOLF, CRITICAL OPERATICS, FireEye, RAPID7, UNISYS

Risk & Compliance

The collage features logos for various cybersecurity companies, organized into five categories:

- Risk Assessment & Visibility:** Includes logos for BitSight, Day Dynamics, Qaivion, Coaction, OBSERVER, CyberRisk, cyberark, and others.
- Security Ratings:** Includes logos for BitSight, Corax, FICO, and others.
- Pen Testing & Breach Simulation:** Includes logos for Cymulate, Ceph, and others.
- GRC:** Includes logos for algossec, Nixlog, Lockmatic, and others.
- Security Awareness & Training:** Includes logos for Baracuda, KnowBe4, and others.

Identity & Access Management

Digital Risk Management

QCE brandprotect. crisp digital shadows...
Digital Shadows | LOOKINGGLASS | NAMQOQO GADIUM
RISKIQ | Social SafeGuard | SOURCE | ZEROFOX

Security Consulting

Blockchain

Fraud & Transaction Security

AU10 TIX BIOCATCH BLOCK ERAUD Brighterion CARDINAL COMMERCIAL DATAVISOR EARLY WARNING emailage ethoca Ever Compliant FICO

Culture of Defense

- You want to do **WHAT** in my control system?
- Your OT Security journey started years ago
- Talent development
- What happens after boom?



Embracing Home Field Advantage

- What do attacks look like?
- What do attacks look like given our tooling?
- Can training replicate this?





**TOOL
MANAGEMENT**



**SECURITY
OUTREACH**



**TALENT
DEVELOPMENT**

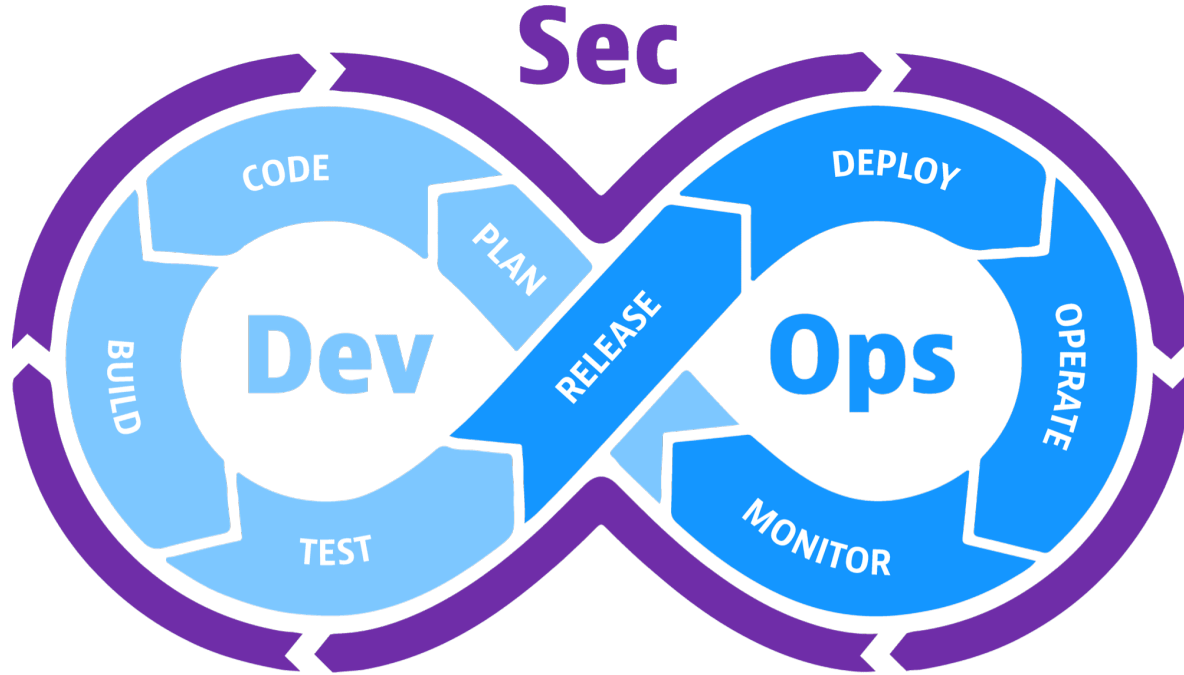
Operationalizing Adversary Emulation

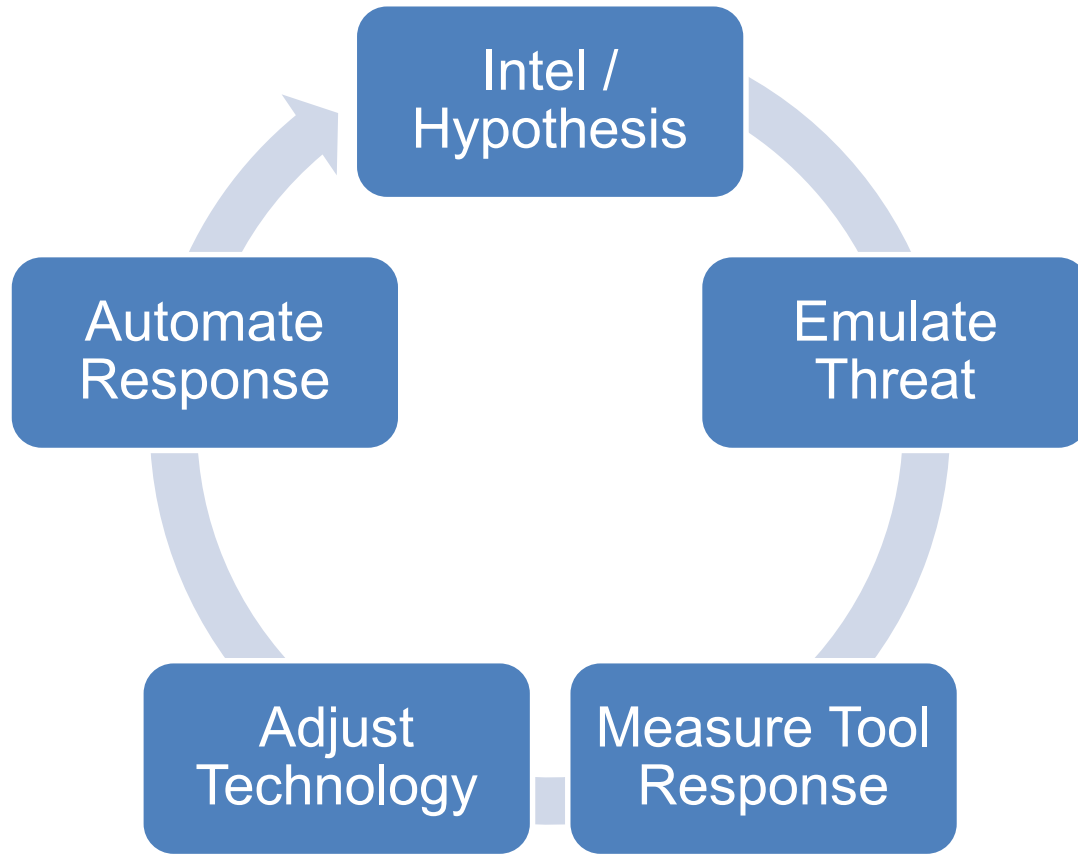


CLARITY

ASSURANCE

RESULTS





The Role of Threat Intelligence



CLARITY

ASSURANCE

RESULTS

Threat Intelligence

- **Measuring posture on risk/exposure**
- **Organizational assurance**
- **Reduce time-to-action on tuning**

Snake/EKANS Attack on Enel Group

According to open source reporting, the European energy company Enel Group, suffered a ransomware attack on June 7th that impacted its internal network. Indicators exist that illustrate that the attack was carried out by a group using the EKANS (SNAKE) ransomware that also targeted Honda on June 8th. Enel Group is an Italian multinational energy company that is active in the sectors of electricity generation and distribution, as well as in the distribution of natural gas. \r\n According to ThreatPost, SNAKE/EKANS was "first publicized in January after being discovered and analyzed by MalwareHunterTeam and reverse-engineer Vitali Kremez". The ransomware typically targets industrial control systems and thus attacks are centered on power grids, oil refineries, sewage treatment plants and factories that produce cars.\r\n Upon deployment, SNAKE will perform checks against internal domains and IP addresses to confirm that it is running in the correct network, including attempting to make...

Threat Intelligence in Action



run

cmd /c sc.exe config ekrn start= auto >nul 2>&1

21T20:15:39Z

technique:T1059']

False

Access is denied.



crypt

--target %USERPROFILE%\Desktop\x_all_the_stolen_files\ --password h3ll0w0rld

21T20:21:17Z

technique:T1560']

True

4100

Endpoint returned status: Success.



CLARITY

ASSURANCE

RESULTS

Threat Intelligence in Action

Incidents > Multi-stage incident on one endpoint



Multi-stage incident on one endpoint

[Summary](#) [Alerts \(4\)](#) [Devices \(1\)](#) [Users \(1\)](#) [Mailboxes \(0\)](#) [Investigations \(1\)](#) [Evidence and Response \(8\)](#) [Graph](#)

Alerts and categories

2/4 active alerts

1 MITRE ATT&CK tactics

1 other alert categories



© 2018 The MITRE Corporation. This work is reproduced and distributed with the permission of The MITRE Corporation.

- Sep 21, 2021, 3:14:55 PM | **Resolved**
A suspicious file was observed on
- Sep 21, 2021, 3:14:55 PM | **Resolved**
Suspicious sequence of exploration activities on
- Sep 21, 2021, 3:15:59 PM | **New**
Suspicious User Account Discovery on
- Sep 21, 2021, 3:16:31 PM | **New**
Suspicious System Network Configuration Discovery on

[View alerts](#)

Scope

1 impacted device

1 impacted user

Top impacted entities

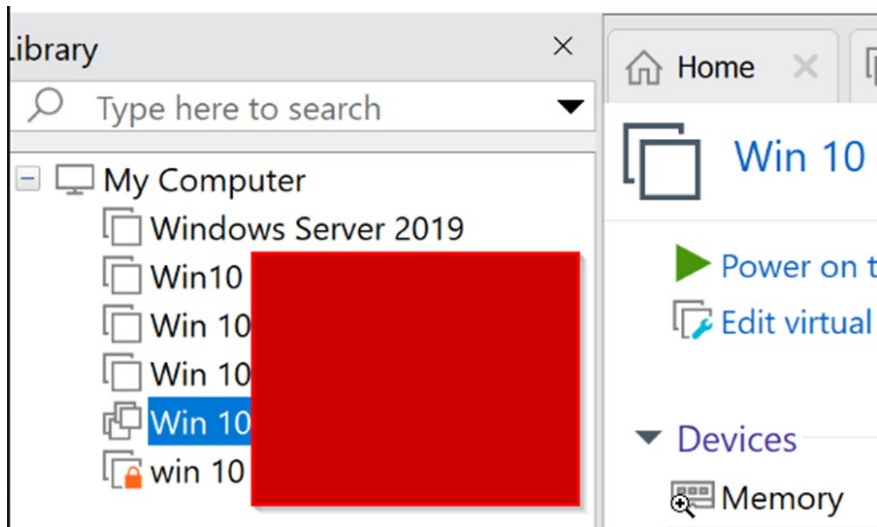
Entity type	Risk level/investigation priority
	■ Low
	No data available

[View entities](#) ▾

Evidence

8 entities found

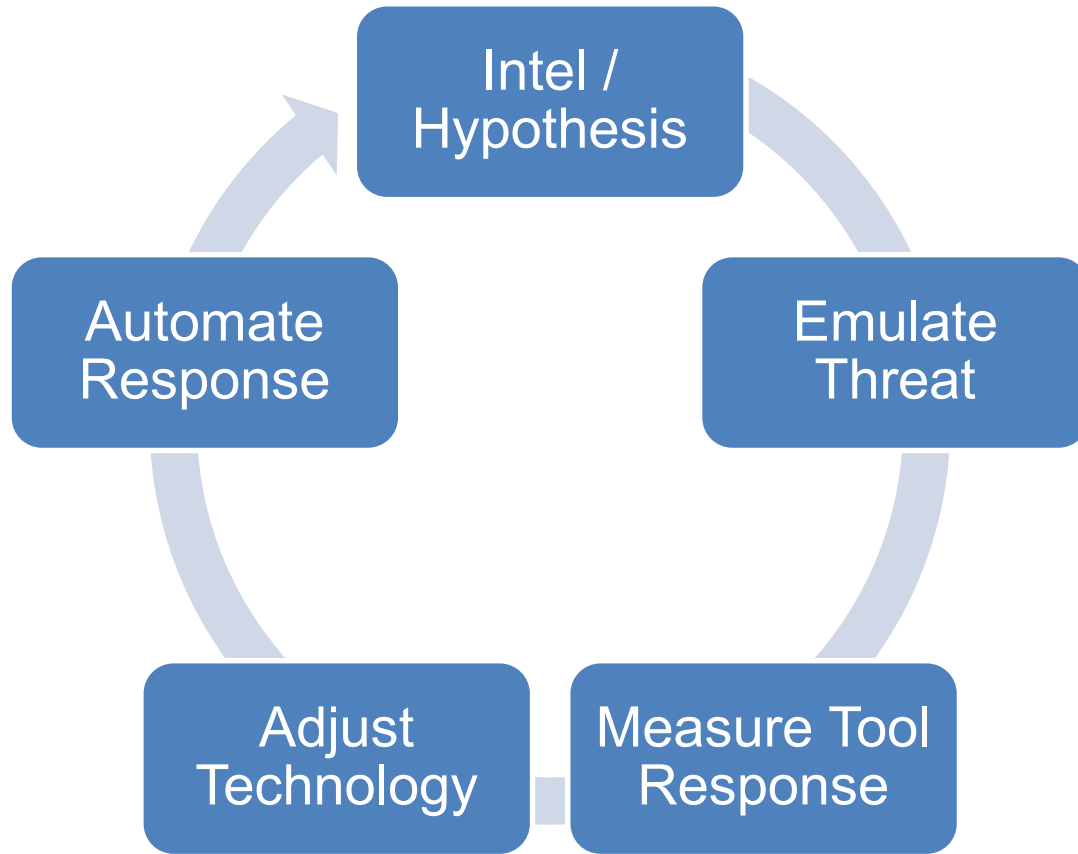
[View all entities](#)



CLARITY

ASSURANCE

RESULTS



Adversary Emulation in OT

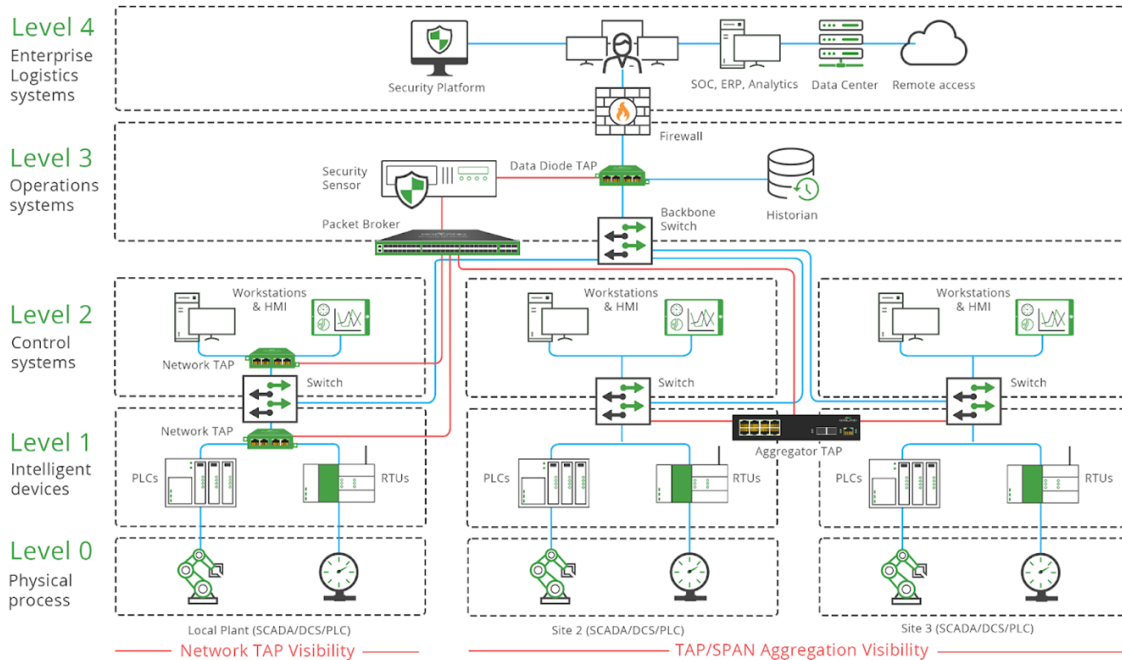


CLARITY

ASSURANCE

RESULTS

Defense in Depth



CLARITY

ASSURANCE

RESULTS

Adversary Perspective

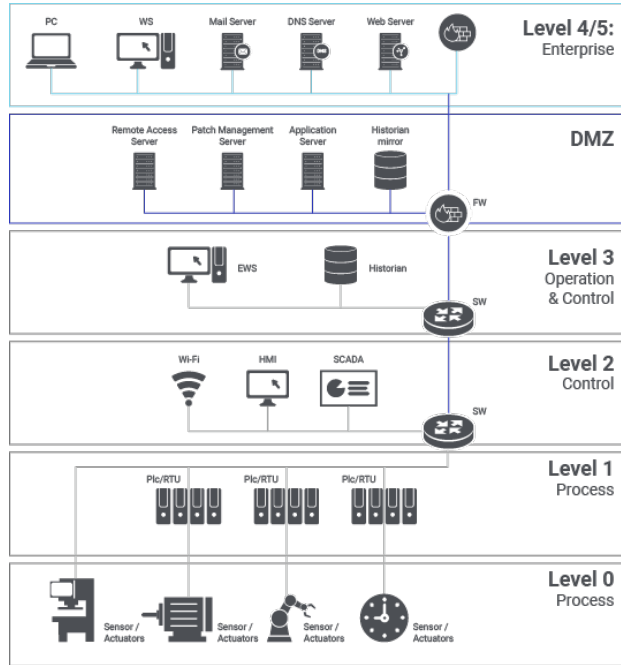
OT
(Levels 0/1)

Beachhead
(Levels 2/3)

IT
(Level 4)



Defender vs Adversary



IT
(Level 4)

Beachhead
(Levels 2/3)

OT
(Levels 0/1)



CLARITY

ASSURANCE

RESULTS

OT Access Operation



CLARITY

ASSURANCE

RESULTS

IT – Enterprise Machine Compromise

- **Planning**
 - Easiest vector to communicate to stakeholders
 - Conceptually high risk due to internet and end user exposure
 - Applications and remote access technologies in scope
- **Execution**
 - Assumed credential compromise / MFA compromise
 - Lessons from Oldsmar Water Treatment Facility attack
- **Findings**
 - Visibility improvement opportunities
 - Tool differences
 - System architecture improvements

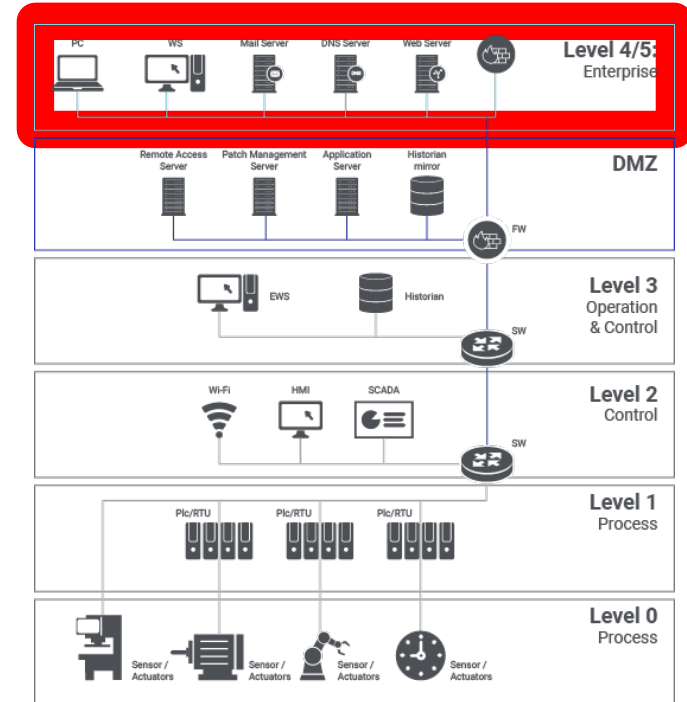
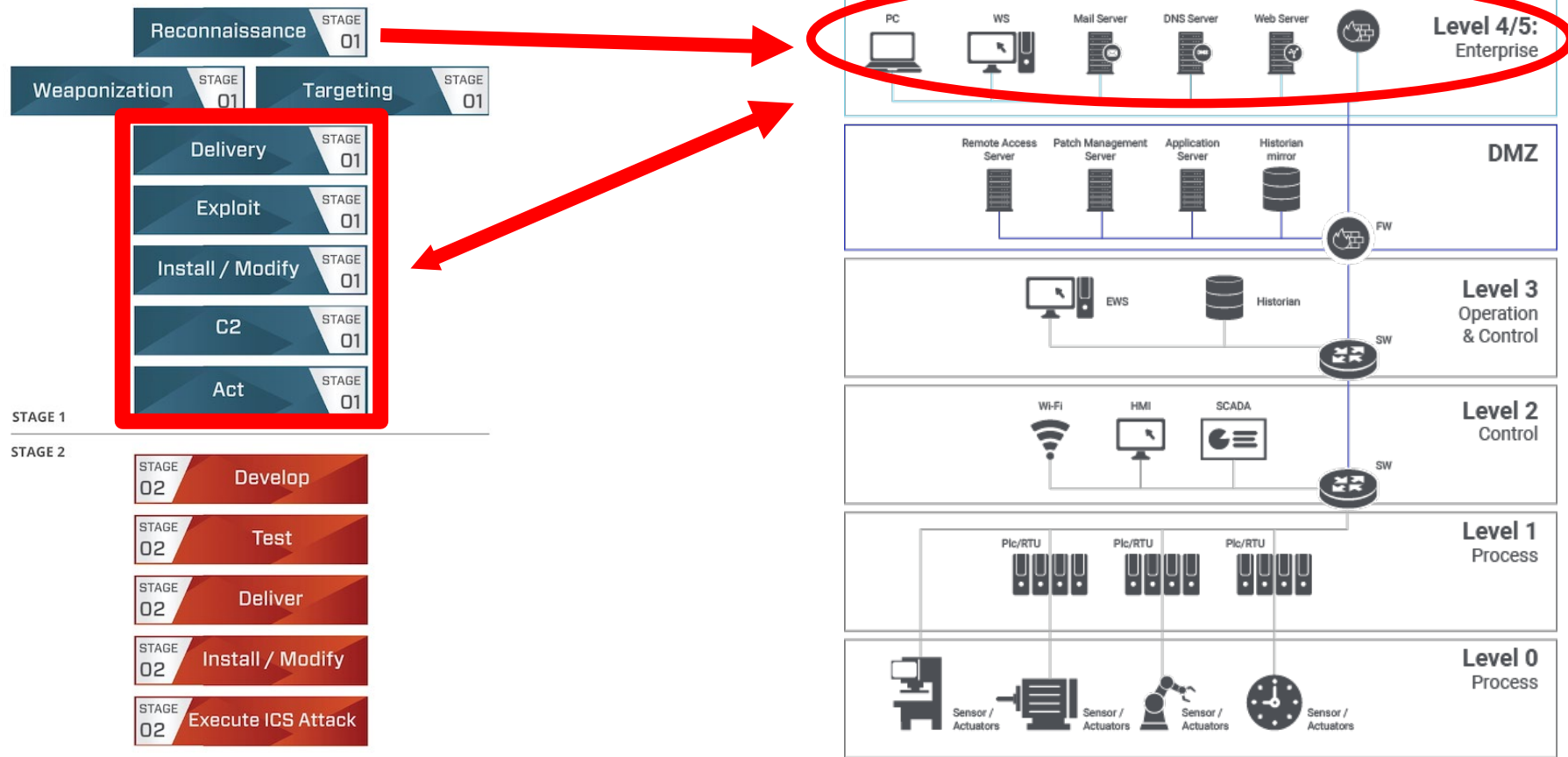


Figure 3: ICS Cyber Kill-Chain



OT Beachhead – Access Operation

- **Planning**
 - Bastion/Jump Server
 - Security tools with privileged access
 - Applications and remote access technologies in scope
 - Replication of adversary tactics from previous campaigns
- **Execution**
 - Leverage OSInt / Recon for pivoting
 - Groups named SCADA, DCS, HMI, etc
- **Findings**
 - Differentiating between normal and malicious
 - Response is greatly improved with strong relationships
 - ACL management is difficult and prone to error

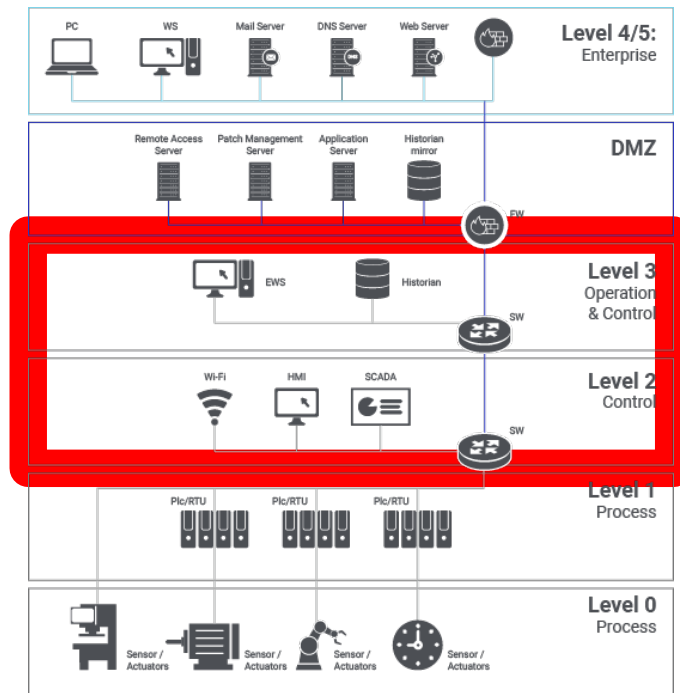
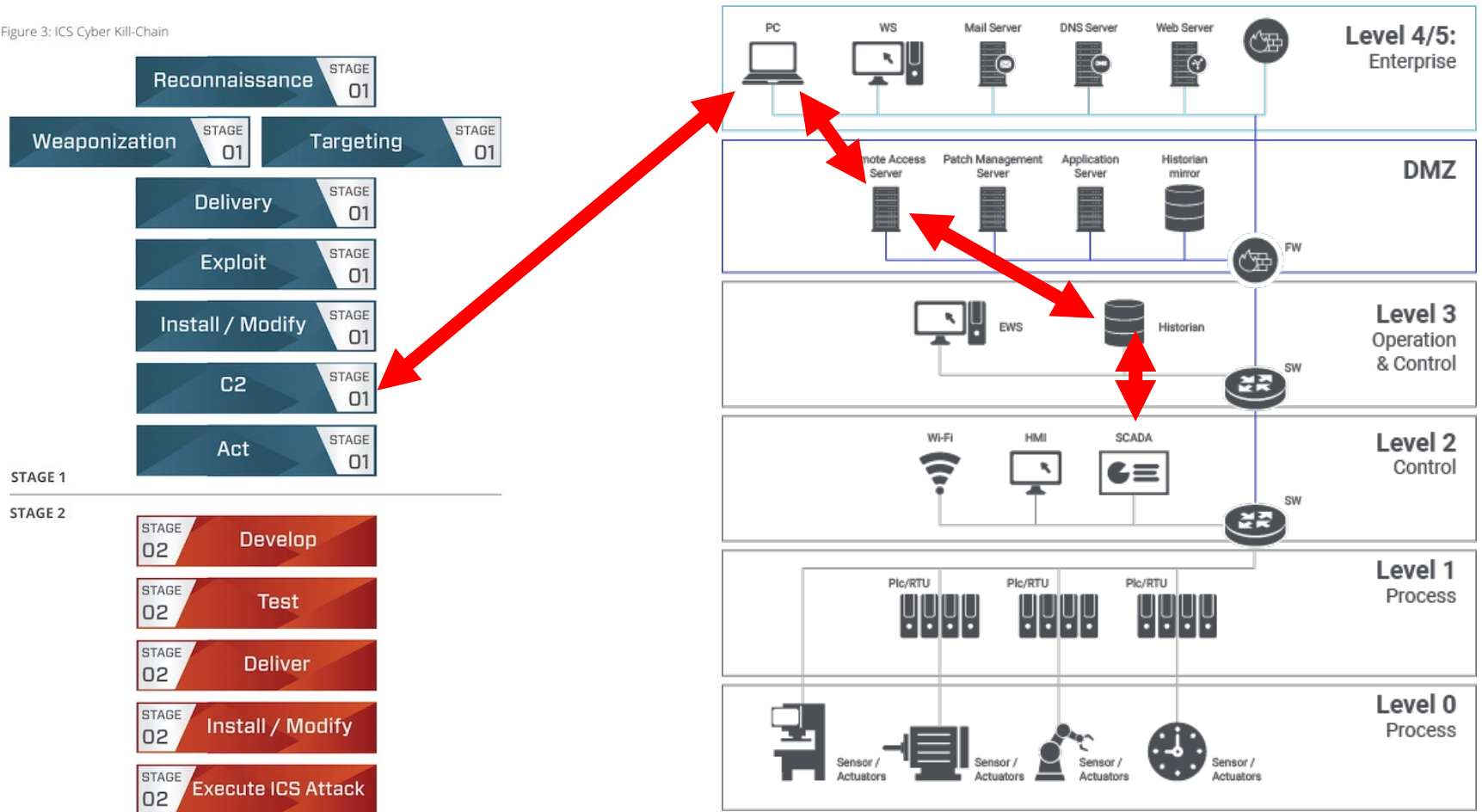


Figure 3: ICS Cyber Kill-Chain



Take Aways

- **The benefits of access operation emulations**
- **Preventing the adversary from reaching the beachhead is of utmost importance**



Conclusion / Questions? Time/Check



CLARITY

ASSURANCE

RESULTS

Bonus: Impact Operations in OT



CLARITY

ASSURANCE

RESULTS

OT - Impact Operation

- **Planning**
 - Access Operation
 - Impact Operation – requires an incredible amount of trust and coordination to do even in test environments.
- **Execution**
 - Desire the ability to emulate emerging threats like PIPEDREAM and Industroyer2
- **Measuring detection and prevention between beachhead and OT (access operations)**
- **Discovery and Lateral Movement**
- **Inhibit Response / Impair Process**

INITIAL ACCESS	EXECUTION	PERSISTENCE	PRIVILEGE ESCALATION	EVASION	DISCOVERY	LATERAL MOVEMENT	COLLECTION	COMMAND & 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 Information		Indicator Removal on Host	Remote System Discovery	Lateral Tool Transfer	Detect Operating Mode	Standard Application Layer Protocol	Block Command Message	Modify 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 via 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		

Figure 3: ICS Cyber Kill-Chain

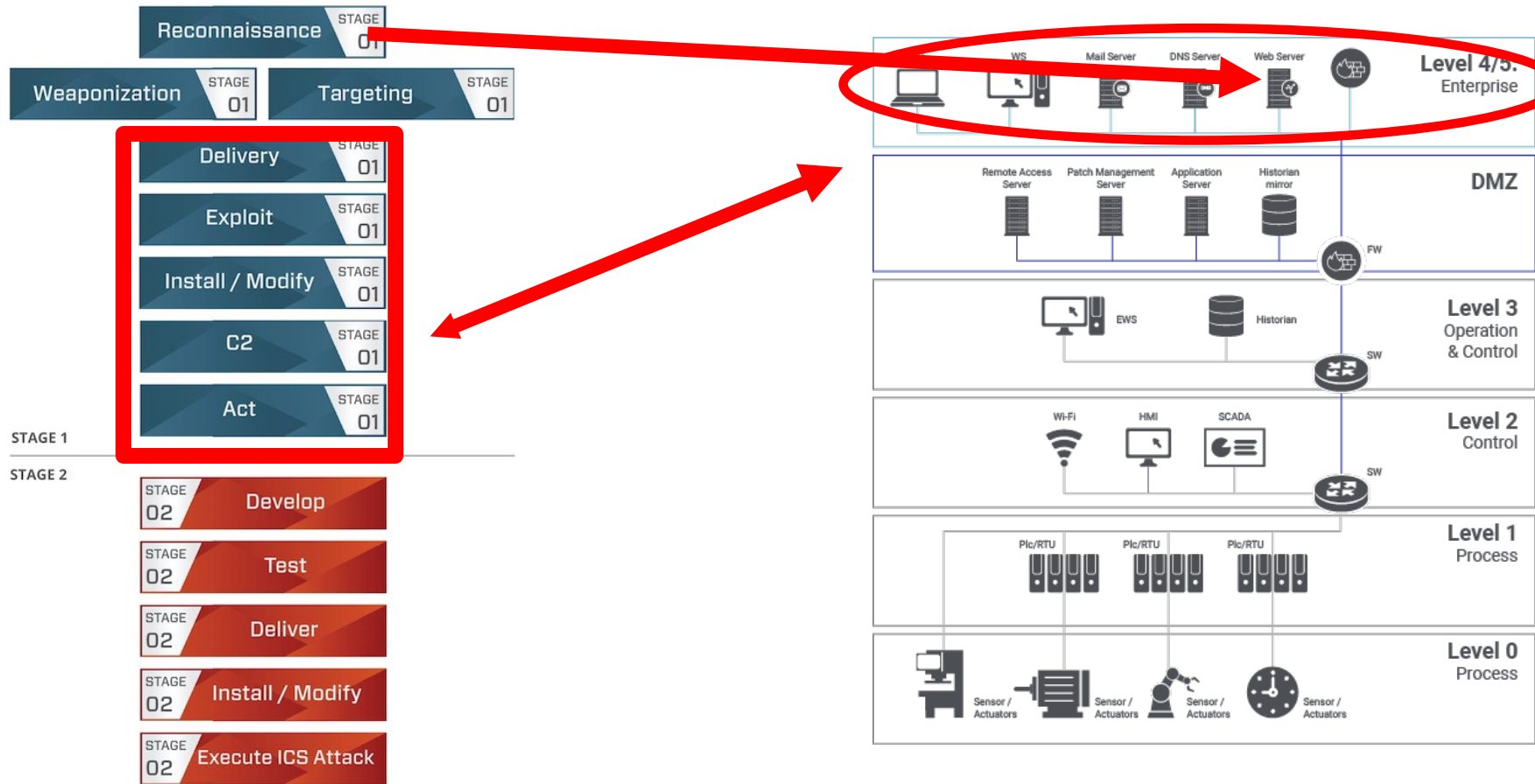
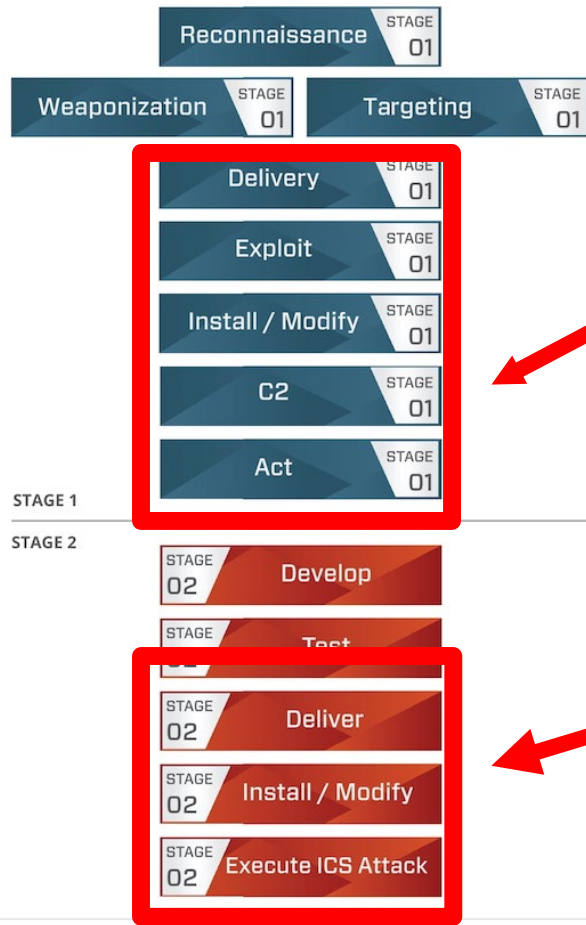
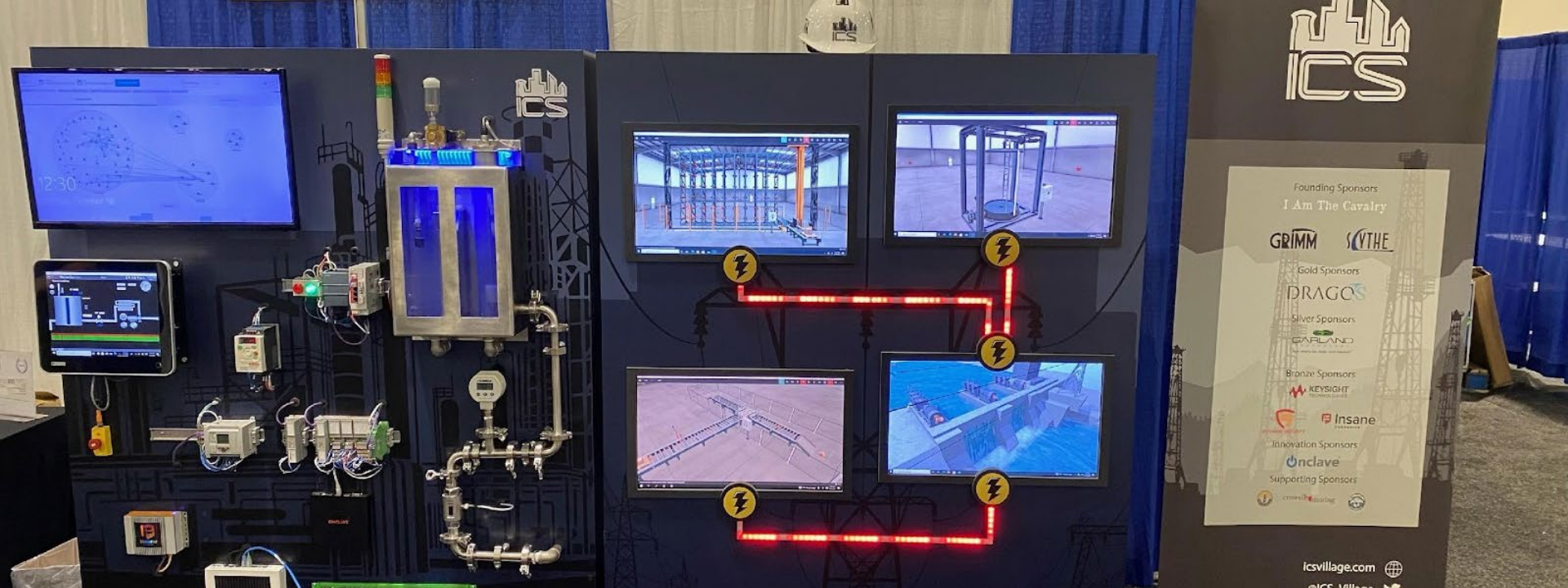


Figure 3: ICS Cyber Kill-Chain





Testing Impact Operations

Build a Lab

- Develop OT skills within security
- Develop security skills within OT ranks
- Break all the things!
- Make friends and have fun!



Portable PLC
(AB Compact)

Student Refer



PLC Motor Control

Objective 1: Describe Two Methods by Which a Controller Drives

PLC Motor

Direct Control

PLC Motor

Direct Control

PLC Motor

Direct Control

PLC Motor

Direct Control

PLC Motor

Direct Control

PLC Motor

Direct Control

PLC Motor

Direct Control

PLC Motor

Direct Control

PLC Motor

Direct Control

PLC Motor

Direct Control

PLC Motor

Direct Control

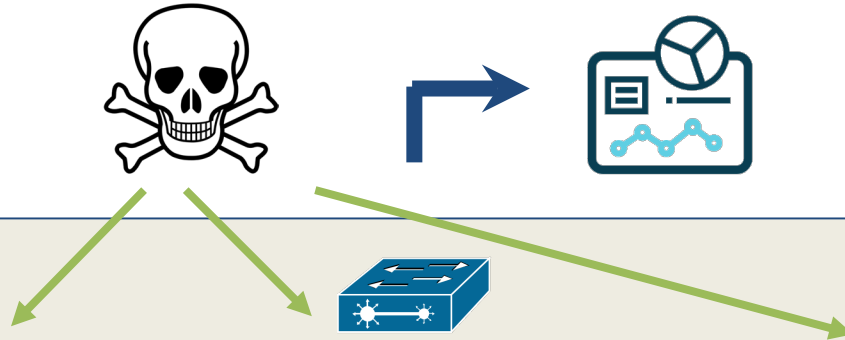
PLC Motor

Direct Control

Emulating OT Access Operations

- Network Sniffing
- Remote System Discovery and Remote System Information Discovery
- Is LOLBAS in play?

Level 1



DISCOVERY

Network
Connection
Enumeration

Network
Sniffing

Remote
System
Discovery

Remote
System
Information
Discovery



CLARITY

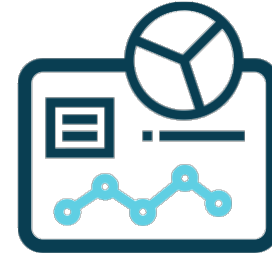
ASSURANCE

RESULTS

Emulating OT Impact Operations

- Inhibit/Impair Operations Testing
- Testing beyond normal IT protocols
- Evaluate OT security offerings and efficacy
 - PLC Pivoting
 - File Upload
 - Reading PLC Status

Isolated Lab Environment



IMPAIR
PROCESS
CONTROL

Brute Force
I/O

Modify
Parameter

Modify
Formware

Spoof
Reporting
Message

Unauthorized
Command
Message

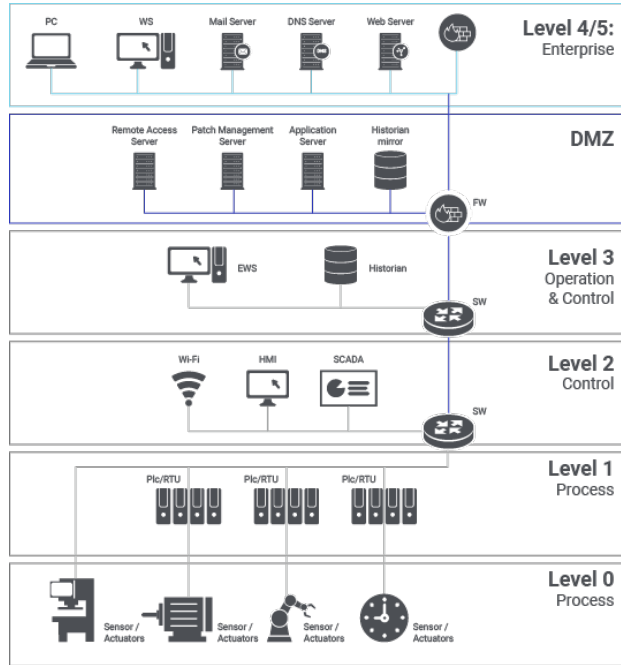


CLARITY

ASSURANCE

RESULTS

Defender vs Adversary



IT
(Level 4)

Beachhead
(Levels 2/3)

OT
(Levels 0/1)



CLARITY

ASSURANCE

RESULTS

Conclusion / Questions

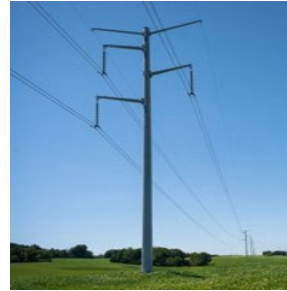


CLARITY

ASSURANCE

RESULTS

Physical Security Monitoring for Remote Locations



Norma Browne
nbrowne@ameren.com





Ameren Corporation is a Fortune 500 company & the parent company of:

- **Ameren Illinois:** ranks as Illinois' third largest natural gas distribution operation
 - **Ameren Missouri:** largest electric power provider in Missouri
 - **Ameren Transmission Company**
-
- Ameren employs more than 9,000 personnel.
 - We power the quality of life for:
 - 2.4 million electric customers
 - Over 900,000 natural gas customers
 - 64,000-square-mile service territory
 - Over 7,500 circuit miles of transmission lines
 - Generation of nearly 10,200 megawatts of electricity



Unique Challenges of Remote Monitoring

Some locations may have LAN

Some locations may have cell carrier signal

Some locations do not have 120ac power

Some locations not even have a building or shelter

Some locations may have site personnel

Some locations may not have a law enforcement response time less than three hours

Some locations may have ominous weather conditions

Some communities welcome you, others, well.... Maybe not

However, there is always a solution if there is justification & funding...

The Basics:

Know WHAT You Are Monitoring & What You Are Monitoring FOR

- What are we protecting?
- What are the unacceptable consequences of loss, unauthorized access or damage?
- What or who is the threat we are monitoring for?
- What are the possible threat vectors or mean of attack?
- Develop a DBT:
 - Reasonable
 - Attainable

The Basics: Monitoring is Not One Size Fits All

Develop a monitoring strategy which allows for an effective response to prevent, detect or interrupt the adversary to prevent unacceptable consequences of unauthorized access, loss or damage:

- To the assets
- To the project
- To site personnel
- To community life-safety
- To the environment
- To the Company's reputation
- To protect from criminal and civil litigation



Real-Time Electronic Monitoring

Perimeter Intrusion Detection Systems

- Require power and communication
- Access control systems monitored real-time by people
- Generates alarms
- Locally &/or remotely audible alerts
- Typically a “permanent” & more costly solution
- If designed to be easily relocated, may be risky:
 - Might be stolen
 - Likely wireless – easy to defeat
- Generally reliable, however the effectiveness is entirely dependent on response time and defense in depth or hardening for an off-site response to be effective
- Plan for back up power and back up communication if needed

Video surveillance monitoring with analytics or alerts

- Optical cams
- Thermal cams
- Monopole units
- Videofied
- Trail cameras with SIM cards

Other:

- Passive (or active) infrared
- Radar
- Fiber ground sensors
- Fiber fence sensors
- Microwave
- Programmable UAS

Real-Time Human Monitoring

Human Monitoring:

- Armed or unarmed patrols by personnel
- Security guards
- Guard patrols
- Random patrols from on-duty law enforcement
- Hire-back of off-duty law enforcement
- Personnel-operated UAS
- Video systems without analytics
- Motion sensitive lighting
- Triggered/audible alerts
- Guard-dog handlers
- Subject to fatigue
- Can only be in one place at a time
- May not be terribly motivated
- Subject to human failure
- May require two or more
- May be your threat...

Monitoring After the Fact

If interruption of the unacceptable consequences is not desired or is not attainable - yet:

Documentation of unauthorized access, damage and thefts may help you develop a strong business case to add or take additional measures. *They always come back.*

- Breaches in protective barriers
- Breached hardened storage
- Smart locks – the core cannot be use to obtain hard keys or internet 3D keys
- Recorded video surveillance (for evidentiary purposes)
- Motivation in remote areas may result in a smaller pool of suspects, e.g. known thieves, radical environmentalists.
- Photos and video may provide great results if the adversary is known



TEST! Rinse & Repeat

- Test your DBT
- Test your physical hardening, protection, and monitoring to the point of failure (yes test your procedures, humans & response time too)
- Add additional hardening or monitoring measures as necessary to achieve the required level of protection
- The monitoring/system costs will be commensurate to the threat. The cost should NOT be a factor if monitoring protection is truly required and is effective to prevent the unacceptable consequences.
- Sleep well, you did a great job



MIDWEST
RELIABILITY
ORGANIZATION

Energy Availability and Renewable Resources

2022 MRO Security Conference

CLARITY

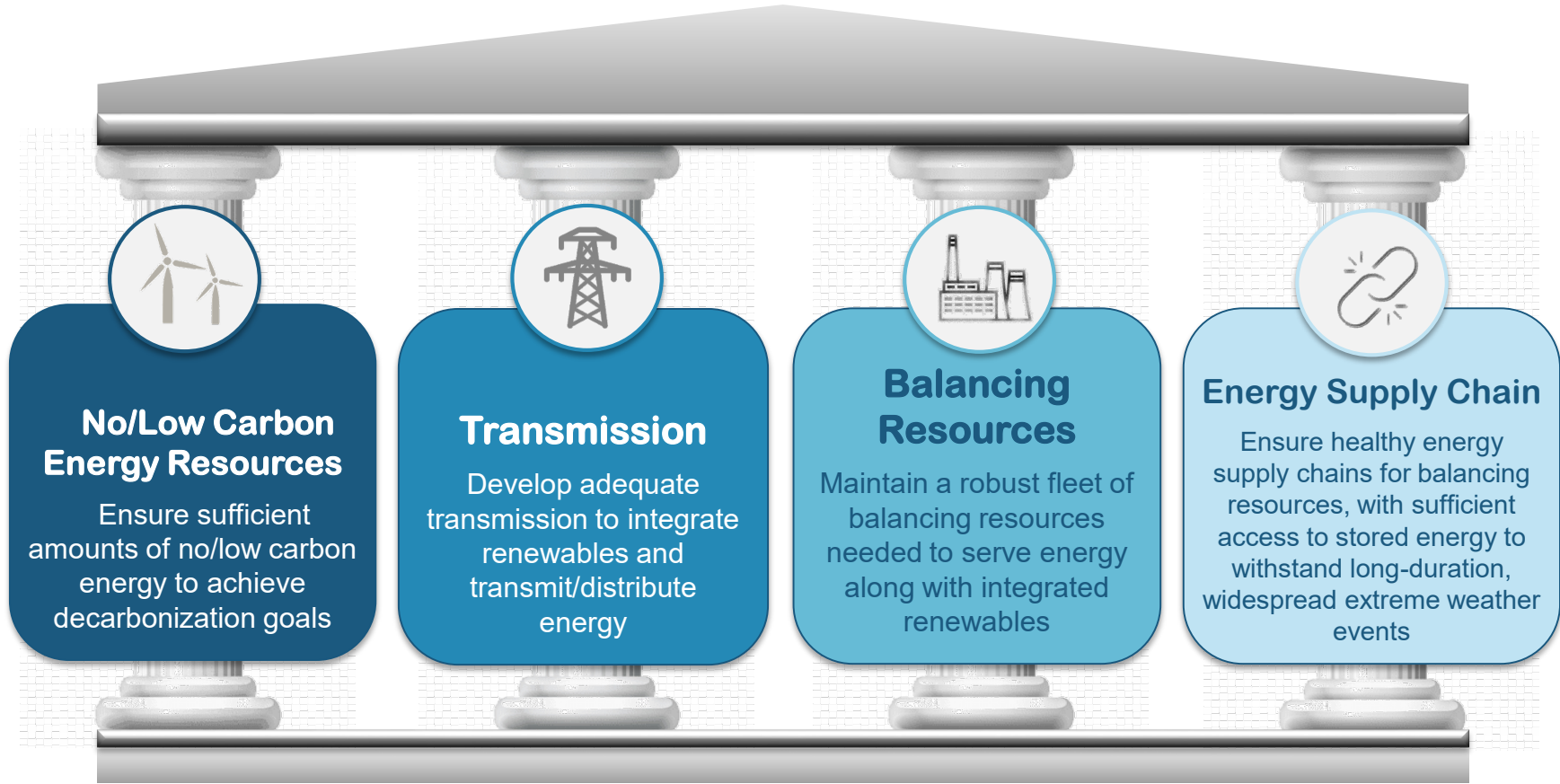
ASSURANCE

RESULTS

Energy Transition Underway

- **The following drivers have led to rapid changes in energy resources:**
 - Governmental policies
 - Changes in resource economics
 - Consumer demand for clean energy
- **In addition to the shift in resources, an increase in extreme weather presents new challenges**
 - Fuel sources are inherently less secure





Four Pillars of the Energy Transition

The Challenge: Sufficient Energy Availability

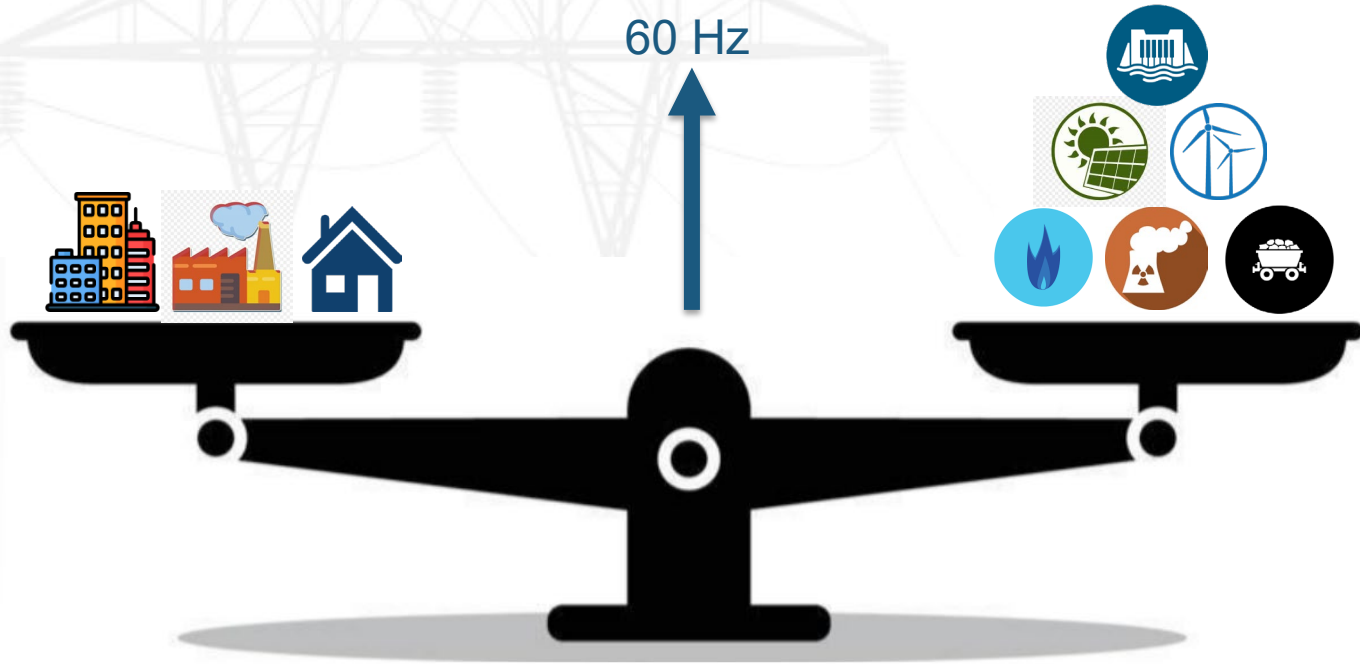


CLARITY

ASSURANCE

RESULTS

Electric Demand vs Supply

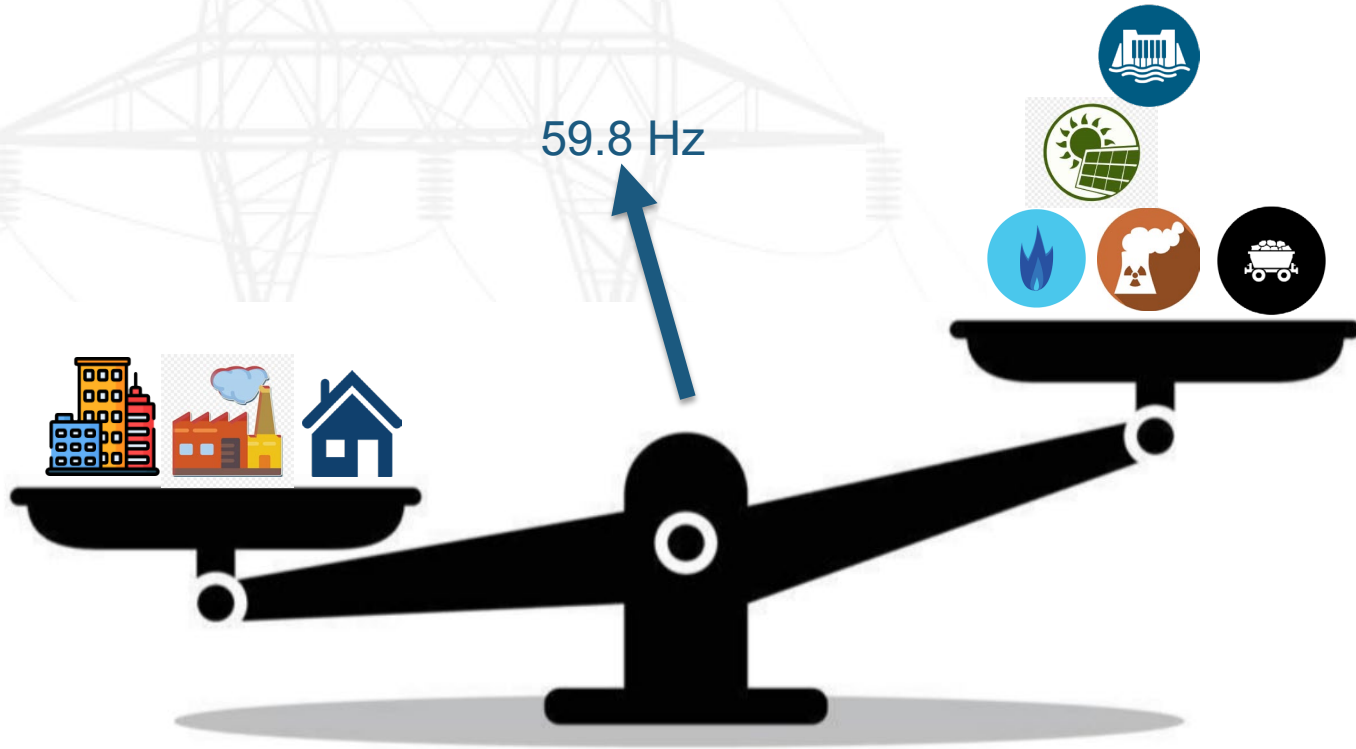


CLARITY

ASSURANCE

RESULTS

Electric Supply vs Demand



CLARITY

ASSURANCE

RESULTS

The Challenge: Sufficient Energy Availability

- Power grid transition is resulting in a higher level of energy uncertainty, regardless of fuel type
 - The current tools, rules of thumb, and approaches used to determine the system's ability to meet demand were not designed for today's grid
- The focus needs not be on fuel type, but rather on *energy availability*

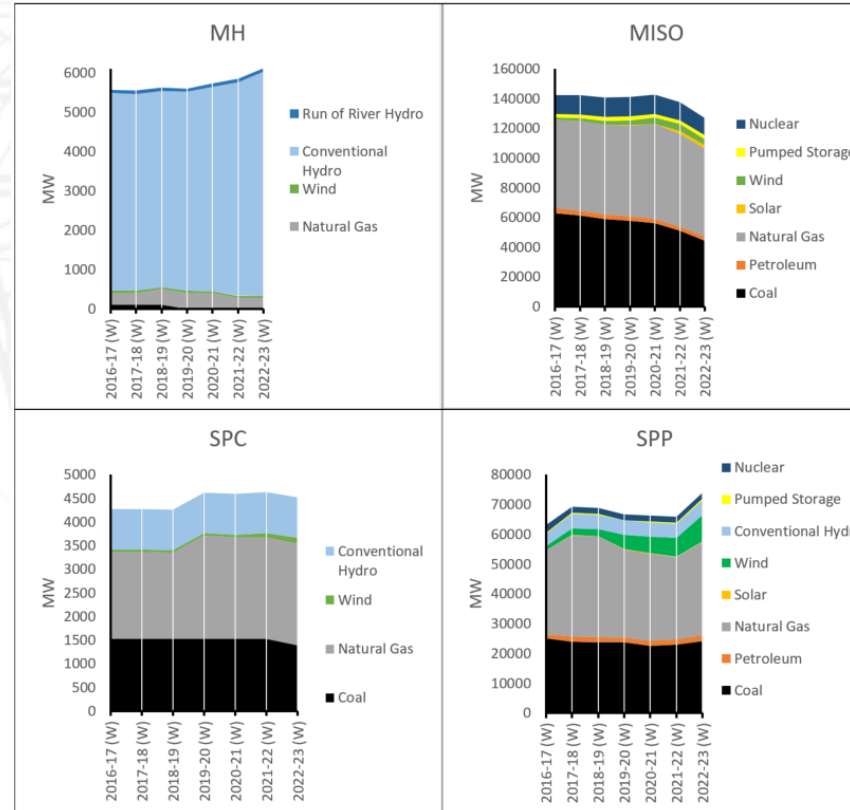




- **Rapidly changing generation fleet**
- **Increasing electrification**
- **Widespread, long-duration, extreme weather events**
- **Historically, industry ensured energy through capacity and reserve margins with assurance of fuel**

Considerations in Solving This Challenge

Regional Generation Changes

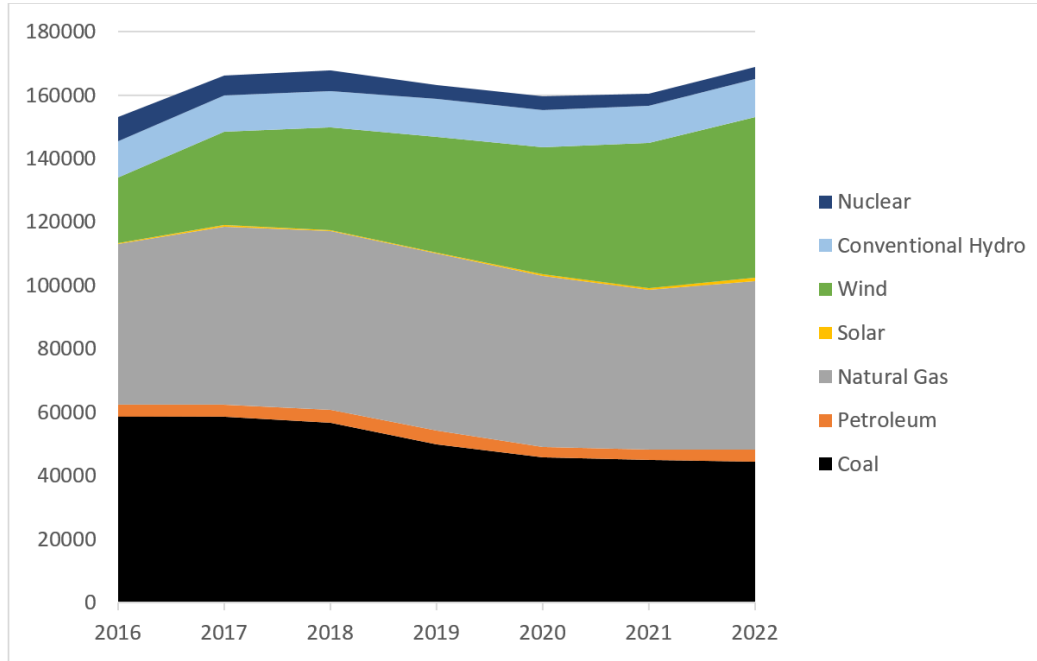


CLARITY

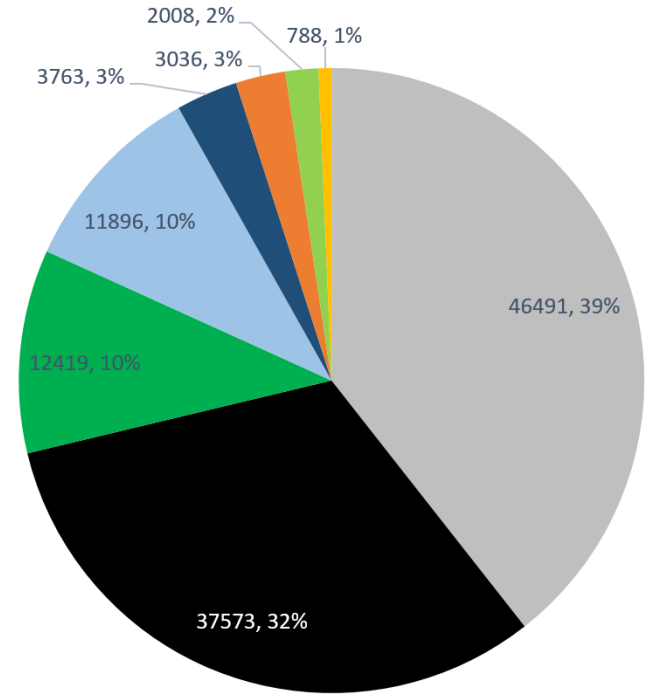
ASSURANCE

RESULTS

MRO Nameplate vs. Capacity



Nameplate



Capacity



CLARITY

ASSURANCE

RESULTS

ERO Capacity vs. Load

NERC
NORTH AMERICAN ELECTRIC
RELIABILITY CORPORATION

2022 State of Reliability

July 2022



An Assessment of 2021
Bulk Power System
Performance

Table 3.2: Generation Resource Capacity by Fuel Type

Generation Fuel Type	2011 On-Peak		2021 On-Peak	
	GW	Percent	GW	Percent
Coal	318.5	30.5%	219.8	21.4%
Natural Gas	385.9	36.9%	462.9	45.0%
Hydro	153.9	14.7%	132.6	12.9%
Nuclear	111.6	10.7%	107.7	10.5%
Oil	50.3	4.8%	39.6	3.8%
Wind	13.7	1.3%	25.4	2.5%
Solar PV	0.5	0.1%	25.7	2.5%
Other	10.0	1.0%	15.0	1.5%
Total:	1,044.5	100.0%	1,028.7	100.0%

2021 installed wind
nameplate = 138 GW

2021 installed solar
nameplate = 41 GW

Yet accredited wind
and solar capacity at
peak load is 51 GW (or
2.5% of total resource
capacity).

Total capacity has dropped by 16 GW from
2011 to 2021, however load has increased
by about 85 GW.



CLARITY

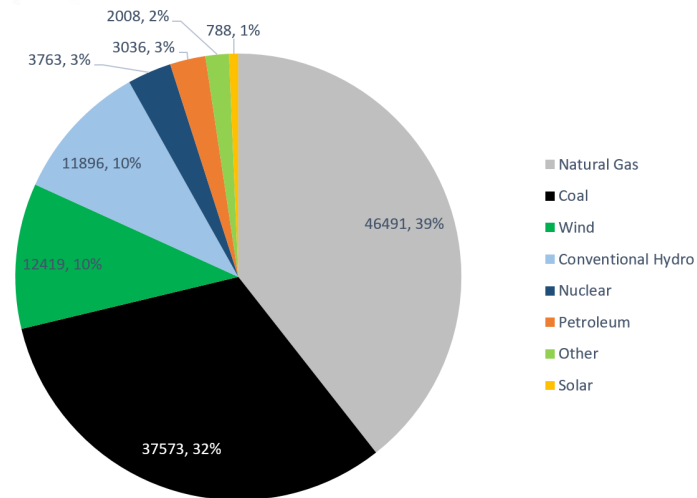
ASSURANCE

RESULTS

Capacity ≠ Energy

- Across North America, from 2011-2021:
 - Load has grown 85 GW while CAPACITY has dropped by 16 GW
 - 2021 Wind Capacity was 2.5% of total (10% in wind-heavy MRO)

Area	2020-21 Winter Nameplate (MW)	2021-22 Winter Nameplate (MW)	2021-22 Winter Peak Capacity (MW)
MH	259	259	52
MISO (MRO)	26,064	28,447	4,561
SPC	241	627	85
SPP	23,546	27,535	6,334



CLARITY

ASSURANCE

RESULTS

Influx of Solar is Coming to MRO

Solar and Wind Nameplate Capacity, Existing and Planned Additions through 2031

Assessment Area	Nameplate MW of Solar					Nameplate MW of Wind				
	Existing	Tier 1	Tier 2	Tier 3	Total	Existing	Tier 1	Tier 2	Tier 3	Total
MISO	728	10,989	53,756	4,907	70,380	22,854	5,593	14,649	730	43,826
MH	0	0	0	0	0	259	0	0	0	259
SPC	2	10	10	57	79	242	385	200	100	927
SPP	278	444	32,170	149	33,041	27,535	4,604	16,892	0	49,031
Total	1,008	11,443	85,936	5,113	103,500	50,890	10,582	31,741	830	94,043

Existing Solar
1,008 MW

Queued Solar: 102,492 MW

Existing Wind
50,890 MW

Future Wind: 43,153



CLARITY

ASSURANCE

RESULTS

North America Planned Resource Mix

2021 Long-Term Reliability Assessment

December 2021

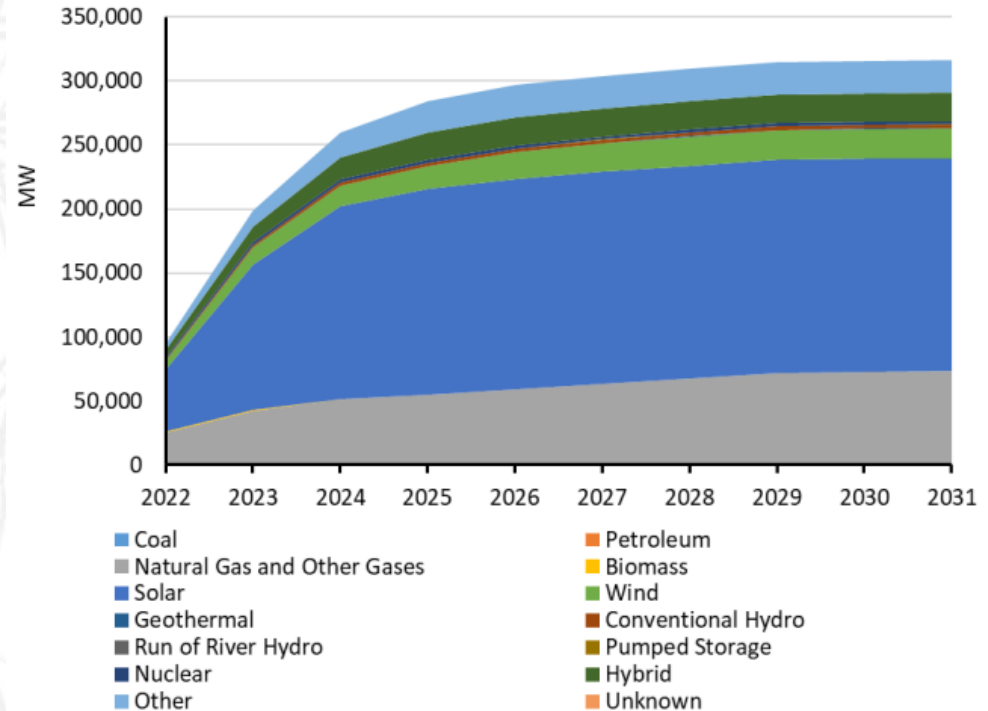


Figure 13: Tier 1 and 2 Planned Resources Projected Through 2031



CLARITY

ASSURANCE

RESULTS



CLARITY

ASSURANCE

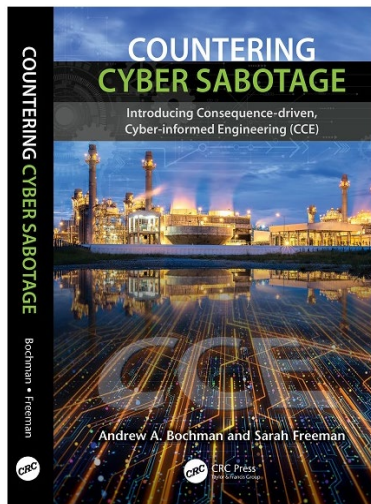
RESULTS



Andy Bochman
Grid Strategist-Defender

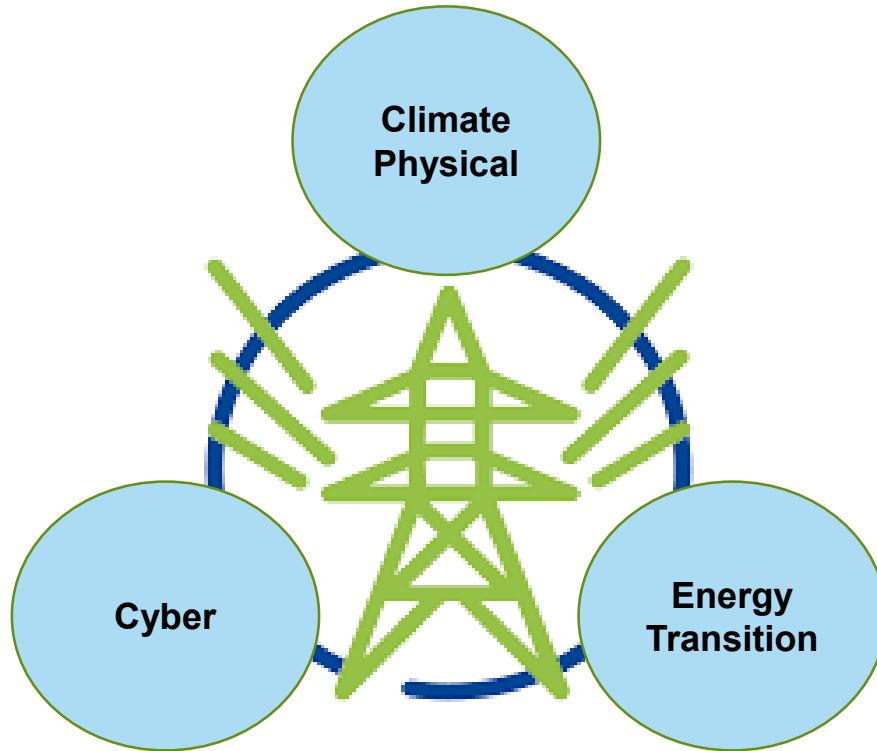
Physical Security 2.0

Infrastructure Cyber → Cyber & Climate Resilience

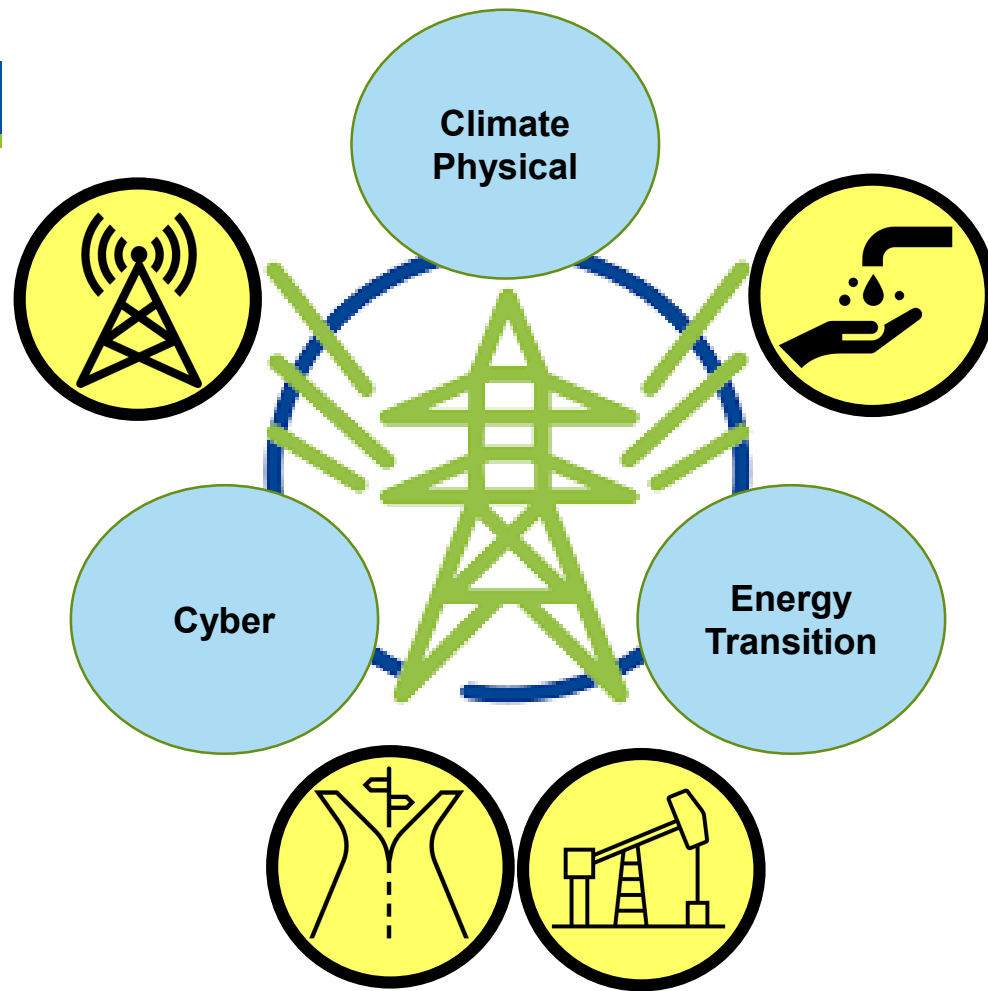


Not Your Grandfather's Physical Security





Mounting Inter-related Threats to Electric Utilities in 2022



Interdependencies Extend Beyond Each Utility's Boundaries:

- Communications
- Water
- Transportation
- Fuels

The Wall Street Journal / July 2022



How Extreme Heat Is Disrupting the Global Economy

Rising global temperatures and heat waves have an effect on everything from transportation infrastructure to supply chains to power generation

By Benoît Morenne

JULY 27, 2022

TAP STORY >

<https://www.wsj.com/story/how-extreme-heat-is-disrupting-the-global-economy-2a1af974>

IDAHO NATIONAL LABORATORY



Disruptive and Destructive Impacts on Infrastructure are Accelerating

**Arriving faster than tradition
infrastructure planning cycles can
handle:**

- Too much heat
- Too little heat (unexpected freezes)
- Too much water (floods, SLR)
- Not enough water (drought)
- Storms with higher velocity winds
- Melting permafrost

Context: Priority Adaptation Actions



2021 Climate Adaptation and Resilience Plan



Report to the White House
National Climate Task Force and
Federal Chief Sustainability Officer
August 2021

1. Assess Vulnerabilities and Implement Resilience Solutions at DOE Sites
2. Enhance Climate Adaptation and Mitigation at DOE Sites
3. Institutionalize Climate Adaptation and Resilience in Policies and Processes
4. Provide Climate Adaptation Tools, Technical Support, and Climate Science Information
5. Advance Deployment of Emerging Climate Technologies

Self Assessments at Every DOE Site

- Identify Critical Assets and Infrastructure
- Characterize Current and Projected Impacts of Climate Change Hazards on Assets and Infrastructure Systems
- Identify and Assess Resilience Solutions
- Develop and Implement a Portfolio of Resilience Solutions

VULNERABILITY ASSESSMENT AND RESILIENCE PLANNING GUIDANCE

This guidance outlines a climate change vulnerability assessment and resilience planning process to help the Department of Energy assess and manage climate change related risks to Departmental assets and operations.

*U.S. Department of
Energy,
Sustainability
Performance
Division*

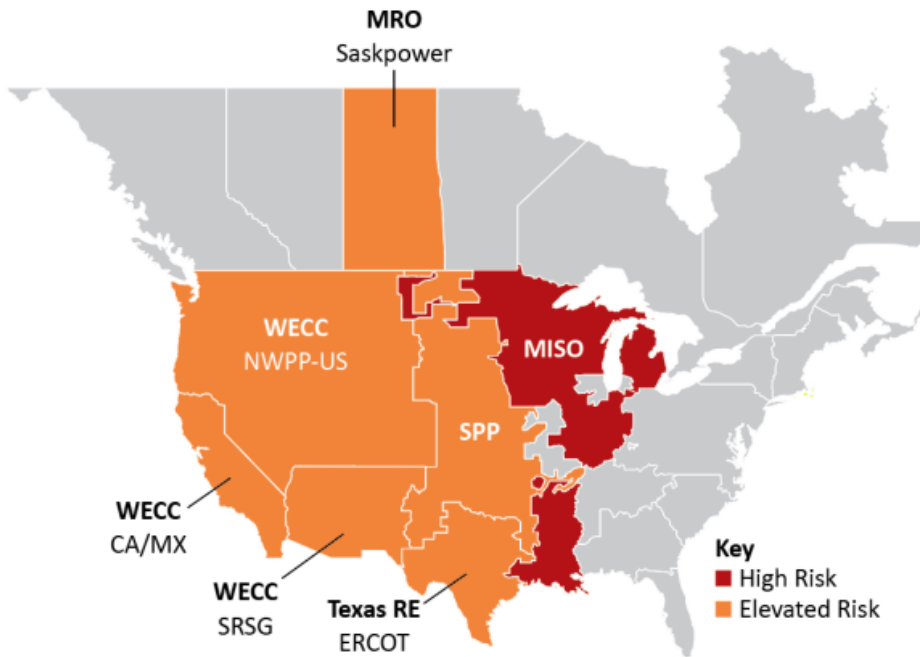


Figure 1: Summer Reliability Risk Area Summary

Seasonal Risk Assessment Summary	
High	Potential for insufficient operating reserves in normal peak conditions
Elevated	Potential for insufficient operating reserves in above-normal conditions
Low	Sufficient operating reserves expected

Operating on the Edge

The West

Drought and extreme heat threaten reliable generation

MISO

Capacity shortfalls likely and transmission trouble

Mitigation

is not

Adaptation

Global Spotlight

- Yearly COP conferences since 1995

Metrics

- Tons of CO2 and methane released

Targets

- Temp increase < 1.5 or 2.0 degrees C

Reporting

- IPCC, TCFD, FSOC / SEC

Rallying Cry

- Net Zero GHG emissions



Global Spotlight

- None – it's local

Metrics

- Emergency supplementals

Targets

- None

Reporting

- None

Rallying Cry

- Resilience!



Climate Impacts to Thermal Plants

ENERGYWIRE

CLIMATE AND WEATHER & 18 OTHERS



Severe heat, drought pack dual threat to power plants

BY: HANNAH NORTHEY, PETER BEHR | 06/28/2021 07:08 AM EDT

"Nationwide, more than 70% of the 1,100 gigawatts of U.S. power plant capacity requires cooling, and half of that supply comes from fresh surface water. All told, power plants suck up almost half of all fresh water used nationwide, and their operations can be curtailed if water levels in reservoirs, lakes or rivers drop too low, or discharges of heated water from plants raise water temperatures too high."

Climate Impacts to Water Infrastructures

An aerial photograph showing a significant flood in a rural area. The water is murky brown and has inundated fields, roads, and parts of several houses. Trees are partially submerged, and the overall scene depicts the severe impact of flooding on infrastructure and the environment.

Water treatment challenges:

- Stronger storms and flooding
- Sea-level rise and storm surge
- More frequent and intense droughts
- Saltwater intrusion, and
- Impacts to source water quality

Water management challenges:

- According to the ASCE, US dams and levees need billions of dollars of repairs
- And that's just to make them safe for the conditions of the previous century

Energy Assets to Defend



Generation

- Coal, natural gas, nuclear, geothermal, hydro, wind, solar

Electricity T&D

- Substations & transformers, transition lines & distribution feeders, towers

National and liquid gas T&D

- Compressor stations, pipelines

Control centers

- Electric, natural gas, liquid gas product

Energy storage

- Pumped hydro, compressed air, battery, hydrogen

Planning Methods are Proving Inadequate

"This weather system in Texas greatly exceeded the planning criteria in which they operate ERCOT."



This says so much.

-- Tom Fanning, Southern Co
CEO



So, then what to do

???



A Conceptual Decision Support Framework for Decision Makers

Figure 1: ICAR Workflow

3 Questions for Decision Makers

1. How confident are we that our most critical assets can operate through slow onset and fast onset extreme conditions?

3 Questions for Decision Makers

2. If we haven't already, should we update our procurement processes to specify new systems and equipment that will be ready to operate in the environmental conditions of today and tomorrow?



3 Questions for Decision Makers

-
-
3. Supply chain – are our trusted partners aware and in motion on these challenges?

A DHS Resource Worth Knowing



Sunny Wescott

Lead Meteorologist – Collaboration Cell

Infrastructure Security Division (ISD)

Cybersecurity and Infrastructure Security Agency (CISA)

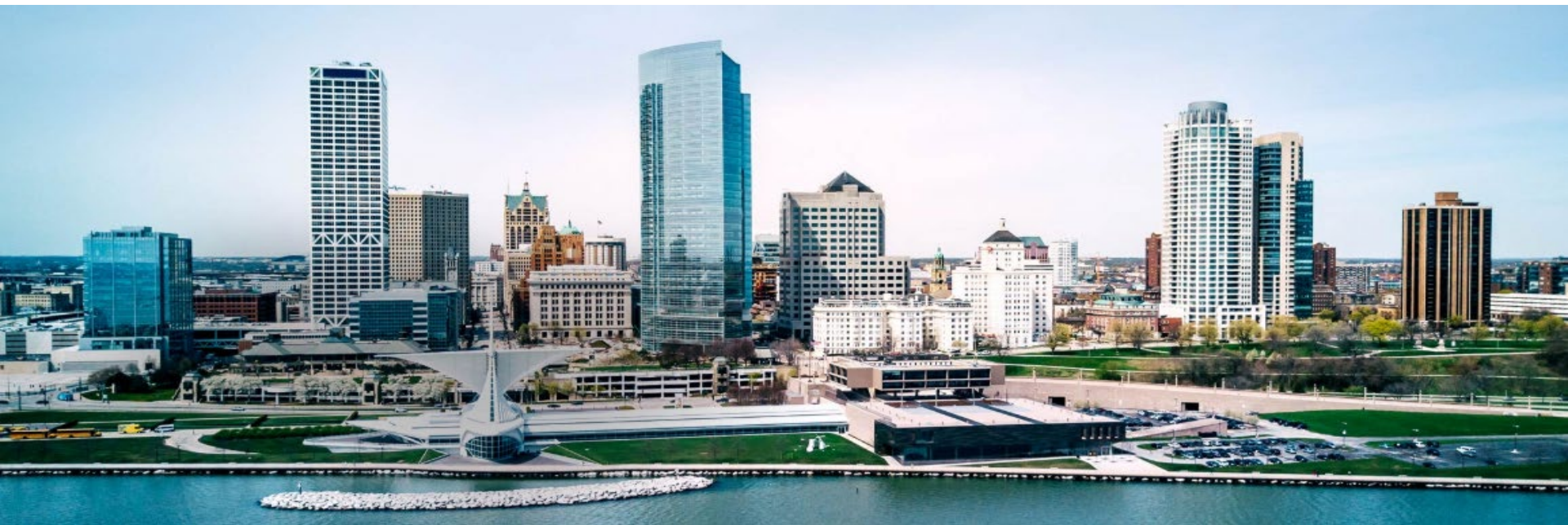
Department of Homeland Security (DHS)

Email: Sunny.Wescott@cisa.dhs.gov

Thanks

andrew.bochman@inl.gov

twitter: [@andybochman](https://twitter.com/andybochman)





Additional Slides



Energy Assets to Defend

Generation

- Coal, natural gas, nuclear, geothermal, hydro, wind, solar

Electricity T&D

- Substations & transformers, transmission lines & distribution feeders, towers

National and liquid gas T&D

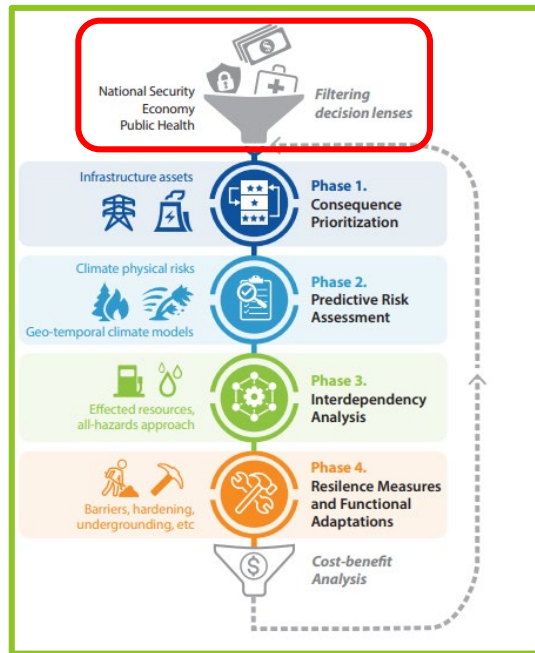
- Compressor stations, pipelines

Control centers

- Electric, natural gas, liquid gas product

Energy storage

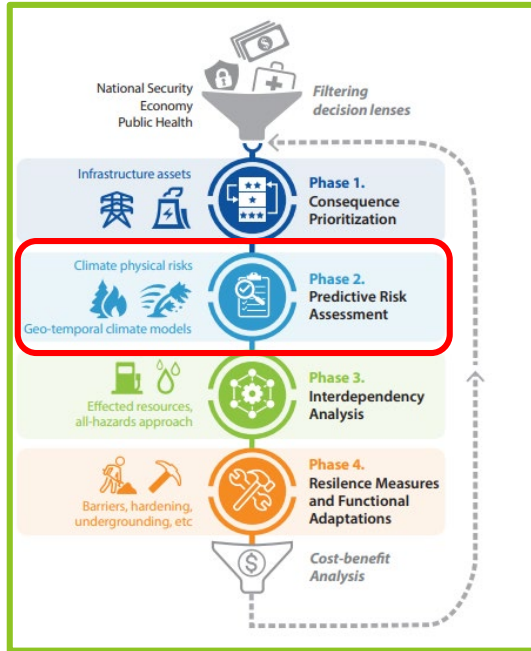
- Pumped hydro, compressed air, battery, hydrogen



Tailorable filters play a role at several different stages of the ICAR workflow. National Security, Economic Security, Public Health, Equity and more can be included or excluded, and weighted to accommodate the circumstances of the missions supported, loads served, geography, community and timeframe.



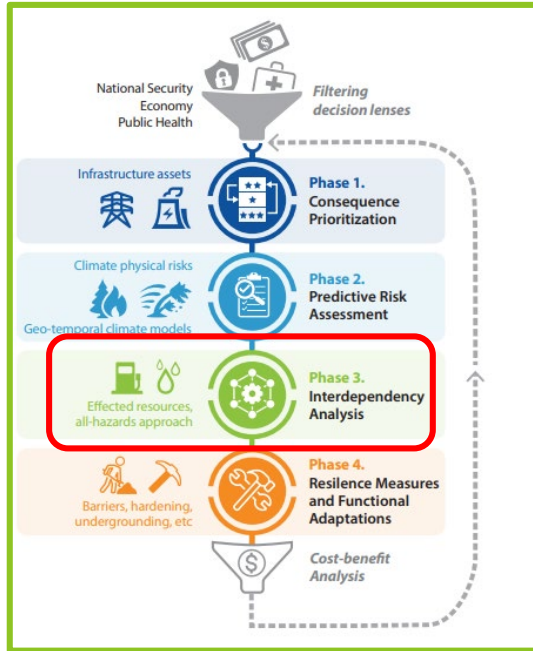
Identifies the energy infrastructure assets that must be protected first and best. We're not going to be able to protect everything, but if we base our asset protection, functional adaption and siting selections on what matters most, we'll be making the best use of scarce resources—including perhaps the most important one: time.



The second phase requires we look to the future with as much as confidence and precision as possible. ICAR imports downscaled data from global climate models to help planners understand the physical risks that will likely assail currently acceptable locations in coming years and decades. Key info to be generated: what impacts are projected, where, and by approximately when.



This phase ensures grid and other sectors' functions are fully factored into the recommendations produced by the framework. For example, thermal generation plants often require substantial amounts of water. For electricity to reach customers, transmission lines and distribution feeders, and the substations that connect them must not be harmed by fires, floods, or temperatures well outside their operating parameters. Water and wastewater treatment requires power. Without proper functioning of water and wastewater treatment plants, their failure brings grave health, environmental, and economic consequences. Other key interdependencies include transportation and communications.





There's a lot that can be done once the assets requiring attention have been identified. Once the risks and the most likely time horizons for their arrival are well described, the most appropriate adaptive design and engineering alternatives are explored, with the best options recommended in prioritized order based on cost-effectiveness and efficiency. At the end of each analysis, ICAR does not seek to provide the best answer, but rather identify the best suite of options, prioritized by weightings tailored to each current protective/adaptive and future siting challenge.



Cost-benefit Analysis

Once all the resilience and adaptation options are generated, CBA is performed drawing on inputs including:

- Confidence – that the measure will provide the required level of asset or function protection against present and projected physical risks
- Duration - anticipated timeframe in decades that the candidate resilience or adaptive measure will continue to perform as required
- Time to execute – how long the project will take to complete, including considerations of funding, permitting, siting (if a new build), etc.
- Cost - initial and full lifecycle costs



Thank you for attending this event!

- Please provide your feedback for the 2022 Security Conference using the link or QR code below:
- <https://www.surveymonkey.com/r/XNWVWTM>

