ICS ASIA PACIFIC SUMMIT 2020

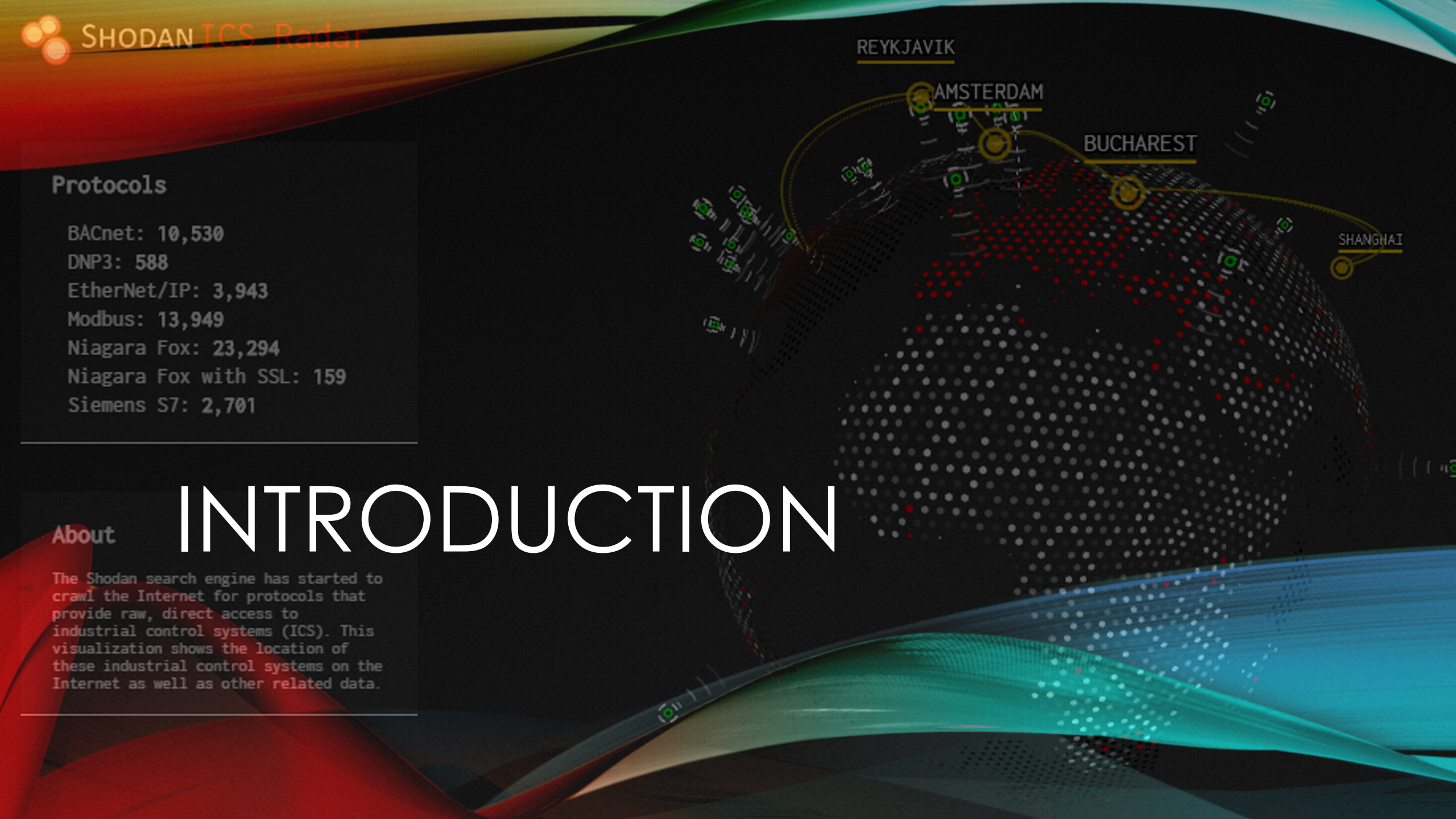
#ICSASIAPACIFIC

STRATEGIES FOR DEFENDING THE CYBER-PHYSICAL BATTLEFIELD

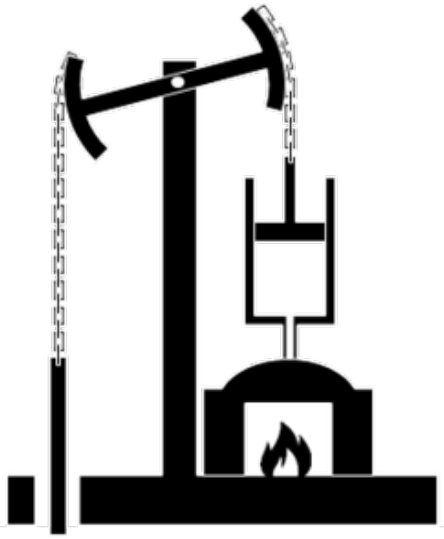
Huang Shao Fei, CISO, Singapore Land Transport Authority

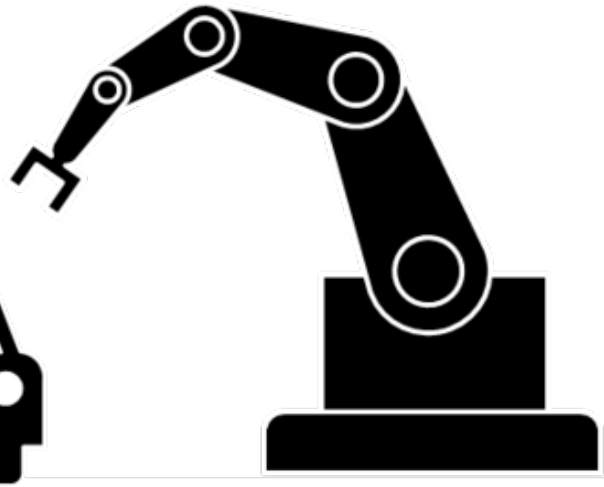
President, Singapore Computer Society Cybersecurity Chapter

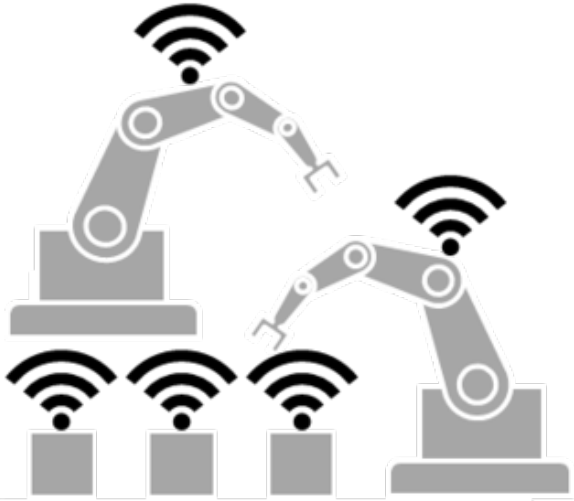
SANS | GIAC CERTIFICATIONS



INTRODUCTION







1st	2nd	3rd	4th
Mechanization, water power, steam power	Mass production, assembly line, electricity	Computer and automation	Cyber Physical Systems

3-5 years
economic lifespan

Standardised systems and
communication protocols

Recovery focuses on data
and system performance

Confidentiality, Integrity & Availability
of Information

Kinetic-Cyber consequences
(critical infrastructure)

Operational impact affecting safety

15-20 years
lifespan

Often outdated, proprietary or special
software and protocols

Recovery focuses on process control
and operational continuity

Safety, Processes
and Environment

Information Technology vs. **Operational Technology**

Extract from “The Dawn of Kinetic Cyber”

https://ccdcoe.org/uploads/2018/10/10_d2r1s4_applegate.pdf

- Cyber attacks are often called non-violent or non-kinetic attacks, but the simple truth is that there is a credible capability to use cyber attacks to achieve kinetic effects.

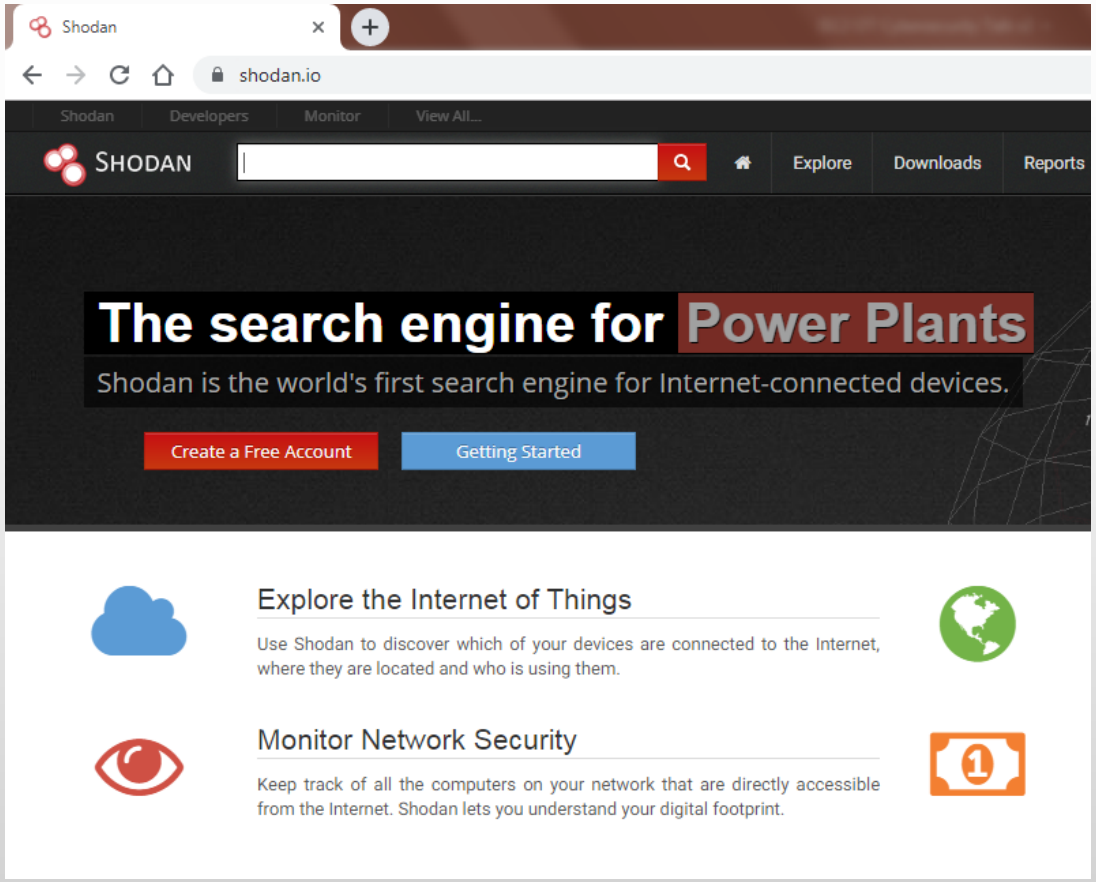
- **Kinetic Cyber** refers to a class of cyber attacks that can cause direct or indirect physical damage, injury or death solely though the exploitation of vulnerable information systems and processes.

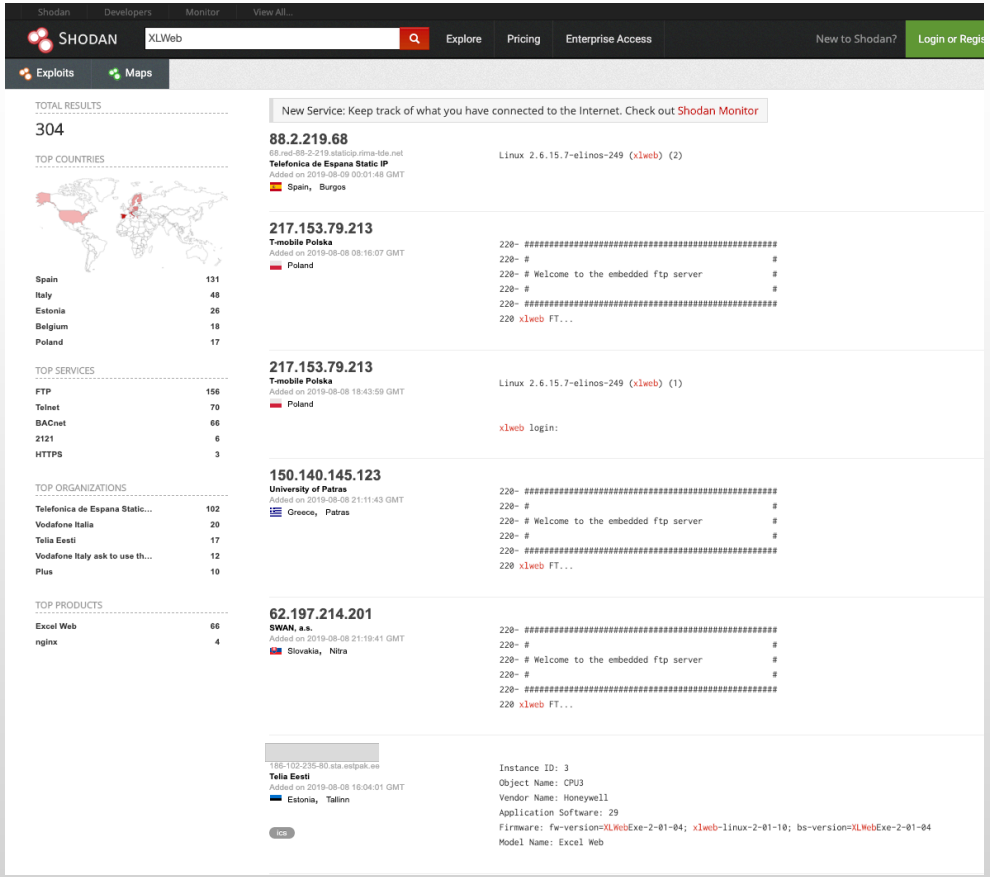
- The rapid growth and integration of **cyber physical systems** into everything from automobiles, aircraft and ships to SCADA systems implies a significant kinetic cyber threat in the near future.

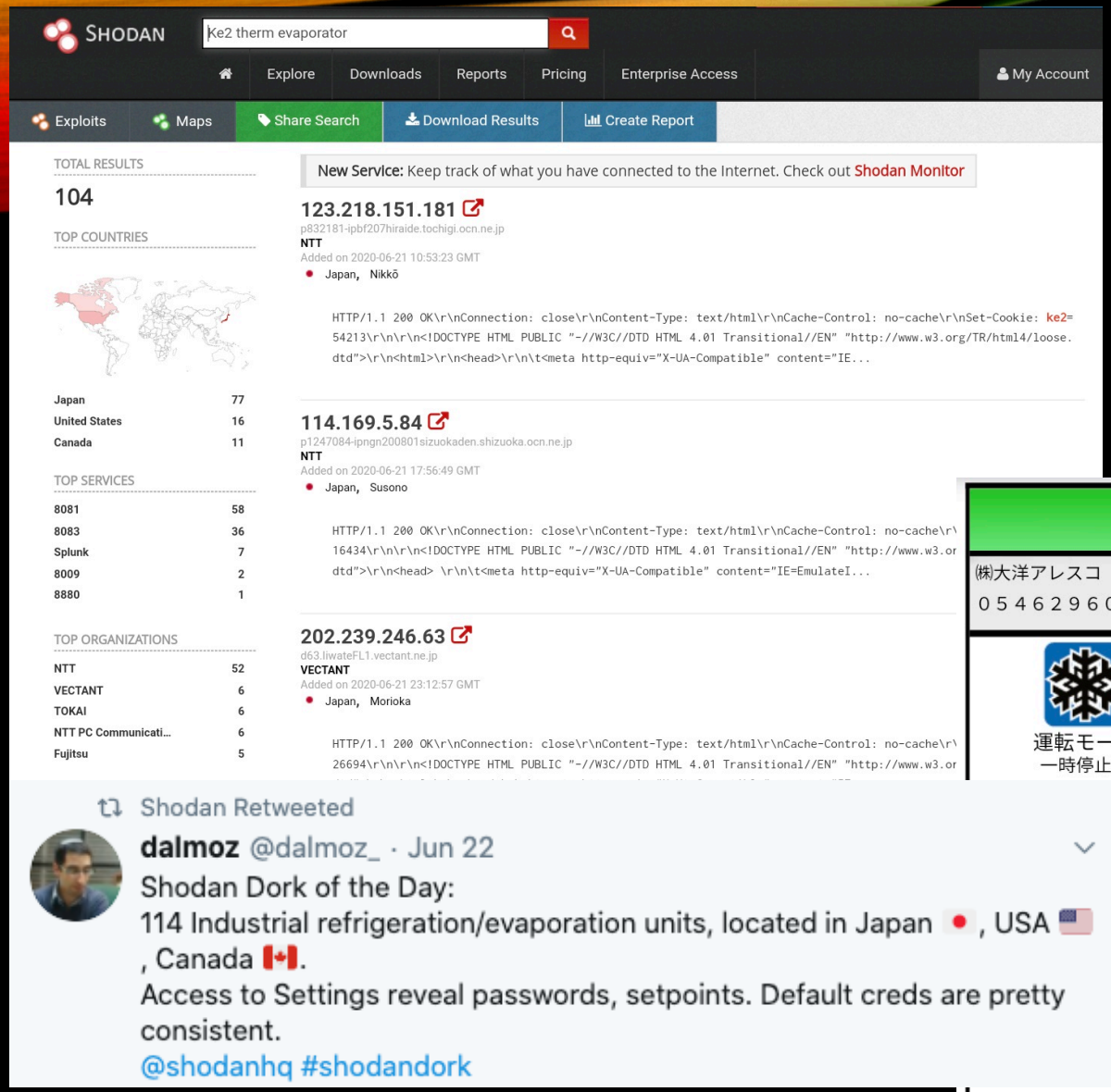
STATE OF OT/ICS CYBERSECURITY - TECH LIMITATIONS

- Not as straightforward as most IT systems - requires specialised domain knowledge e.g. engineering, train operations
- Safety-critical OT components cannot be patched like IT equipment - requires elaborate verification & validation
- Forensic investigations difficult, and in some cases, impossible
- Legacy technology e.g. floppy disk drives, serial-port modems
- Outdated Operating Systems, incompatible software and drivers
- Performance limitations (CPU, memory etc.)

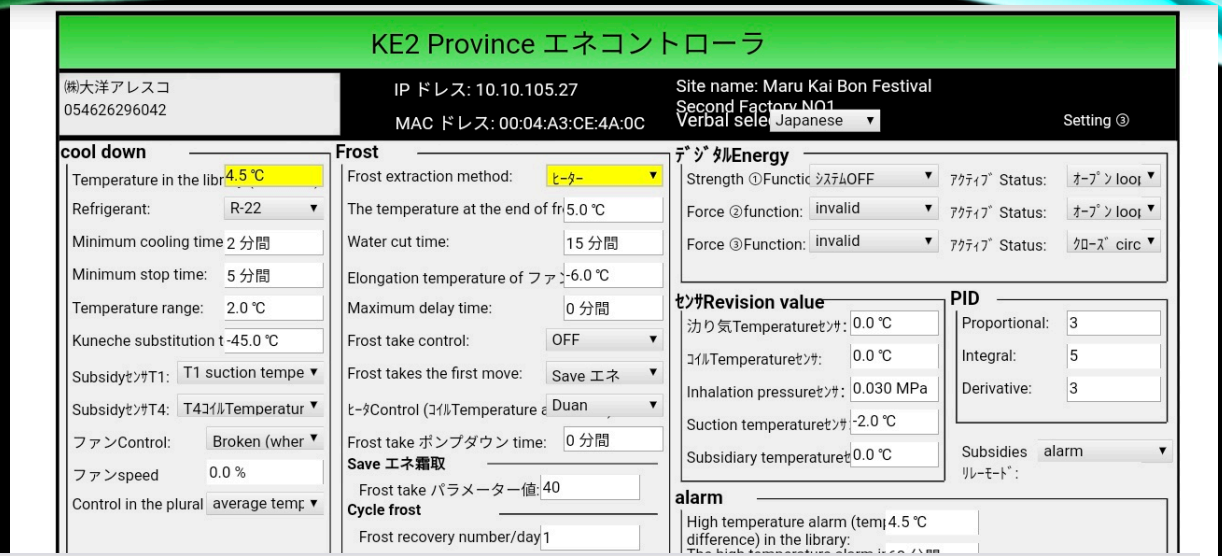
STATE OF OT/ICS CYBERSECURITY - ATTACK SURFACE++





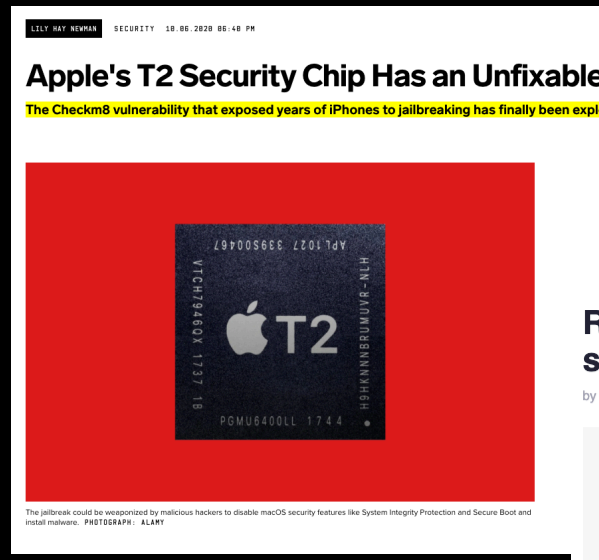


https://twitter.com/dalmoz_/status/1274939892431228928?s=20



STATE OF OT/ICS CYBERSECURITY - SUPPLY-CHAIN RISKS

- Unconventional, chain-linked threats that do not depend on one single attack vector.
- Supply-chain threats include Tier 2 and Tier 3 suppliers and sub-contractors that could compromise security, with organisations being the last one to find out they've been compromised.
- **Supply-chain challenges are especially acute in Operational Technology systems and may become worse.**

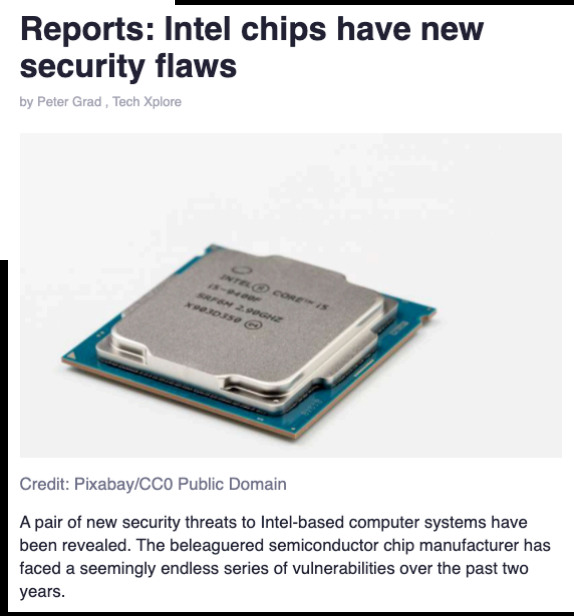


LILY HAY NEWMAN SECURITY 10.06.2020 06:40 PM

Apple's T2 Security Chip Has an Unfixable Flaw

The Checkm8 vulnerability that exposed years of iPhones to jailbreaking has finally been exploited in Macs as well.

The jailbreak could be weaponized by malicious hackers to disable macOS security features like System Integrity Protection and Secure Boot and install malware. PHOTOGRAPH: ALAMY



Reports: Intel chips have new security flaws

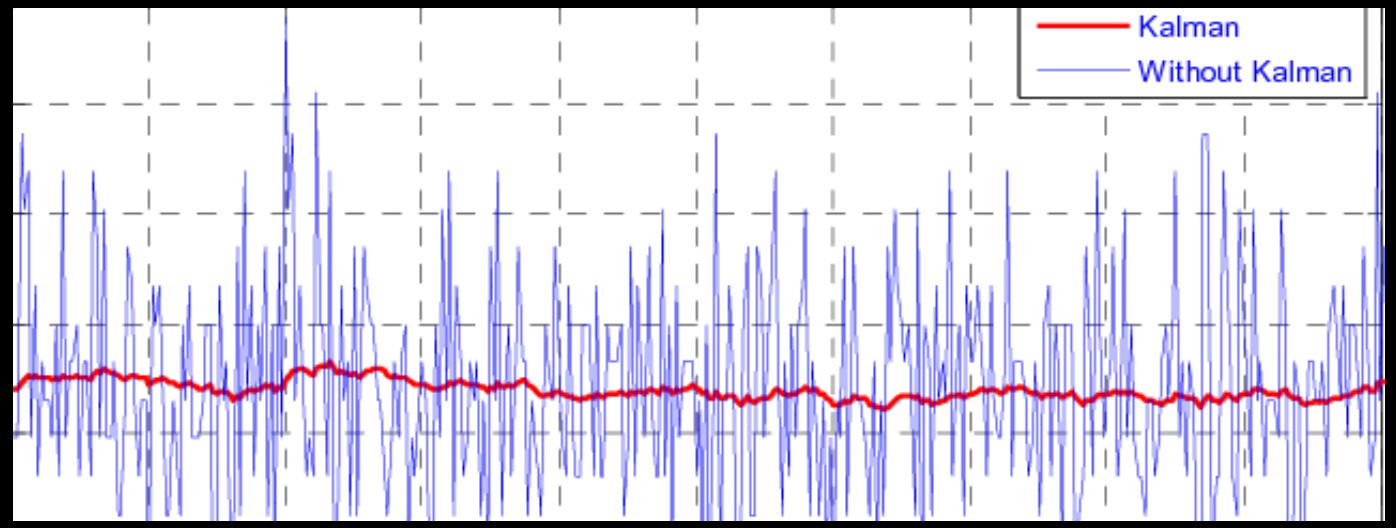
by Peter Grad , Tech Xplore

Credit: Pixabay/CC0 Public Domain

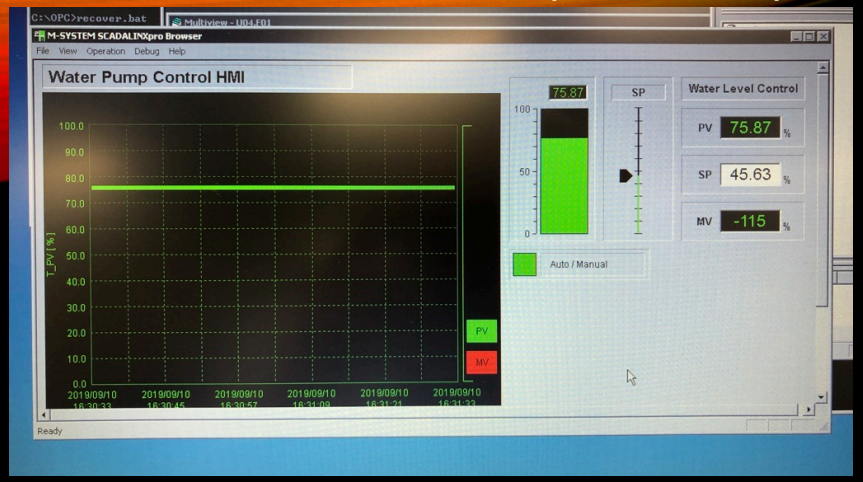
A pair of new security threats to Intel-based computer systems have been revealed. The beleaguered semiconductor chip manufacturer has faced a seemingly endless series of vulnerabilities over the past two years.

STATE OF OT/ICS CYBERSECURITY - MONITORING RISKS

- "Noise" tells you about the process and the sensor performance
- Noise is filtered out e.g. Kalman before the Serial-To-Ethernet converter
- Information about nuances of the processes and the sensors are not available for network anomaly detection



Operator's View (post-filter)




```
client = ModbusTcpClient('10.0.21.10', port=502)
client.connect()

result = client.read_coils(1,1)
print('Manual or Auto: ' + str(result.bits[0]))


result = client.read_coils(5,1)
print('Plus/Minus sigh: ' + str(result.bits[0]))


Rr = client.read_holding_registers(address=0,count=1,unit=1)
PV = float(Rr.registers[0])
print('PV(mm) = %f' % PV)

client.write_register(address=1,value=5000,unit=1)

# to make fake indicator
client.write_register(address=11,value=20000,unit=1)
client.write_register(address=12,value=00000,unit=1)

time.sleep(1)

# Read value
SVr = client.read_holding_registers(address=1,count=1,unit=1)
SV= float(SVr.registers[0])
print('SV(%%) = %f' % SV)

RHr = client.read_holding_registers(address=11,count=1,unit=1)
RH = float(RHr.registers[0])
print('RH(mm) = %f' % RH)

RLr = client.read_holding_registers(address=12,count=1,unit=1)
RL = float(RLr.registers[0])
print('RL(mm) = %f' % RL)
```

Hacker's View

Factory Floor (Process Datal)

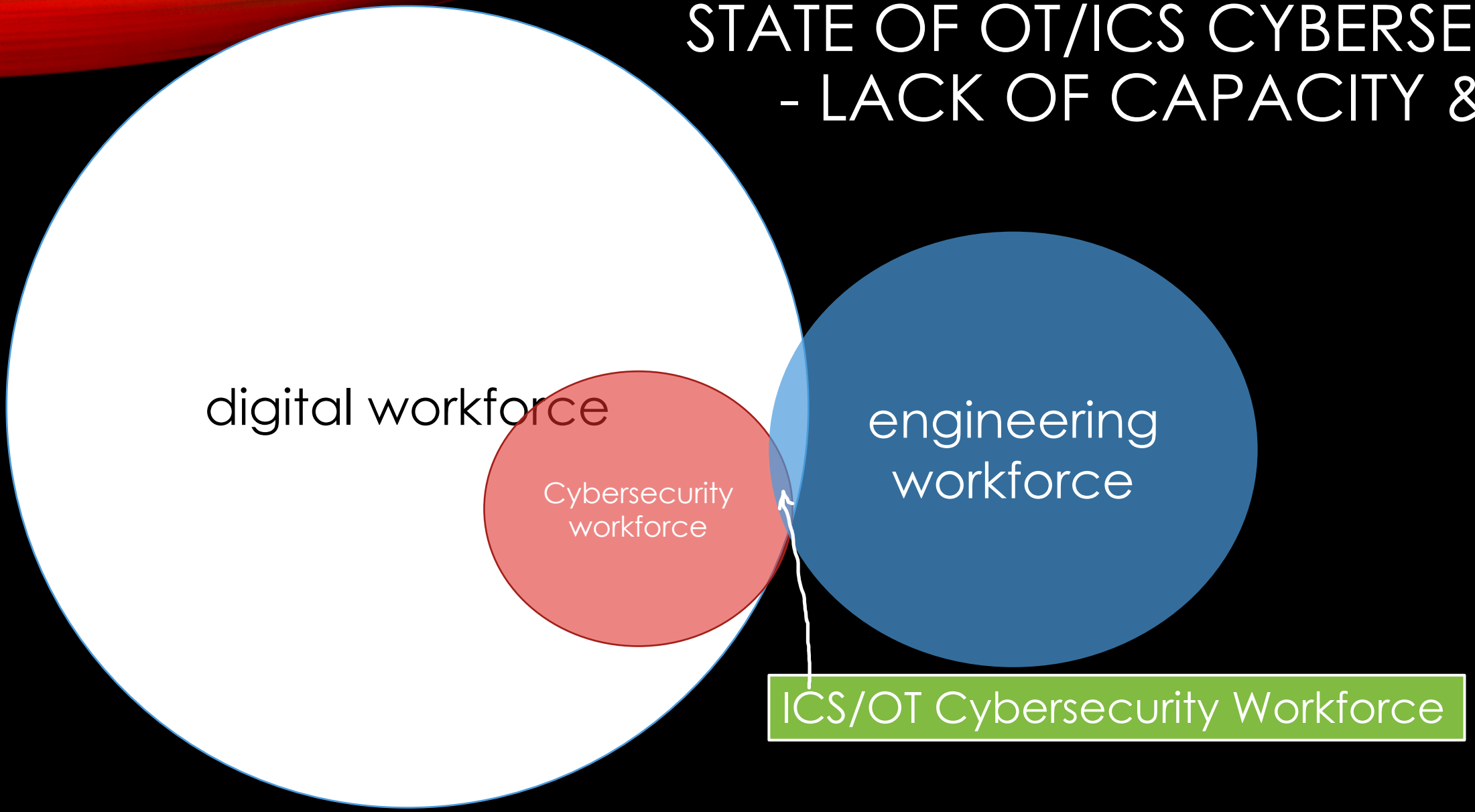
OT cyber monitoring is not sufficient to identify many significant control system cyber incidents

Submitted by Joe Weiss on Mon, 01/27/2020 - 23:01

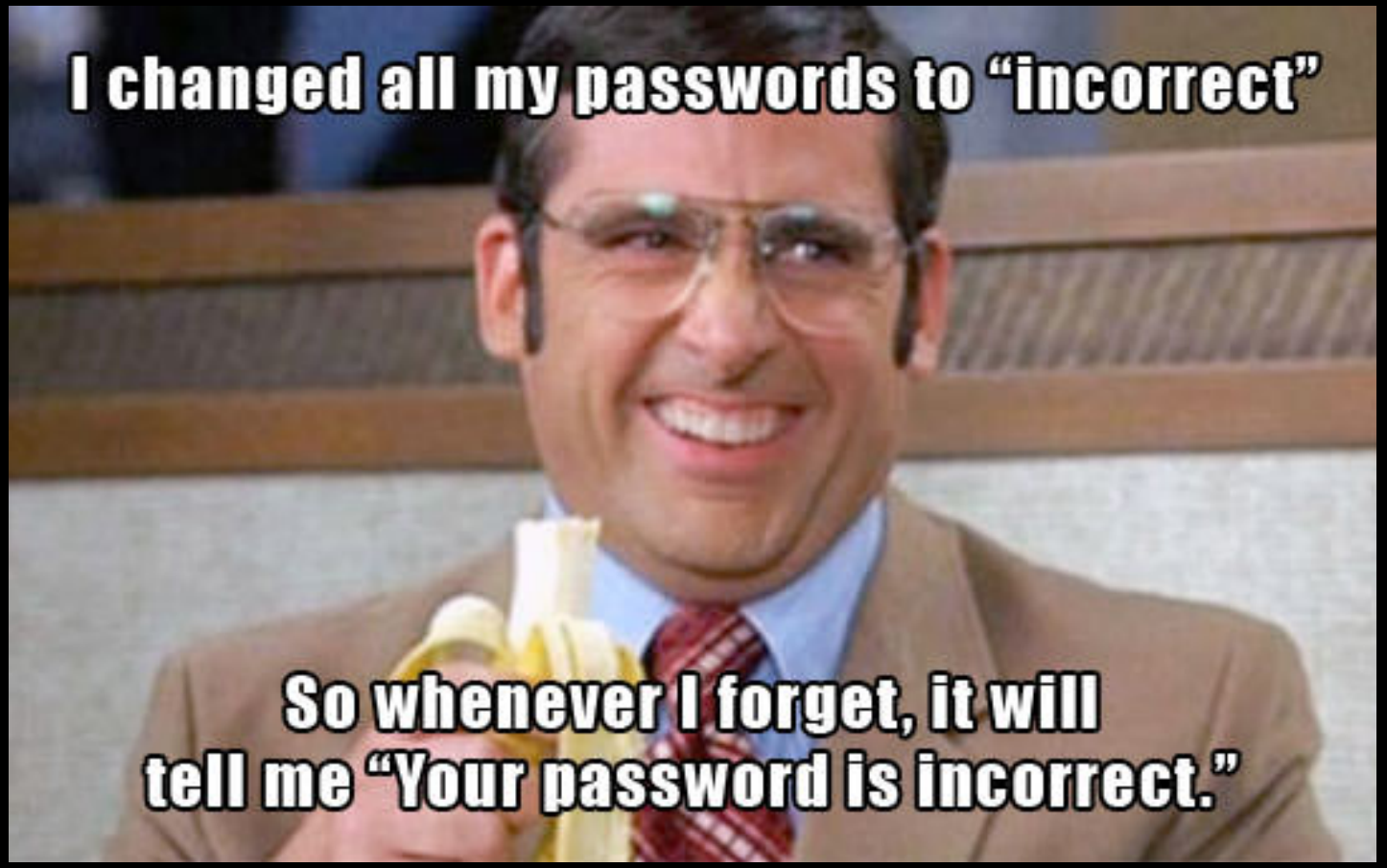
A major news organization contacted me about my control system cyber incident database. I have been very clear the database is not public but I could provide sanitized information. Until now, that was not sufficient to get media interest as they wanted names. Since this news organization was willing to go without names, I provided sanitized summaries of 20 actual cases. I chose a combination of cases representing domestic and international, unintentional and malicious, multiple industries (e.g., power, water, pipelines, transportation, etc.), and various levels of impact (e.g., business disruption, major environmental spills, major blackouts, catastrophic failures including deaths, etc.) An important finding was many cases would NOT have been detected from OT network monitoring as these were control system cyber incidents. This is a clarion cry for training the control system engineers to question when incidents happen if they could be cyber-related. This becomes very important as sophisticated hackers can, and have, made cyber attacks look like equipment malfunctions.

Joe Weiss

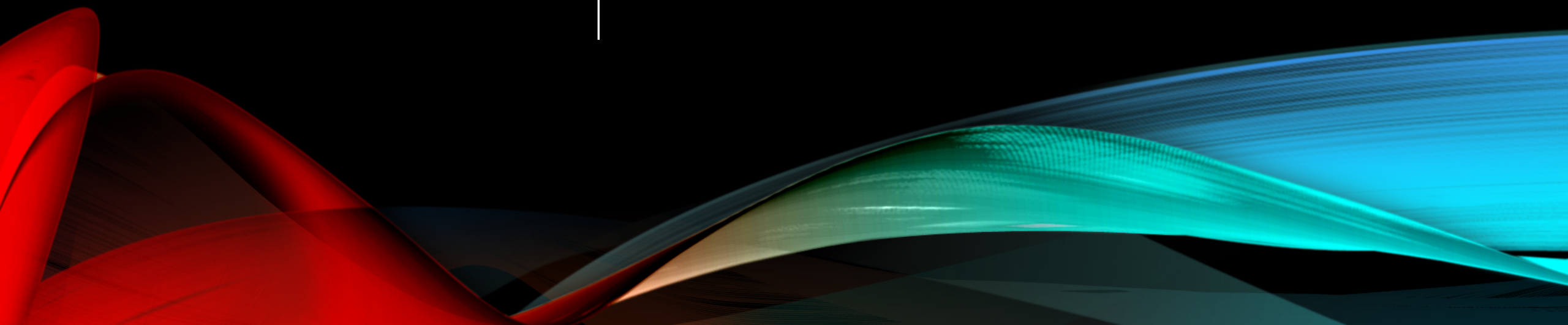
STATE OF OT/ICS CYBERSECURITY - LACK OF CAPACITY & SKILLS



STATE OF OT/ICS CYBERSECURITY - CULTURE & MINDSET



IMPLEMENTING AN OT CYBER DEFENCE STRATEGY



Recap of OT Cybersecurity Masterplan

SINGAPORE'S OPERATIONAL TECHNOLOGY CYBERSECURITY MASTERPLAN 2019

- ✓ Announced at the opening of SICW 2019
- ✓ Outlined efforts to **enhance the cyber resilience** of OT stakeholders, **improve cross-sector responses** and **strengthen partnerships with industry and stakeholders** by driving multiple OT cybersecurity initiatives to address key challenges and emerging cyber threats in the OT environment

"The Masterplan will guide the development of capabilities to secure systems in the OT environment, and mitigate emerging OT cyber threats."

SM Teo Chee Hean - SICW 2019

Overview of Masterplan's Key Thrusts

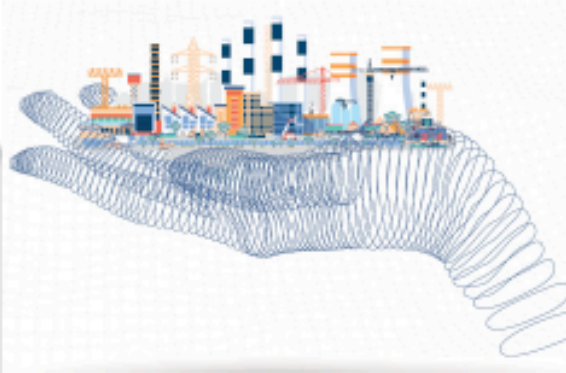
The OT cybersecurity masterplan outlines the key thrusts to uplift the cybersecurity posture of people, process and technology of OT stakeholders. Key thrusts include:

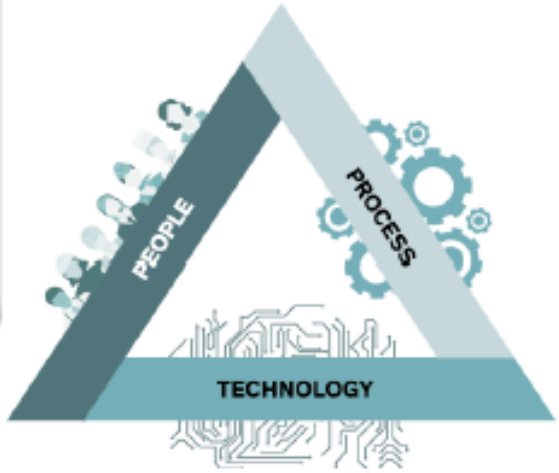
Key Thrust 1: OT Cybersecurity Training

Key Thrust 2: OT Cybersecurity Information Sharing and Analysis Center (OT-ISAC)

Key Thrust 3: Strengthening Policies and Processes

Key Thrust 4: Adopting Technologies for Cyber Resilience





KEY THRUST 1: OT CYBERSECURITY TRAINING

1. Make cybersecurity training an organization-level priority.
2. Focus on incremental efforts, do not try to change the world overnight.
3. Reward and reinforce positive behaviours.
4. Make content engaging and relatable.

KEY THRUST 3: STRENGTHEN POLICIES AND PROCESSES

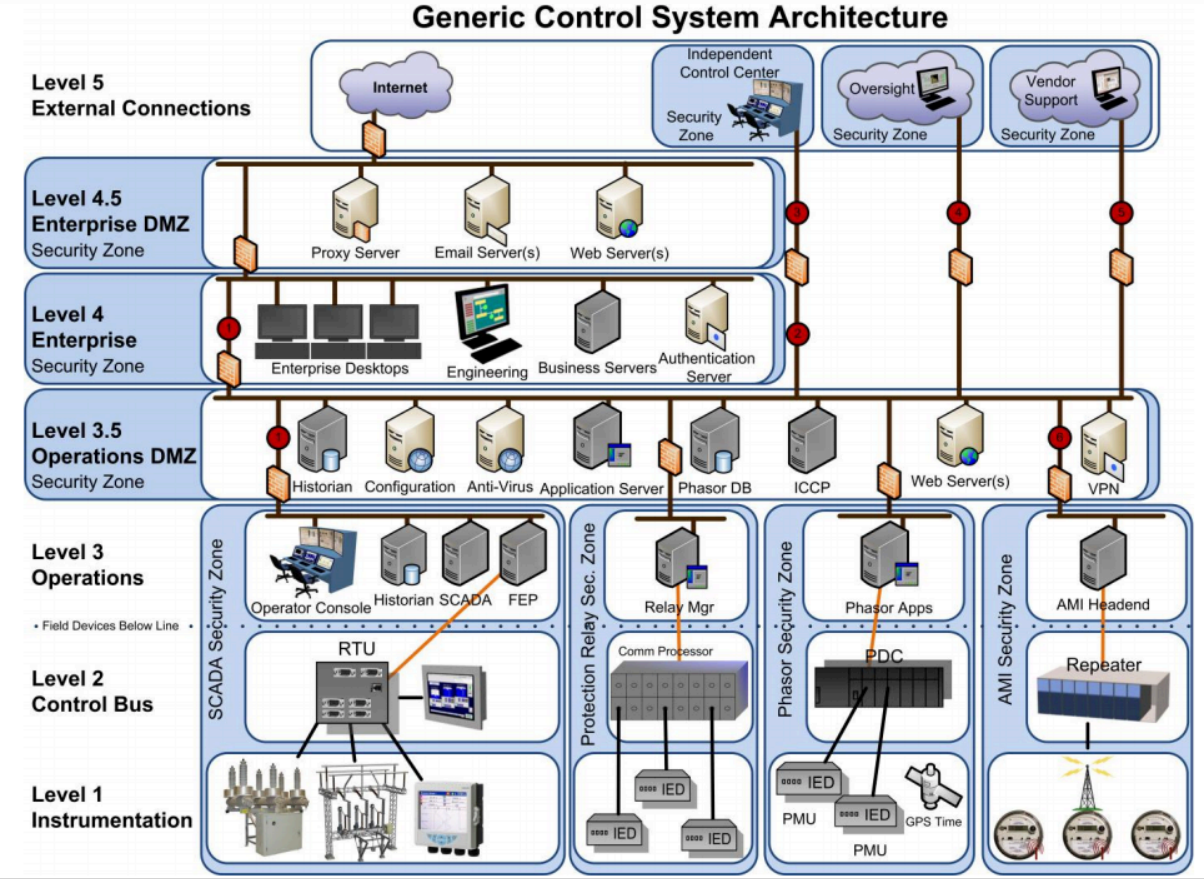
- Framework focusing on using business drivers to guide cybersecurity activities and considering cybersecurity risks as part of the organization's risk management processes.

- Knowing where you / your organisation is at (in terms of cyber maturity) is important, but do not set unrealistic goals.

- **NIST Cybersecurity Framework Version 1.1**

  https://www.nist.gov/cyberframework/framework

SURVEY THE BATTLEFIELD

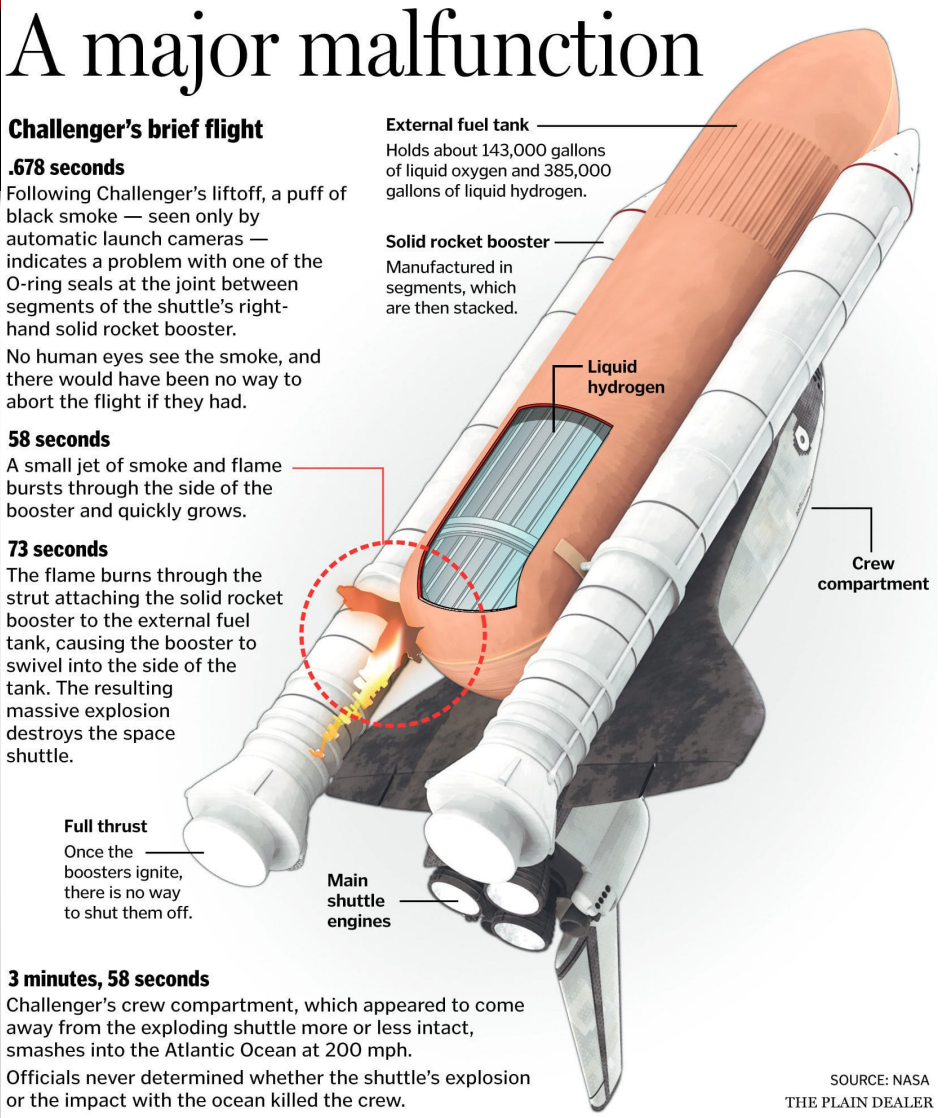


- Inventorize and understand what needs to be protected
- Differentiate between end-points that need raw data and those that need information
- Consider carefully decisions related to safety-critical equipment, and involve stakeholders early

https://www.pnnl.gov/main/publications/external/technical_reports/PNNL-20776.pdf

The consensus of the Commission and participating investigative agencies is that the loss of the Space Shuttle Challenger was caused by a failure in the joint between the two lower segments of the right Solid Rocket Motor. The specific failure was the destruction of the seals that are intended to prevent hot gases from leaking through the joint during the propellant burn of the rocket motor.

EXPLOIT POWER OF **DATA**



Dataset	Inference from data	Decision	Result
Selective Data *(actuality)*	Low temperatures have little to no effect on O-ring failure rate	Allow space shuttle launch at low temperatures	Space Shuttle Challenger explosion leading to 7 deaths
All Data *(ideal)*	Low temperatures have a substantial effect on O-ring failure rate, especially as all launches below 65° had O-ring issues	Don't allow space shuttle launch at low temperatures, due to the substantially elevated risk of failure	*Unknown*; likely, significantly lower risk of O-ring failure and subsequent explosion

https://priceonomics.com/the-space-shuttle-challenger-explosion-and-the-o/

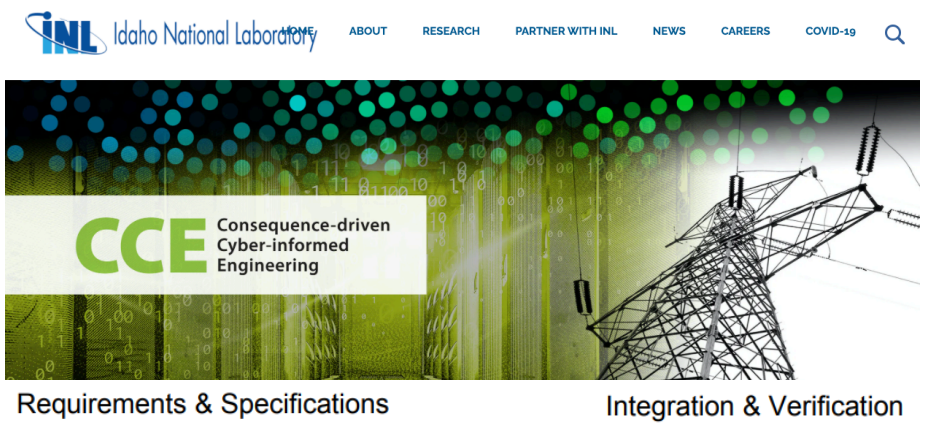
- The problem with most ICS/OT environments today is not the lack of data, but the overwhelming volume of "dirty" data
- Focus on building up cyber threat detection and response capability (and importantly, data analytics)
- Detecting "signals" from the noise

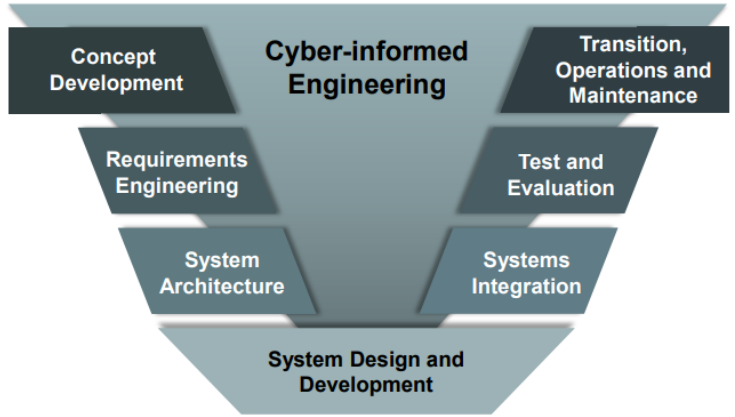
ALIGN YOUR STRATEGY

- ICS/OT systems generally engineered against **deterministic** outcomes, backed by evidence
  - Safety cases are a good example of this (https://en.wikipedia.org/wiki/Safety_case)
  - "A vehicle safety case may show it to be acceptably safe to be driven on a road, but conclude that it may be unsuited to driving on rough ground, or with an off-center load for example, if there would then be a greater risk of danger e.g. a loss of control or an injury to the occupant."
- Cyber-attacks (i.e. rogue threats) often produce **random** outcomes, never observed before during testing
- Strategies must be ALIGNED to operational and safety risks, and remain reasonably practical

KEY THRUST 4: ADOPT TECH FOR RESILIENCE

- **Consequence-driven Cyber-informed Engineering (CCE)** is a methodology focused on securing the nation's critical infrastructure (CI) systems
- Developed at Idaho National Laboratory, CCE begins with the assumption that if CI is targeted by a skilled and determined adversary, the targeted operation can – *and will* – be sabotaged
- Consequences in ICS/OT are largely engineering and domain-specific. Compare to information security (C.I.A. triad)
- Manage legacy tech by focusing on safety-directed cybersecurity goals i.e. reach a **Safe State**





http://inl.gov/cce

- Institutionalize cybersecurity policies & processes to inculcate good cybersecurity hygiene.

Cyber Processes

- Stand up CERT capabilities to defend systems and skills to face cyber threats.

Cyber Capacity

- Conduct training to educate people and suppliers with awareness and skills to face cyber threats.

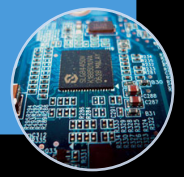
Cyber Competency

- Equip systems with cyber tools to protect networks and repulse cyber attacks.

Cyber Tools

- Explore and adopt advanced technologies to sharpen cybersecurity capabilities and operational readiness.

Cyber Technology



No 100% Cybersecurity - Multi-Layered Strategy is Key!

"Think like a **hacker**, but act like an **engineer**"

- Marty Edwards, former Director, US ICS CERT

THANK YOU

And Stay Safe And Healthy!

Connect with me on LinkedIn -
http://www.linkedin.com/in/shaofei