WATERFALL®
Stronger Than Firewalls

The Top 20 CyberAttacks on Industrial Control Systems

Andrew Ginter

VP Industrial Security
Waterfall Security Solutions

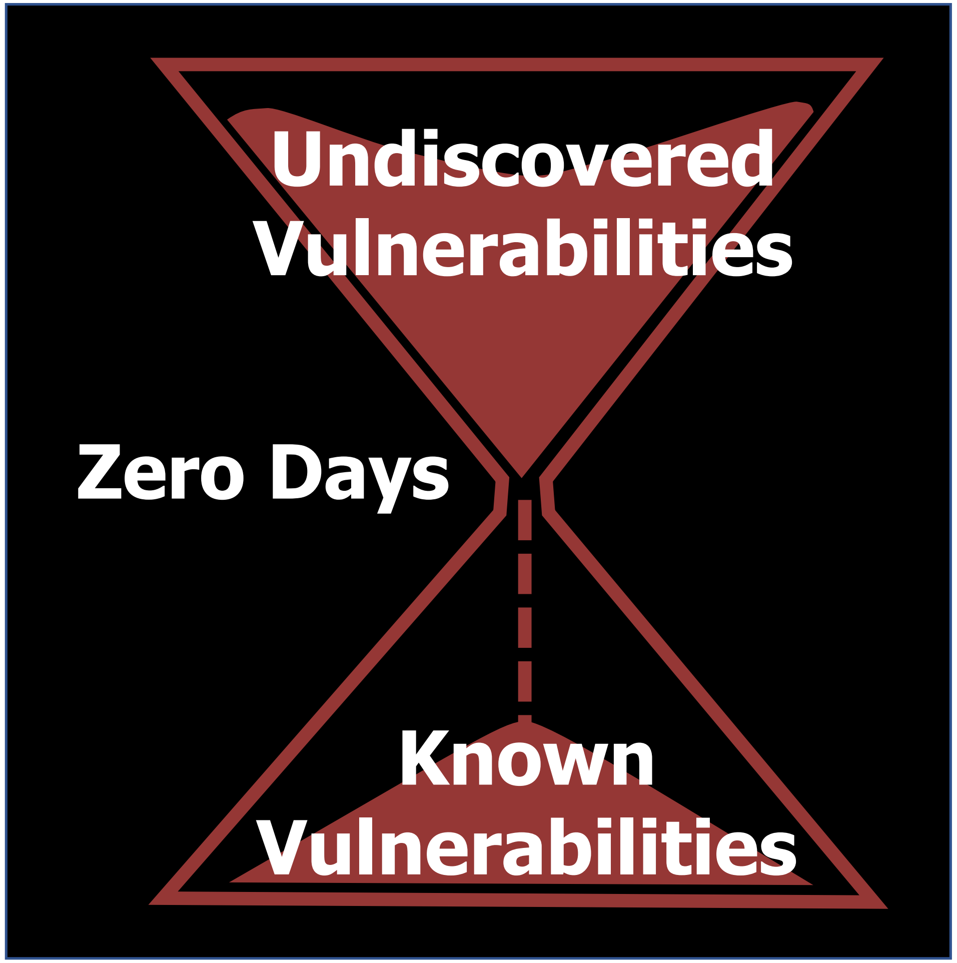
http://waterfall-security.com/20-attacks

Vulnerabilities?

- Risk = Threat x Vulnerability x Consequence
- So … if I can reduce my vulnerabilities to zero, I am ***invulnerable***
- Quick – patch everything!

This is of course nonsense…

Security updates are not useless, but are much less useful than most practitioners believe



Top 20 Attacks

WATERFALL
Stronger Than Firewalls

- We can evaluate our defenses only if we understand how we might be attacked – understanding attacks is essential to defense
- Twenty attacks – across a range of: attack types, attacker resources, cyber sophistication, physical engineering sophistication, and control system engineering sophistication
- Bar: “defeats reliably” – eg: AV does not defeat reliably because of how long it takes to create signatures

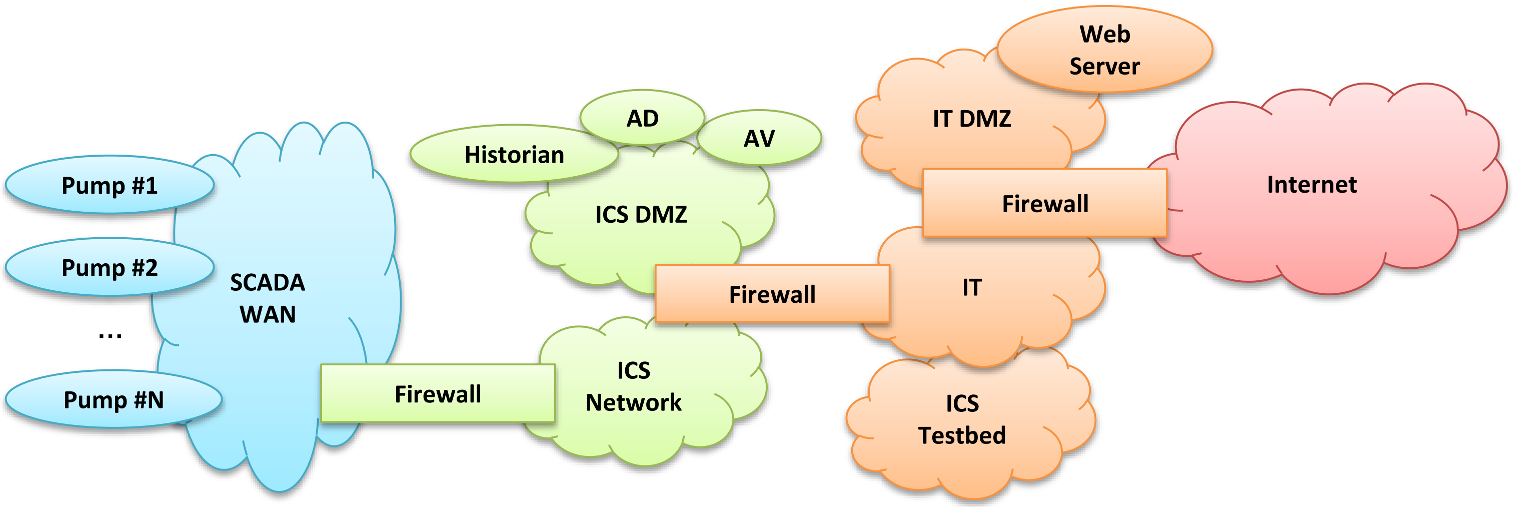
“Defeats reliably” is a high bar

#1 ICS Insider	#8 Market Manipulation	#15 Compromised Remote Site
#2 IT Insider	#9 Sophisticated Market Manipulation	#16 Vendor Back Door
#3 Common Ransomware	#10 Cell-phone WIFI	#17 Stuxnet
#4 Targeted Ransomware	#11 Hijacked Two-Factor	#18 Hardware Supply Chain
#5 Zero-Day Ransomware	#12 IIoT Pivot	#19 Nation-State Crypto Compromise
#6 Ukrainian Attack	#13 Malicious Outsourcing	#20 Sophisticated Credentialed ICS Insider
#7 Sophisticated Ukrainian Attack	#14 Compromised Vendor Website	

Example Target: Waterworks

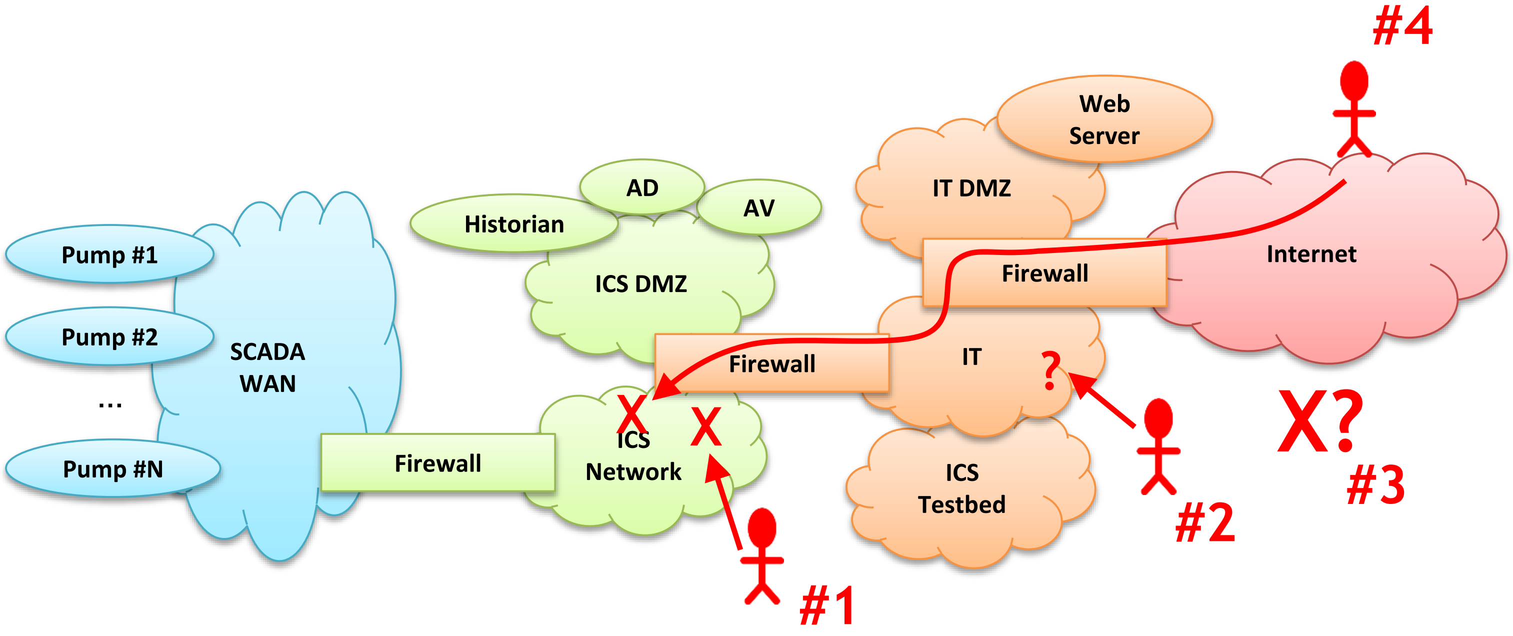
- SCADA WAN – dedicated telecoms infrastructure, firewall at every remote site
- ICS defended to first-gen ICS security best practices:
- Firewalls, DMZ's and encryption
- Anti-virus & security updates
- Two-factor + jump hosts = "secure" remote access
- Local IDS & SIEM

Completely patched = zero vulnerabilities!



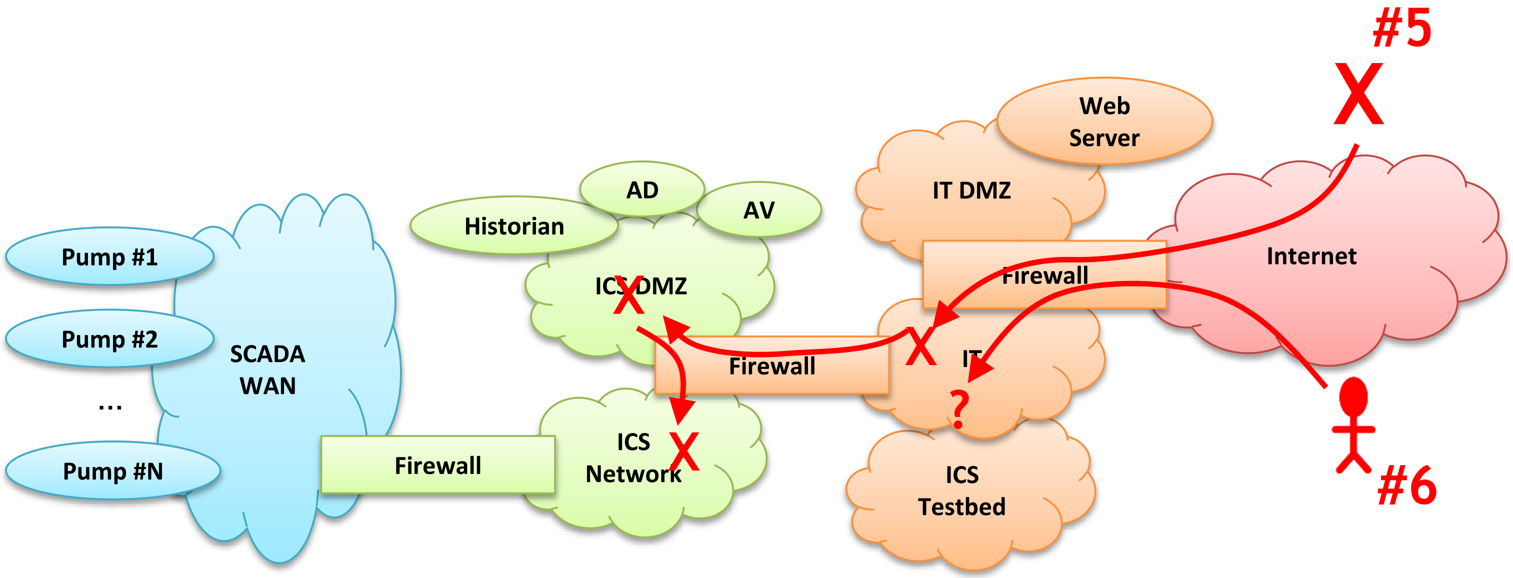
Attacks #1-4

- #1 ICS insider – not defeated – physical access trumps cyber defenses
- #2 IT insider social engineering – reliably defeated by two-factor auth
- #3 Common ransomware – defeated – cannot download, cannot auto-run
- #4 Targeted ransomware – not defeated – professional-grade attackers



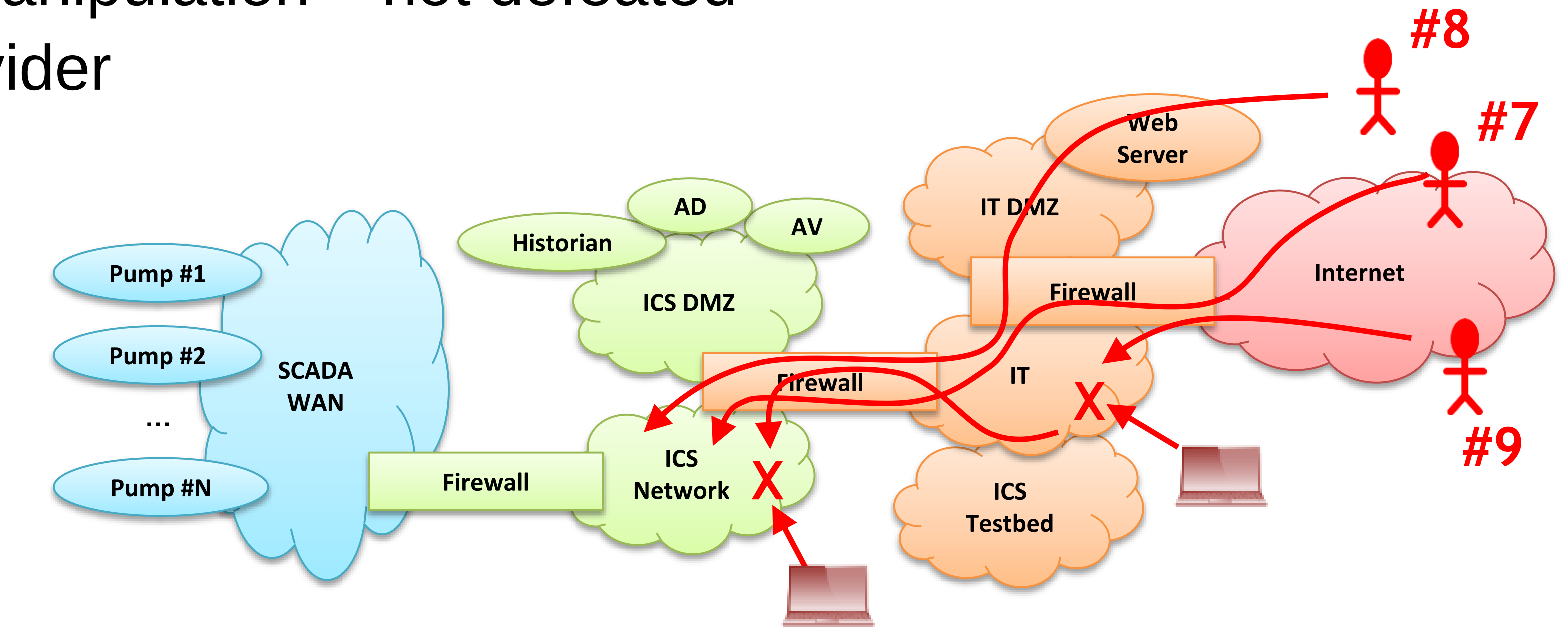
Attacks #5-6

- #5 Zero-day ransomware – not defeated – spreads through zero-day in file sharing connections through firewalls
- #6 Ukrainian attack – defeated by two-factor authentication



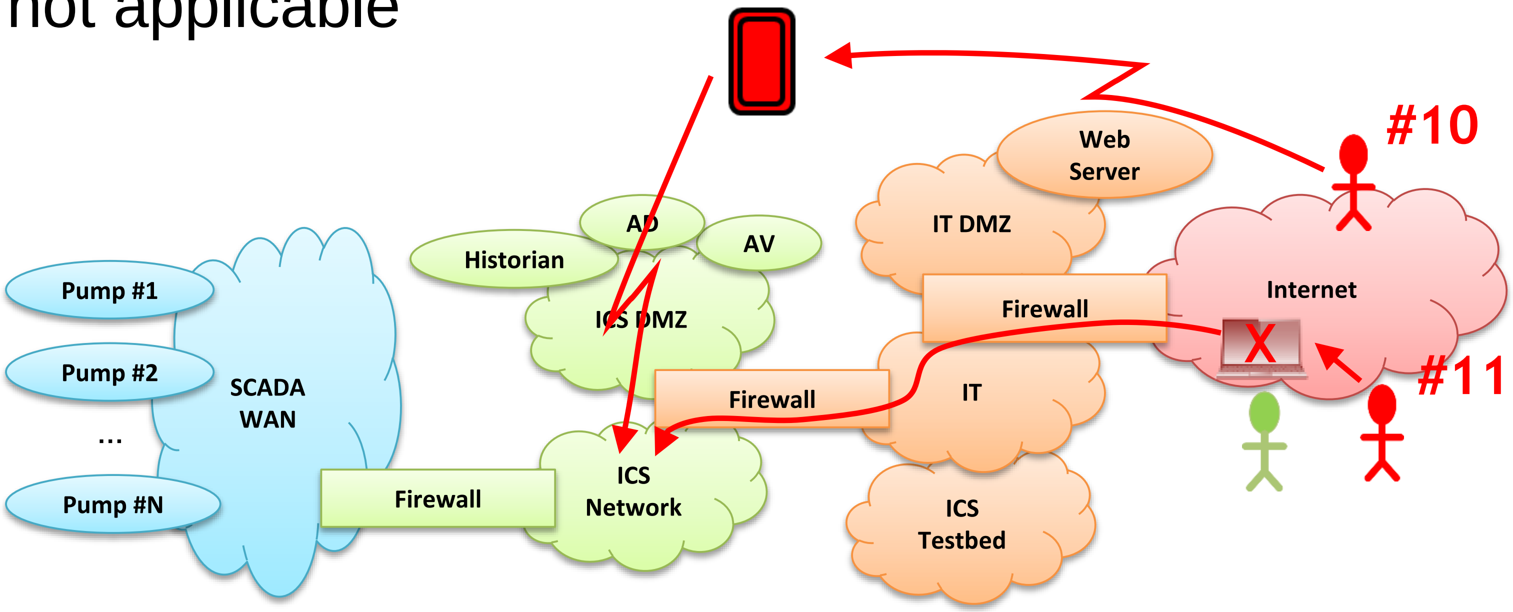
Attacks #7-9

- #7 Sophisticated Ukrainian attack – not defeated – professional grade attack
- #8 Market manipulation attack – not defeated - even fully-patched Internet-facing servers have windows of opportunity when POC exploits circulate before security updates exist
- #9 Sophisticated market manipulation – not defeated – compromised services provider



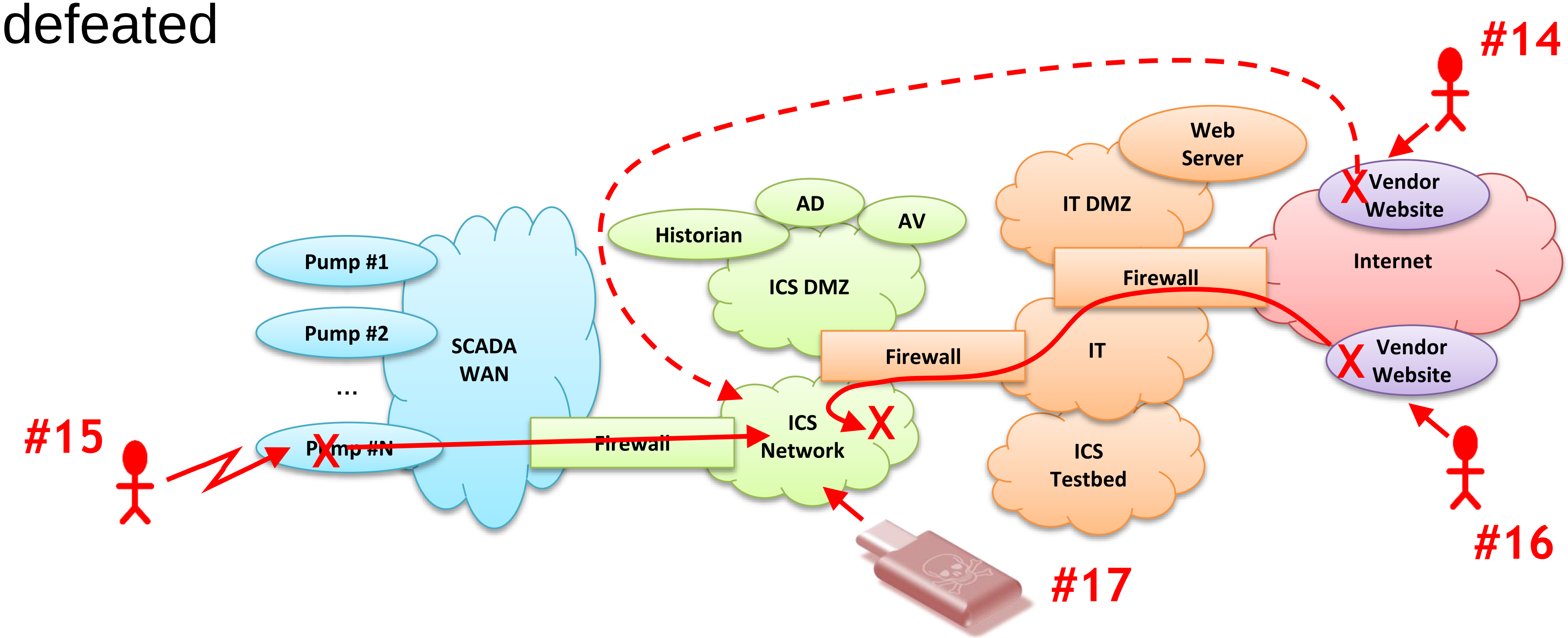
Attacks #10-13

- #10 Cell phone WIFI – not defeated – trojan app searches for ICS WiFI
- #11 Hijacked two-factor – not defeated – take over remote session after two-factor authentication
- #12 IIoT pivot – not applicable
- #13 Malicious outsourcing – not applicable



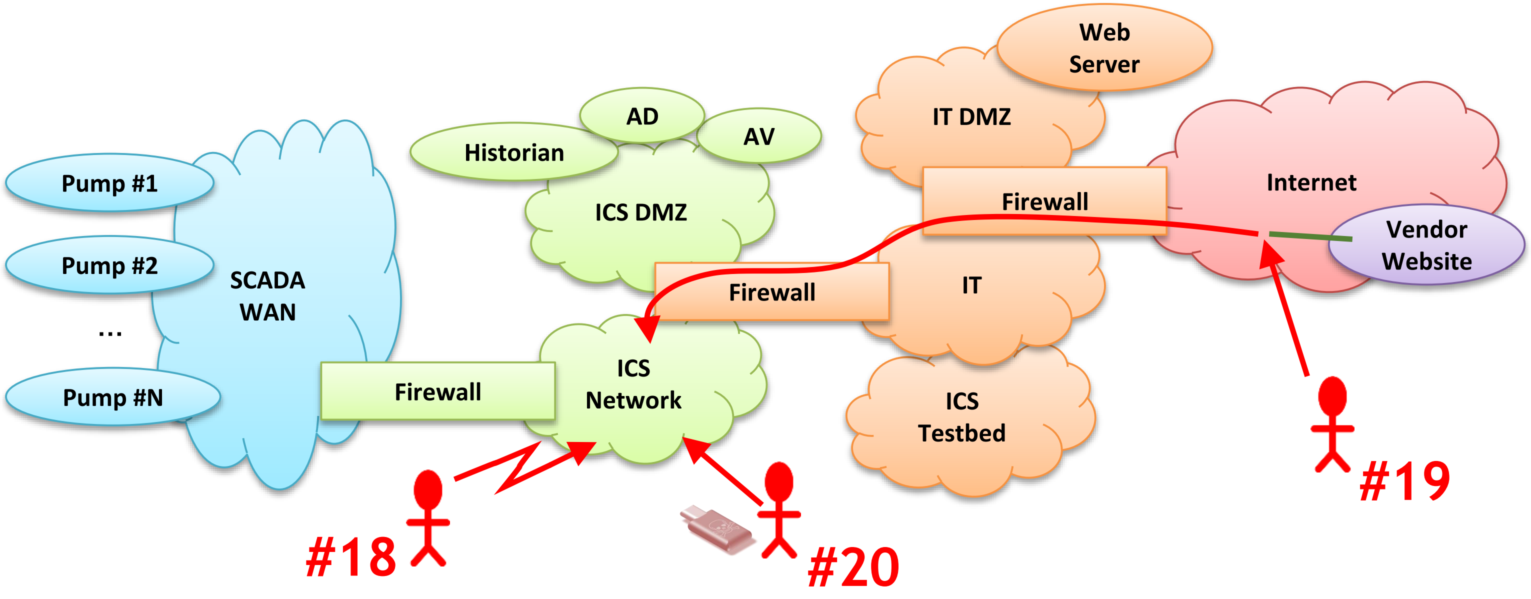
Attacks #14-17

- #14 Compromised vendor website – not defeated
- #15 Compromised remote site – not defeated
- #16 Vendor back door – not defeated
- #17 Stuxnet – not defeated



Attacks #18-20

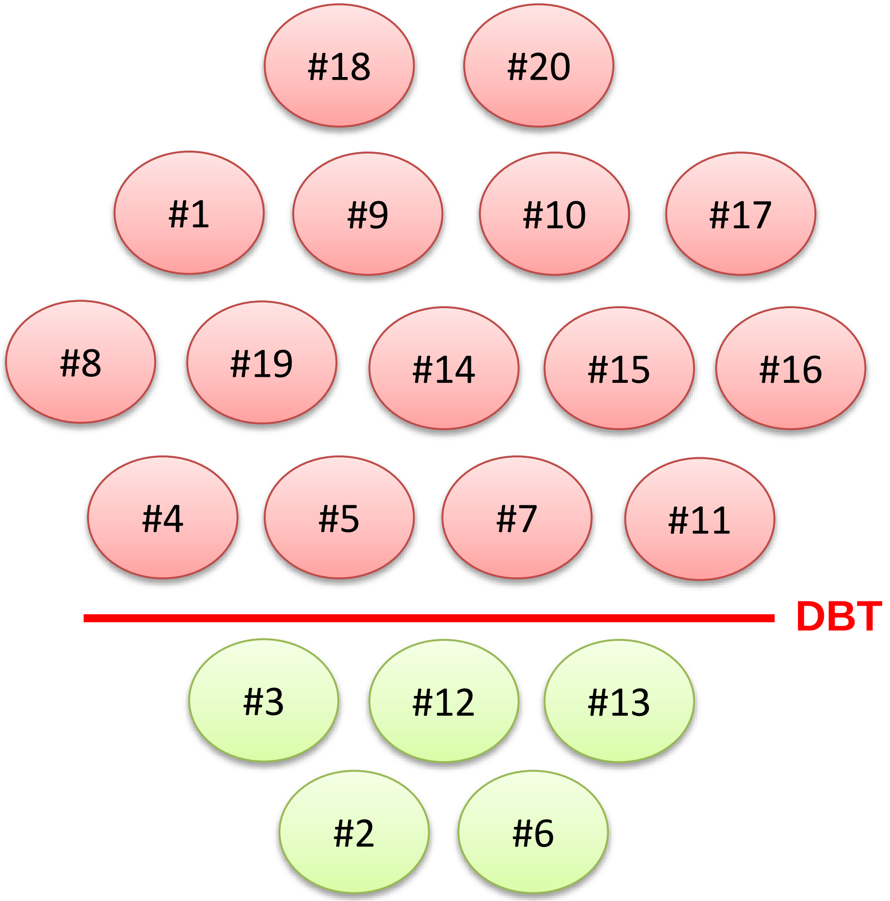
- #18 Hardware supply chain – not defeated
- #19 Nation-state crypto compromise – not defeated
- #20 Sophisticated, credentialed ICS insider – not defeated



Waterworks 1st-Gen Summary

WATERFALL
Stronger Than Firewalls

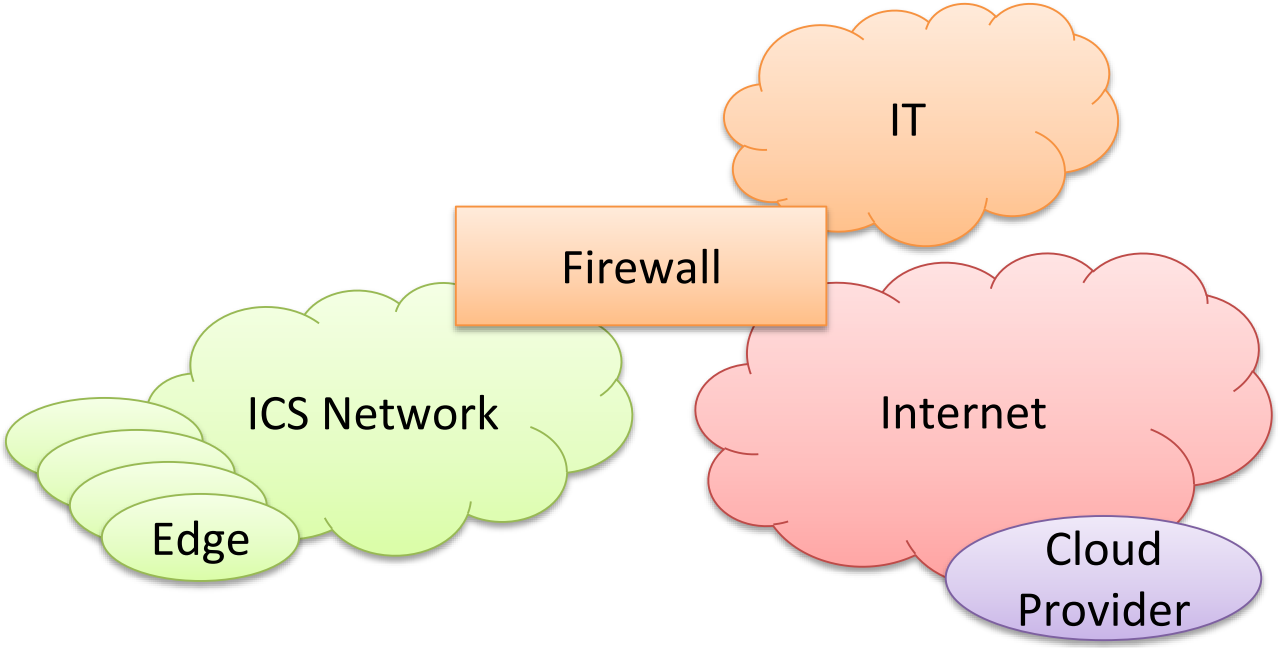
- Design Basis Threat = physical security concept – description of attacks a site is required to defeat reliably
- Use DBT line to communicate risk & compare risk postures
- Business decision-makers can ask what cost to move the line, and what attacks are not defeated reliably



Boards of directors and C-levels tend to understand attacks more quickly than abstract risk scores or made-up probabilities

Waterworks With Cloud

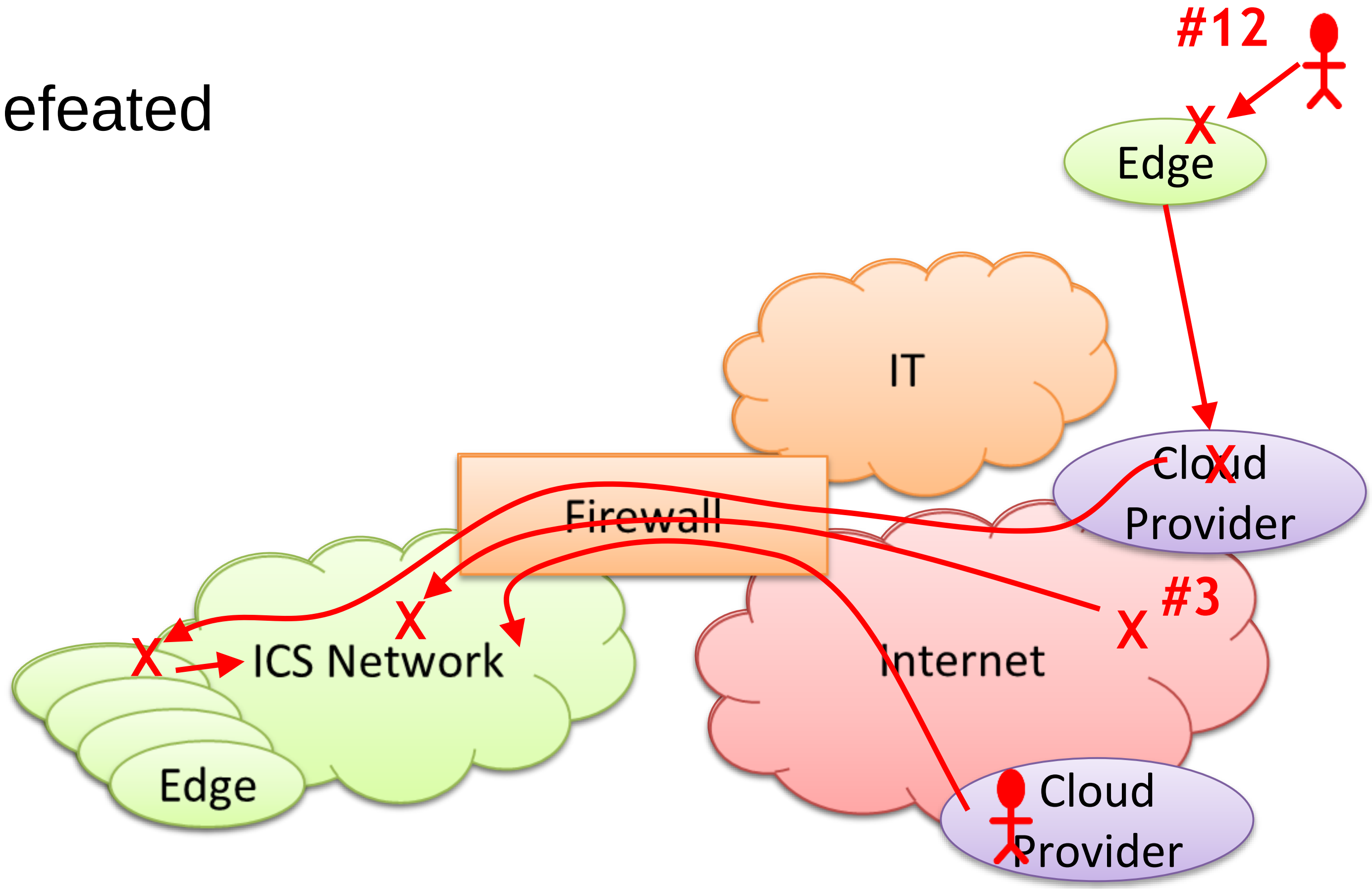
- Add edge devices and software directly connected to cloud sides on Internet
- Add outsourced ICS monitoring and maintenance – cloud personnel can remote into site and change configurations – “fix” things
- Ie: edge devices need to route directly to Internet



What does this do to the attack surface?

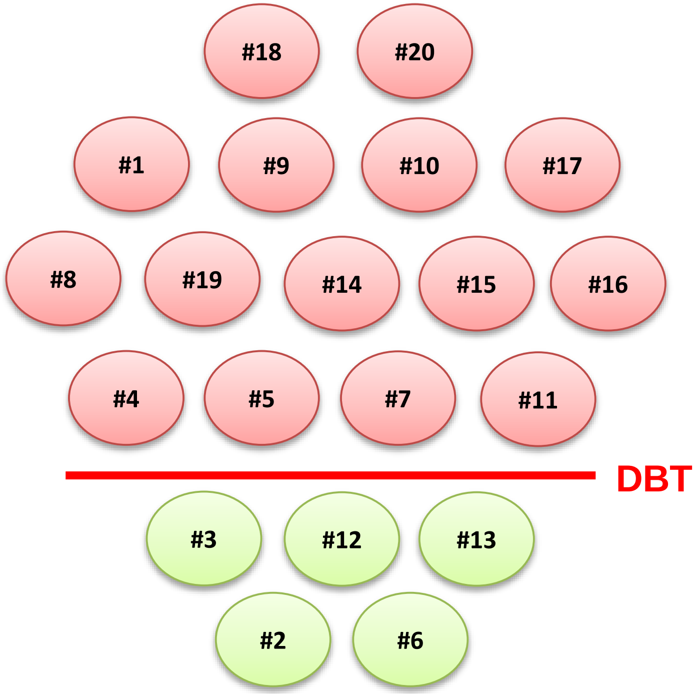
Attacks #3, #12-13

- #3 Common ransomware – not defeated – ICS has route to Internet
- #12 IIoT pivot – not defeated
- #13 Malicious outsourcing – not defeated

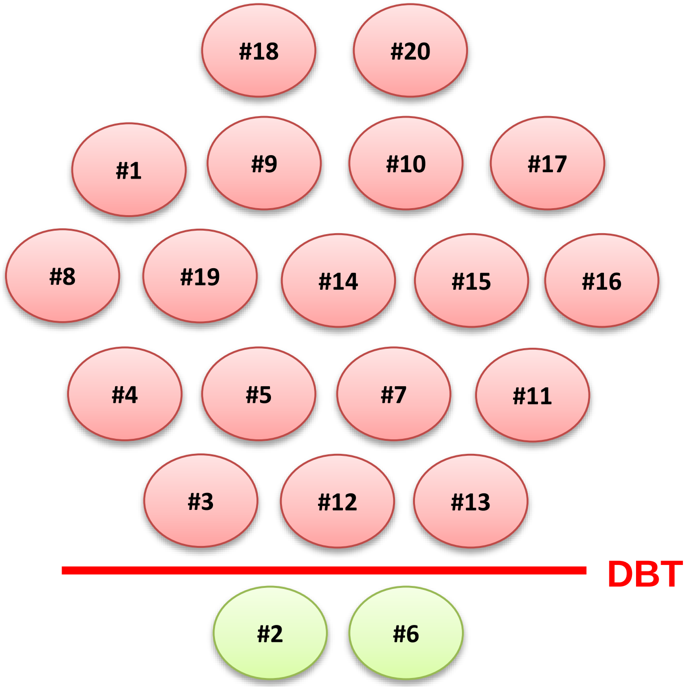


Waterworks With Cloud Summary

- Routinely routing information from our most sensitive control system networks to the Internet introduces risk



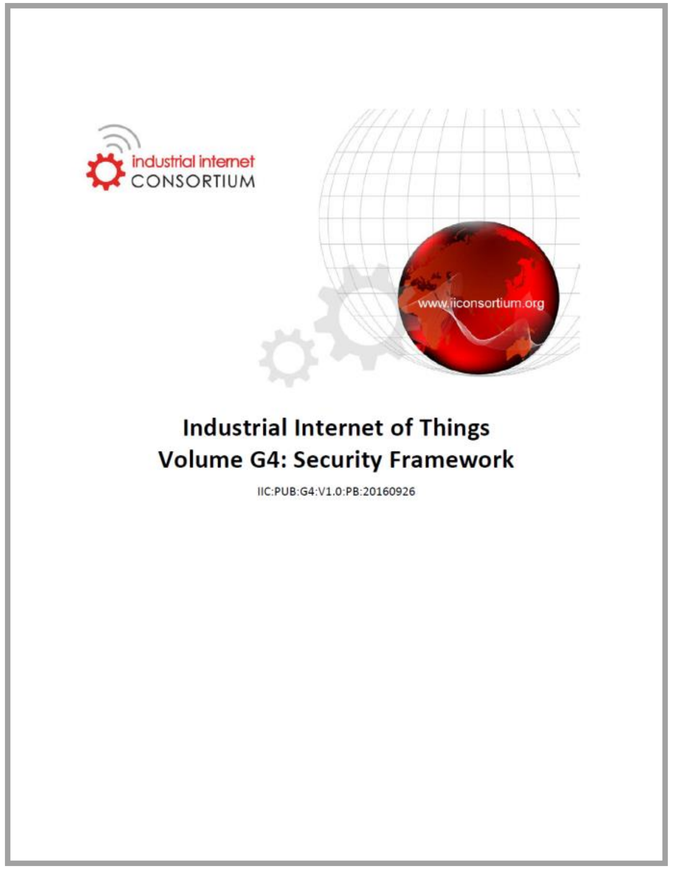
First-generation ICS



First-gen with cloud

IIC Security Framework

- Edge device protection options:
- #1 Device hardening – TPM, encryption, secure boot, trusted hypervisor
- #2 Software security gateway – convert edge to Internet
- #3 Firewalls – controlled routing to Internet
- #4 Unidirectional Gateways – physically able to transmit information only one way



industrial internet CONSORTIUM

www.iiconsortium.org

Industrial Internet of Things
Volume G4: Security Framework

IIC:PUB:G4:V1.0:PB:20160926

First-gen waterworks already has #1-3 – let’s try #4

Unidirectional Gateways

WATERFALL® Stronger Than Firewalls

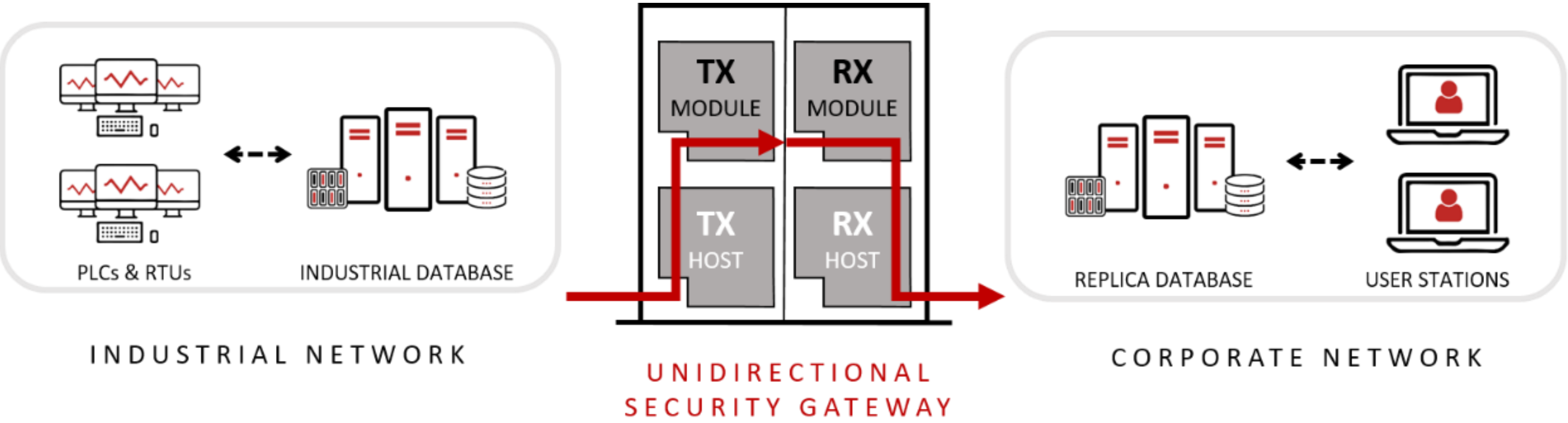
Safe IT/OT Integration
Combination of Hardware and Software

HARDWARE

- TX Module hardware is a fiber-optic transmitter/laser & RX Module is an optical receiver with no laser
- Physically able to transmit information in only one direction

SOFTWARE

- Replicates servers and emulates devices
- Corporate users access replicas normally – seamless integration
- Never forwards network traffic

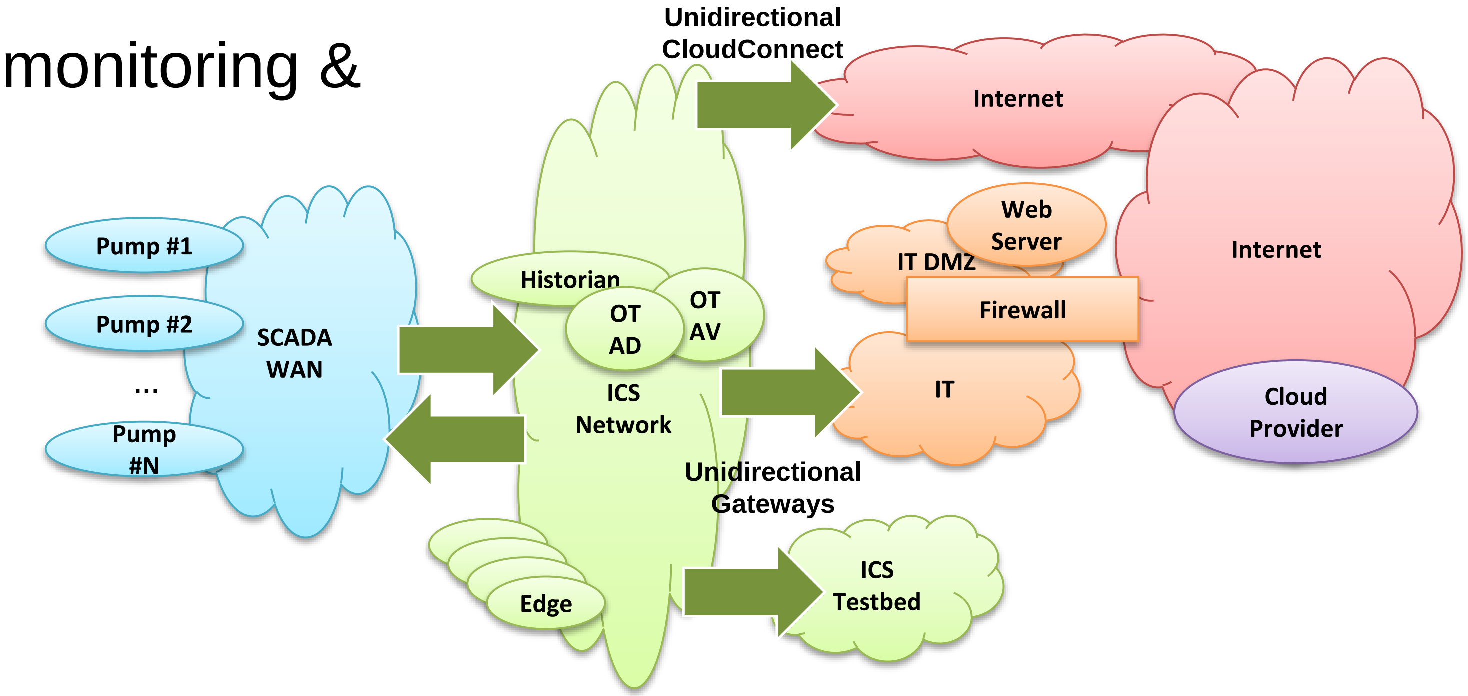


SEC-OT for the Waterworks

WATERFALL Stronger Than Firewalls

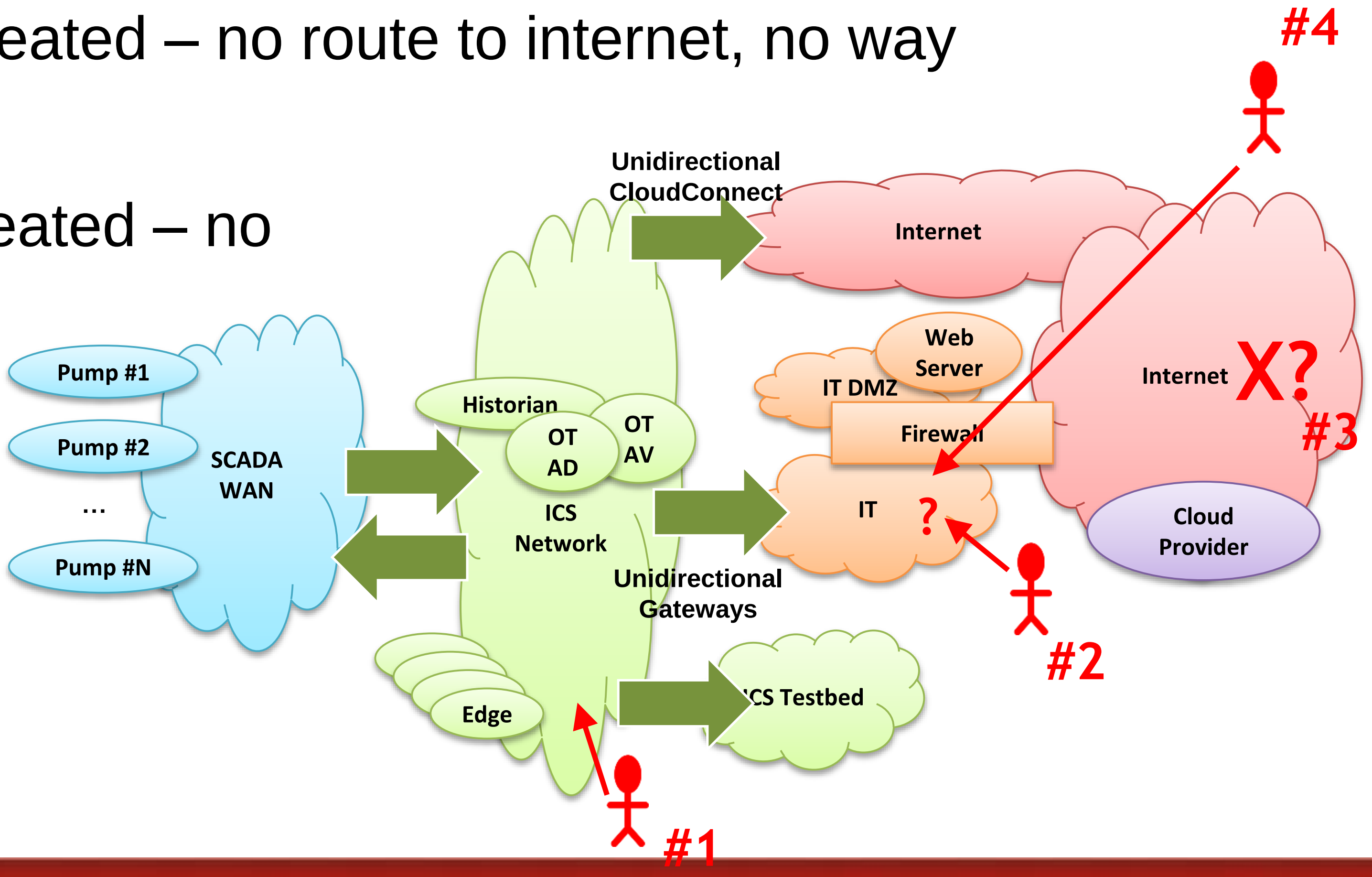
- Unidirectional gateway technology is interface between networks at different levels of trust – ie: between ICS network and all other networks
- Unidirectional CloudConnect has UGW under hood, translating to websockets & other cloud formats
- Strict removable media policy, monitoring & follow-up
- Test bed instrumented as sandbox

Reflects modern advice such as NIST 800-82r2, ANSSI, NERC CIP V5 & IIC SF



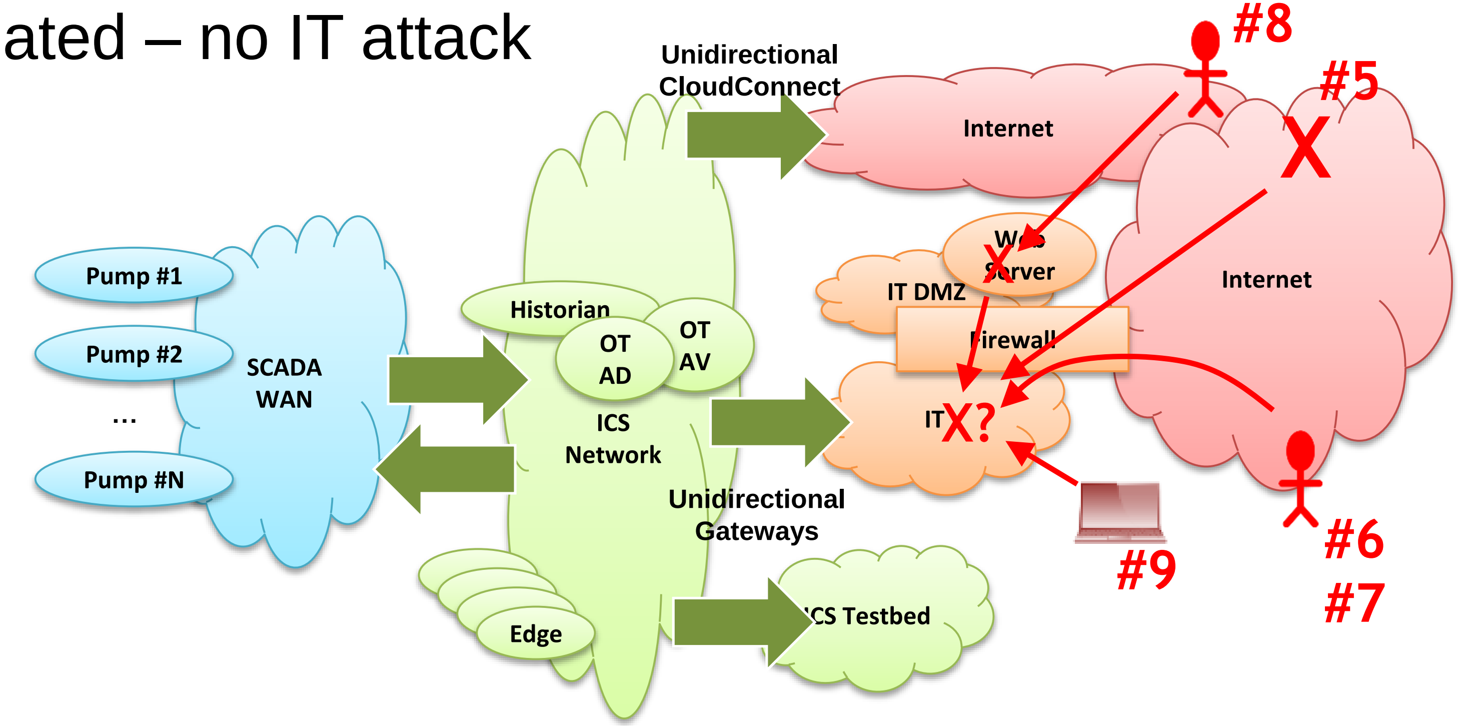
Attacks #1-4

- #1 ICS insider – not defeated – unchanged
- #2 IT insider – defeated – UGW prevents all IT attacks
- #3 Common ransomware – defeated – no route to internet, no way to download, no AUTORUN
- #4 Targeted ransomware – defeated – no way to establish remote control



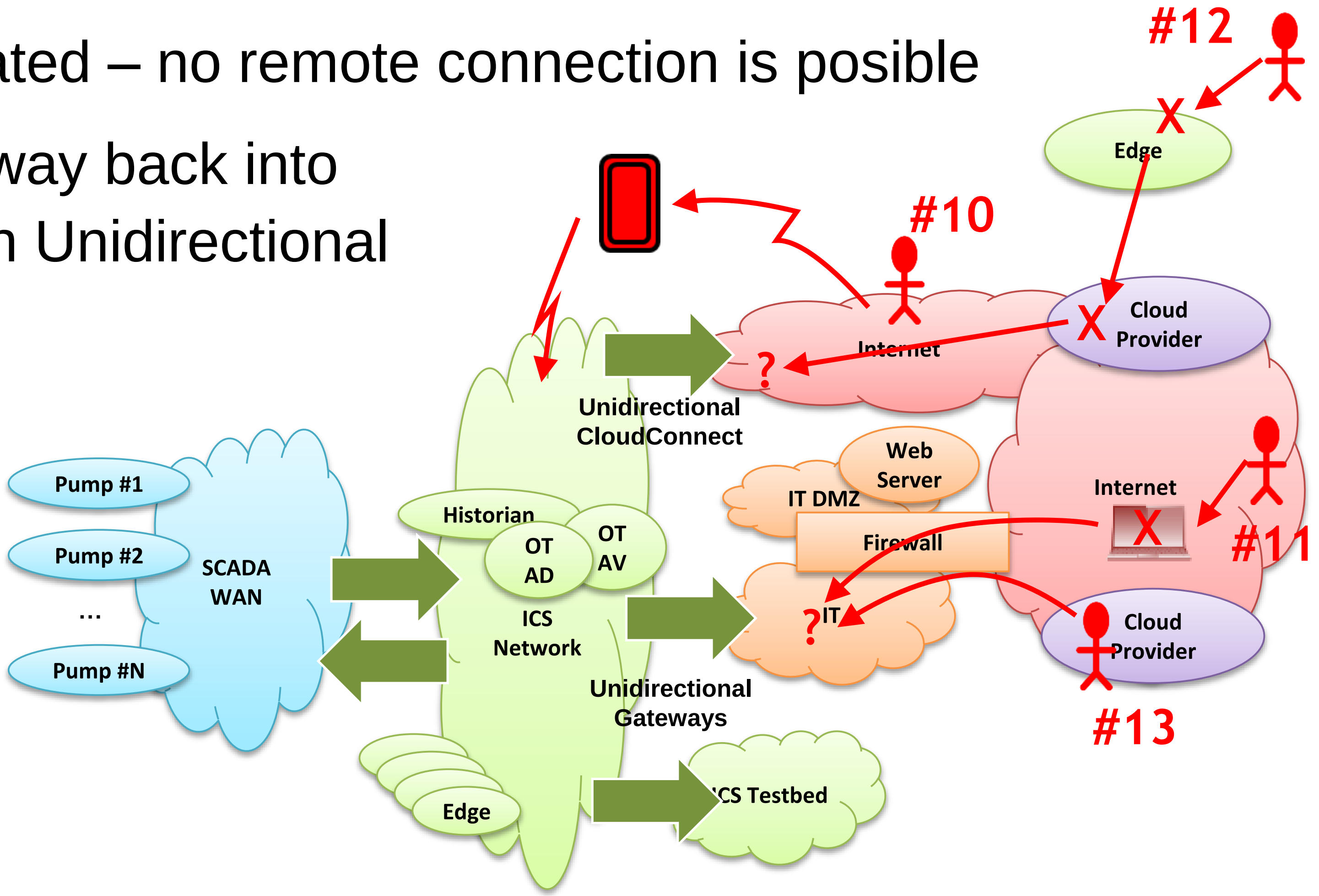
Attacks #5-9

- #5 Zero-day ransomware – defeated - no opportunity to propagate
- #6 Ukrainian attack – defeated - no remote attack possible
- #7 Sophisticated Ukrainian attack – defeated – no remote attack possible
- #8 Market manipulation – defeated – no IT attack can reach the ICS network
- #9 Sophisticated market manipulation – defeated – no remote control attack can reach ICS network



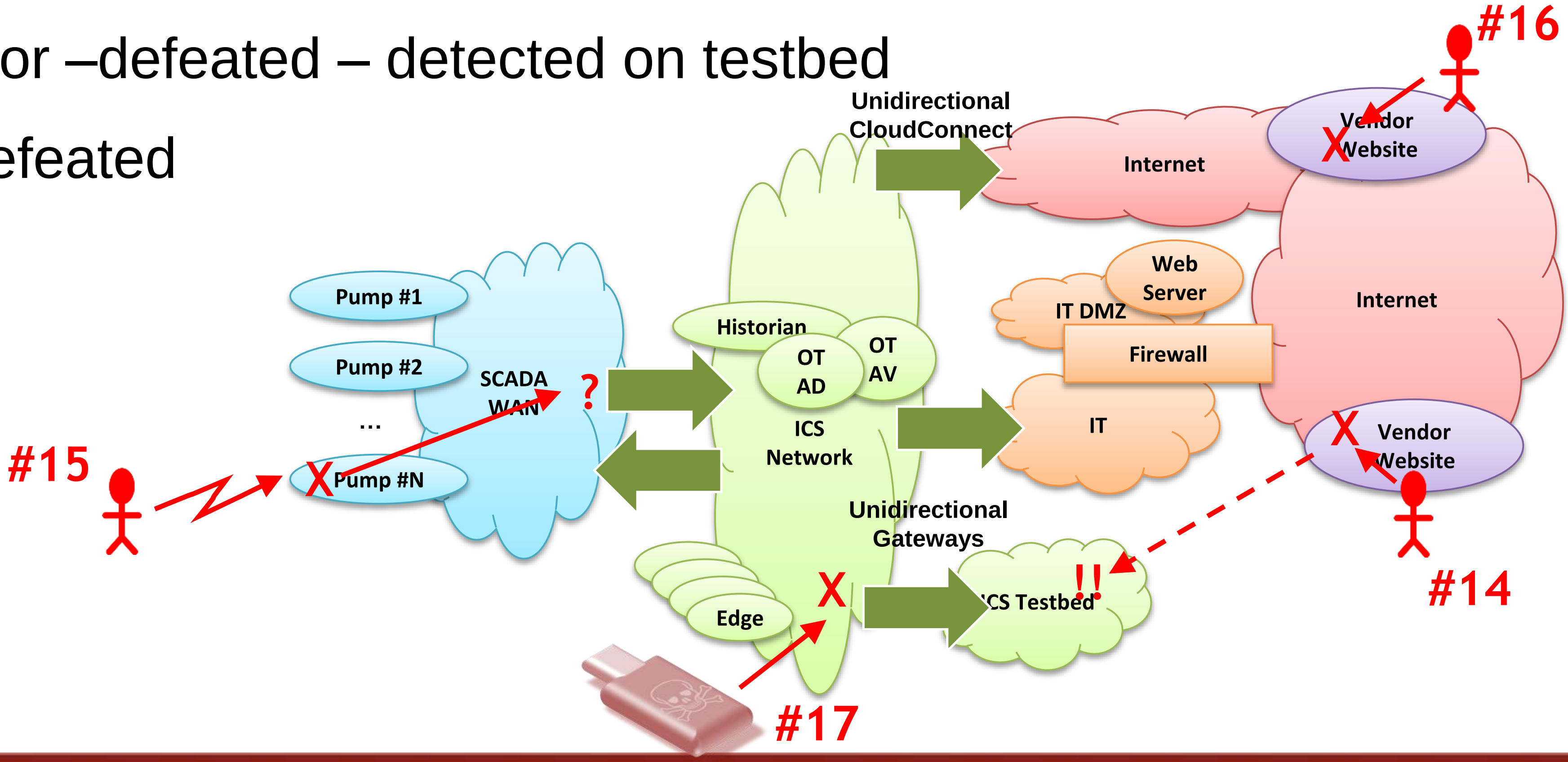
Attacks #10-13

- #10 Cell phone WIFI – not defeated
- #11 Hijacked two-factor – defeated – no remote connection is posible
- #12 IIoT pivot – defeated – no way back into a protected ICS network through Unidirectional CloudConnect
- #13 Malicious outsourcing – defeated – unidirectional Remote Screen View requires cooperation of insiders at ICS site



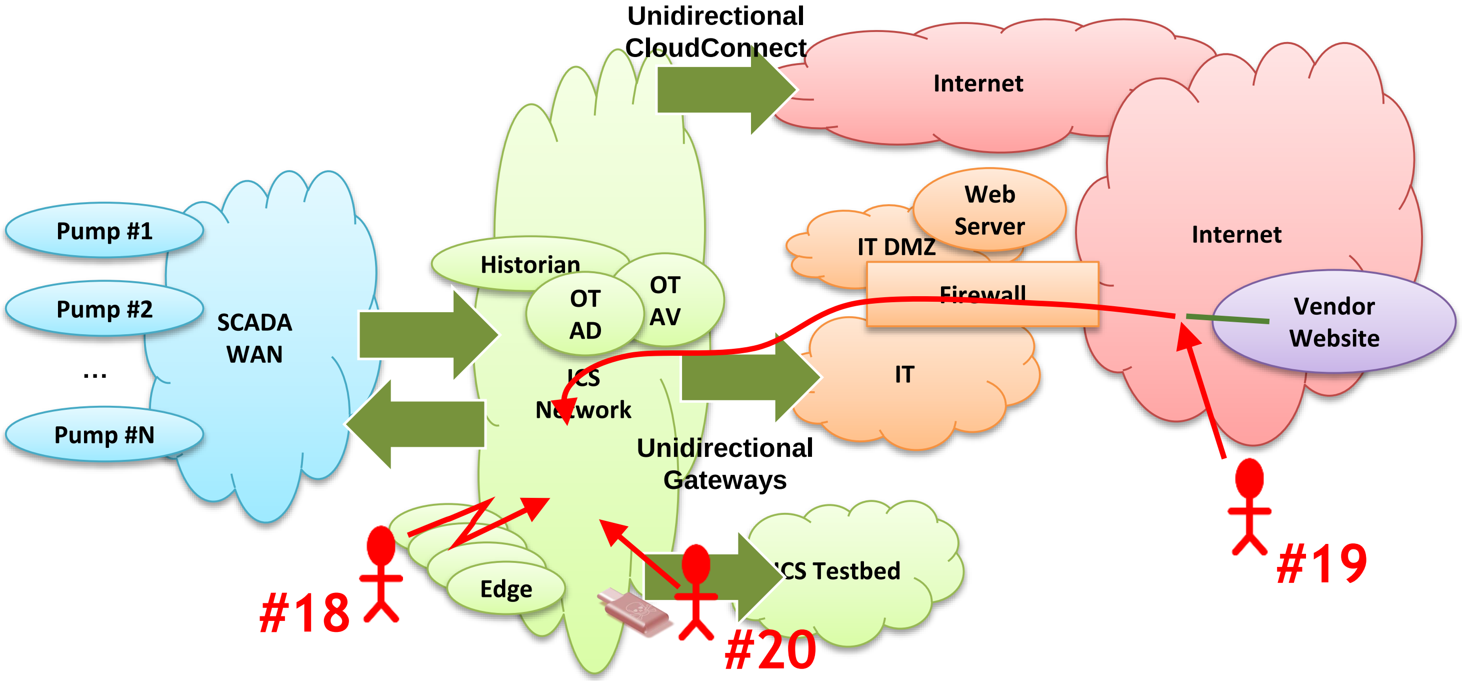
Attacks #14-17

- #14 Compromised vendor website – defeated – new software is deployed first on heavily-instrumented ICS testbed
- #15 Compromised remote site – defeated – no entry through unidirectional gw
- #16 Vendor back door –defeated – detected on testbed
- #17 Stuxnet – not defeated



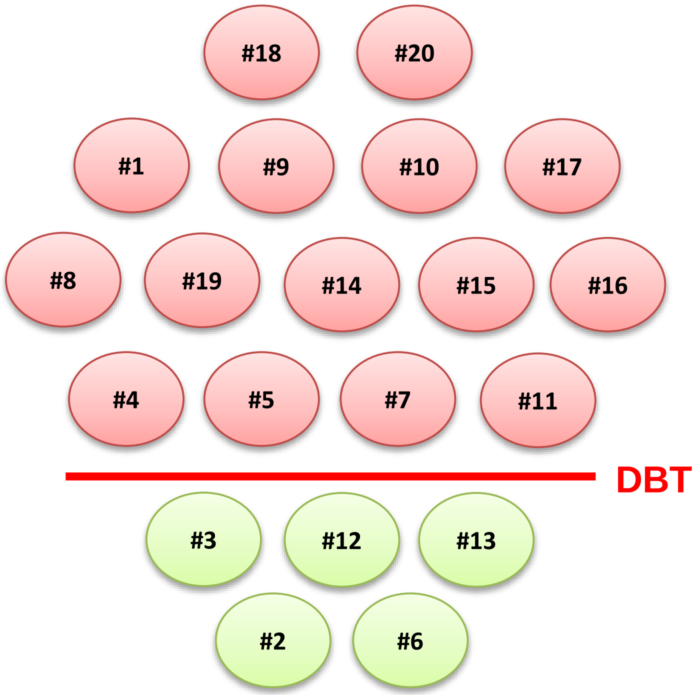
Attacks #18-20

- #18 Hardware supply chain – not defeated
- #19 Nation-state crypto compromise – defeated – no remote connection penetrates Unidirectional Gateways or CloudConnect
- #20 Sophisticated, credentialed ICS insider – not defeated

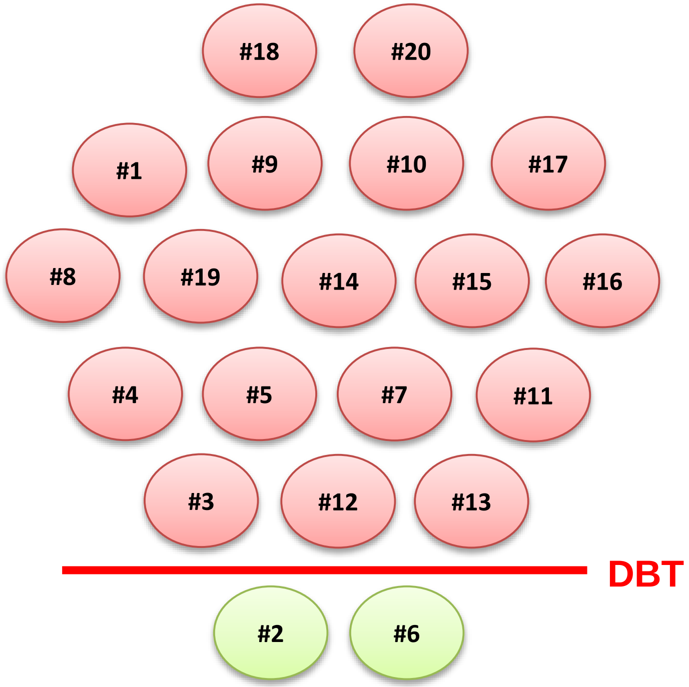


Risk Summary

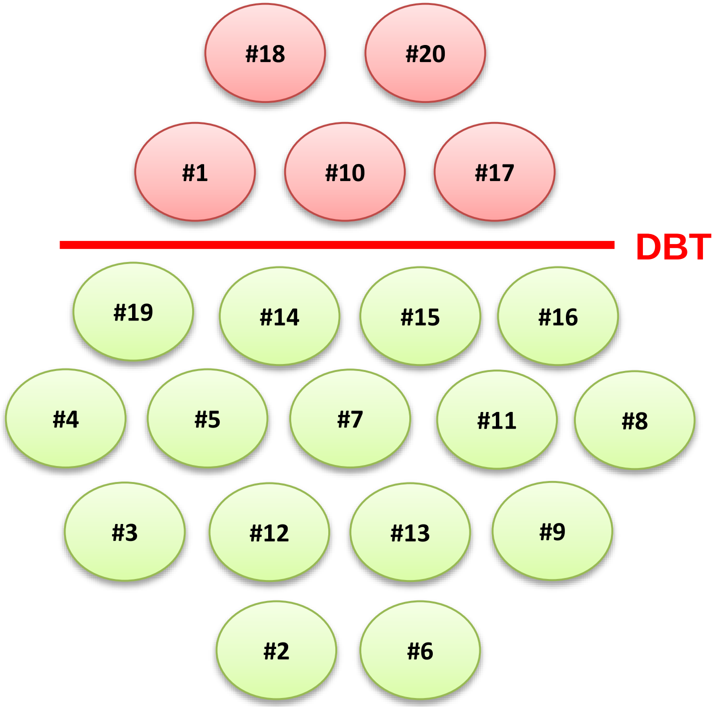
- Modern, unidirectional gateway protection yields IIoT systems even more secure than classic ICS designs



First-generation ICS



First-gen with cloud



SEC-OT

Communicating Risk

- Communicate risk to business decision-makers by describing attacks
- What is the simplest attack with serious consequences that we do not defeat reliably?
- If there is no such attack we are using the wrong set of attacks – nothing is “secure”

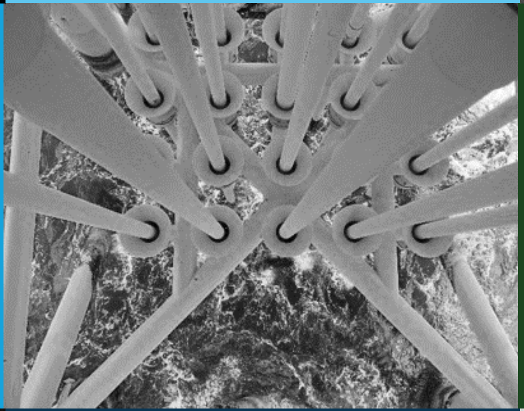
How high should we draw the line?

About Waterfall

Founded in 2007

1000+ sites worldwide

Headquarters in Israel



Deployed in all critical infrastructure sectors

Sales & operations in the USA, EU & APAC

Multiple registered US patents

Technology & sales collaboration with global partners

Drawing The Line

- Understanding attacks is essential to planning and evaluating defenses
- Unidirectional Gateway and Unidirectional CloudConnect dramatically improve defenses
- Example attacks communicate risk effectively to business decision-makers

http://waterfall-security.com/20-attacks

andrew.ginter@waterfall-security.com

+1-587-897-6788