RSAConference2020
Asia Pacific & Japan

A Virtual Learning Experience | 15–17 July

HUMAN ELEMENT

SESSION ID: **AIR-F06V**

Intelligence Sharing for Critical Infrastructure Resiliency

John Lee

Managing Director
GRF Asia-Pacific
OT-ISAC@OT-ISAC

KEY TAKEAWAYS

- Why is Operational Technology Security Importance?
- Securing Operational Technology
- Case Study on Information (Intelligence) Sharing

RSAConference2020 APJ

A Virtual Learning Experience

Importance of Operational Technology Security

Critical Infrastructure (CI)

CIs' defined according to a nation's needs, resources and development.

In Singapore the 11 critical infrastructure sectors are (1) Government, (2) Infocomm, (3) Energy, (4) Aviation, (5) Maritime, (6) Land Transport, (7) Healthcare, (8) Banking & Finance, (9) Water, (10) Security and Emergency, and (11) Media.



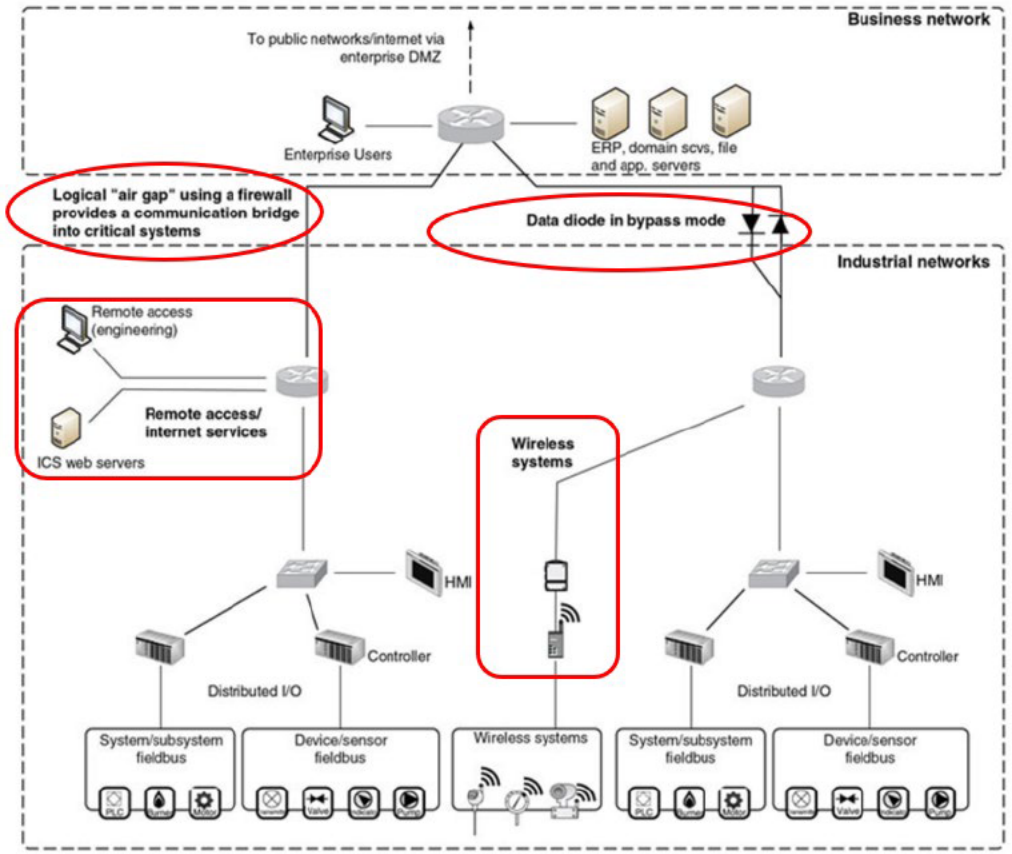


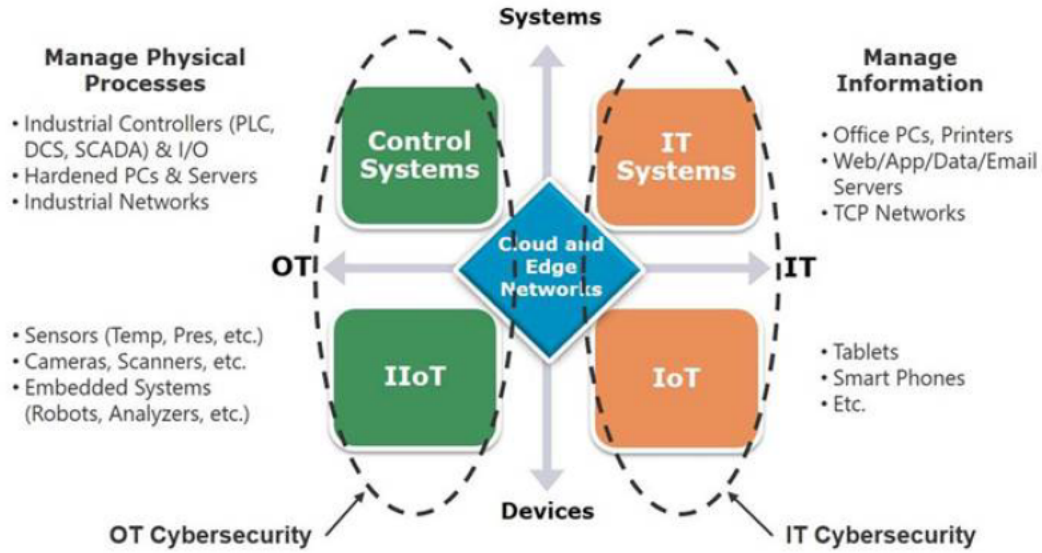

USA has 16 critical infrastructure sectors https://www.cisa.gov/critical-infrastructure-sectors

The impact of a breach to Critical Infrastructure can have serious repercussions such as disruptions to daily life, physical harm and financial consequences.

Industrial Control Systems (ICS) are more exposed

Legacy ICS are air-gapped. ICS today are increasingly connected to the Internet for efficiency and remote monitoring.





OT systems are built for reliability, functionality and safety. Security is getting prioritized due to the increasing attacks.

Notable ICS Attacks (non exhaustive)

Cyber Attacks on ICS are increasing

Year	Target	Impact
2010	Iranian Nuclear Plant	Targeted PLCs and destroyed connected centrifuges
2012	Saudi National Oil Company	30,000 workstations affected and needed to be restored.
2014	German Steel Mill	Breakdown of Control System causing physical damage
2015	Ukranian Power Grid	Loss of power to about 225,000 consumers
2016	New York Dam	SCADA system connected to the Internet was targeted.
2017	Saudi Petrochemical Plant	Safety Instrumentation Systems targeted. Force Plant shutdown.
2019	Hydro Norsk	Ransomware encrypted thousands of servers and PCs that impacted production facilities. Financial impact more than $71m.

There are 94 APT groups documented by MITRE.
https://attack.mitre.org/groups/

Some of them:

- APT1 (Unit 61398 linked to PLA)
- APT28 (Fancy Bear, Russian)
- APT29 (Cozy Bear, Russian)
- Dragonfly/Dragonfly2 (espionage targeting defense, aviation, ICS)
- Sandworm (espionage targeting energy, government, media)

Recent Threats to ICS (1) – LOSS OF REVENUE

Alert by CISA in February 2020. US Natural Gas Facility was hit by Ransomware

Impact: 2 days shutdown leading to a loss of revenue

Kill Chain	Tactic	Technique	
Delivery	Initial Access	T1192- Spear phishing attachment	Spear Phishing email
Installation	Impact	T1486 (Data Encrypted for Impact)	Ransomware
		T826 (Loss of Availability)	Assets (HMI, Historians, Polling Servers) on OT Network could not read/aggregate data from OT devices
		T829 (Loss of View)	Human operators had no visibility
		T828 (Loss of Productivity & Revenue)	PLCs were not impacted or major loss of operations suffered. However the operations were shut down for 2 days.

Recent Threats to ICS (2)- SAFETY

Israel Water Facilities suffered a Cyber Attack in April 2020

Impact:

- 6 plants were hit with the intention to disrupt the water operations.
- Data was wiped in a plant,
- Another plant had one of the pumps running in auto mode prompting a shutdown by operators,
- There was also unplanned change in data in the facility

There may be grave consequences if the attackers could get into the systems that controlled the level of chlorine added to the water. It could have led to poisoning of the water and loss of lives.

OT Cybersecurity is a growing concern

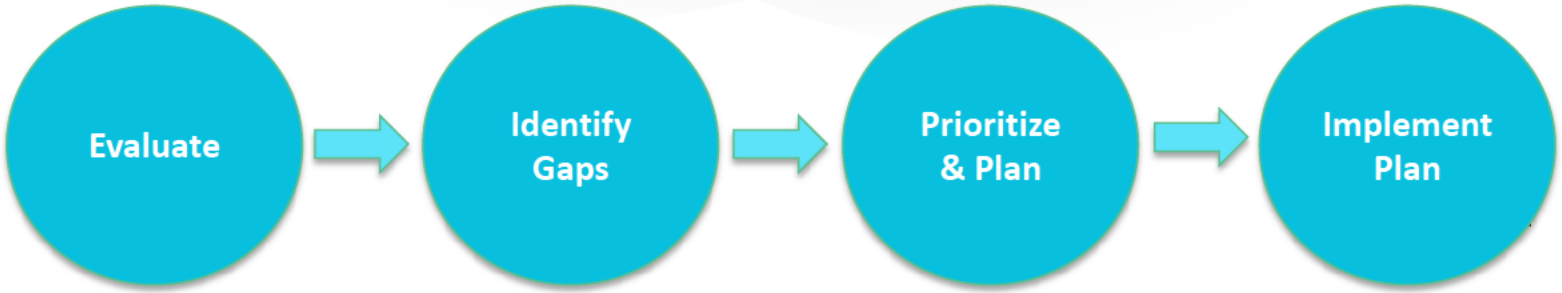
- 90 % suffer one or more attacks in past 2 years
- 62 % considers identifying OT and IOT assets an important KPI
- 60 % are worried against an attack against OT infrastructure
- 67 % state that ability to keep up with sophisticated attackers is important
- 80 % attribute the importance of threat intelligence sharing

Cybersecurity in Operational Technology: 7 insights you need to know (Ponemon Institute)-March 2019

Cyber Security Maturity Model (developed by DOE)

Current state of maturity vs Desired future state = Gap to be addressed

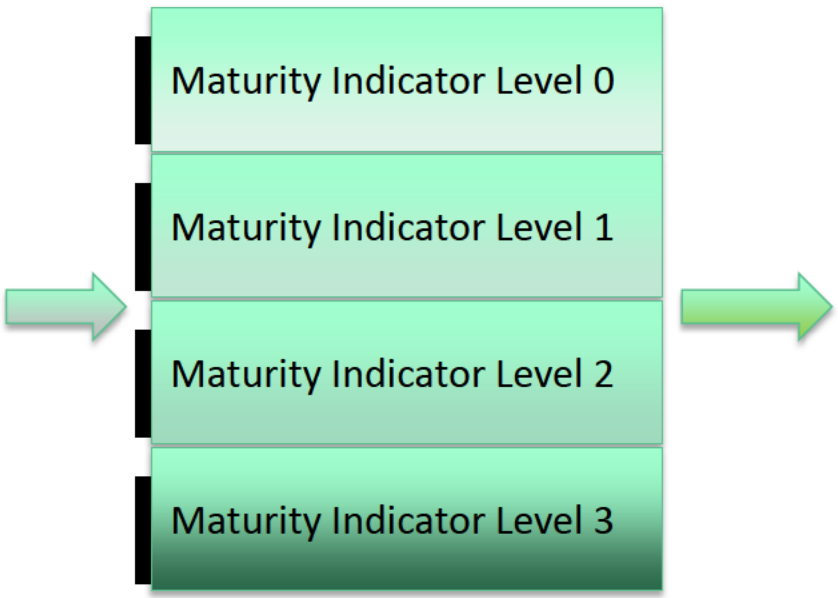
ASSESSMENT PROCESS



SCOPE OF ASSESSMENT

10 DOMAINS

- RISK
- ASSET
- ACCESS
- THREAT
- SITUATION
- RESPONSE
- DEPENDENCY
- WORKFORCE
- ARCHITECTURE
- PROGRAM

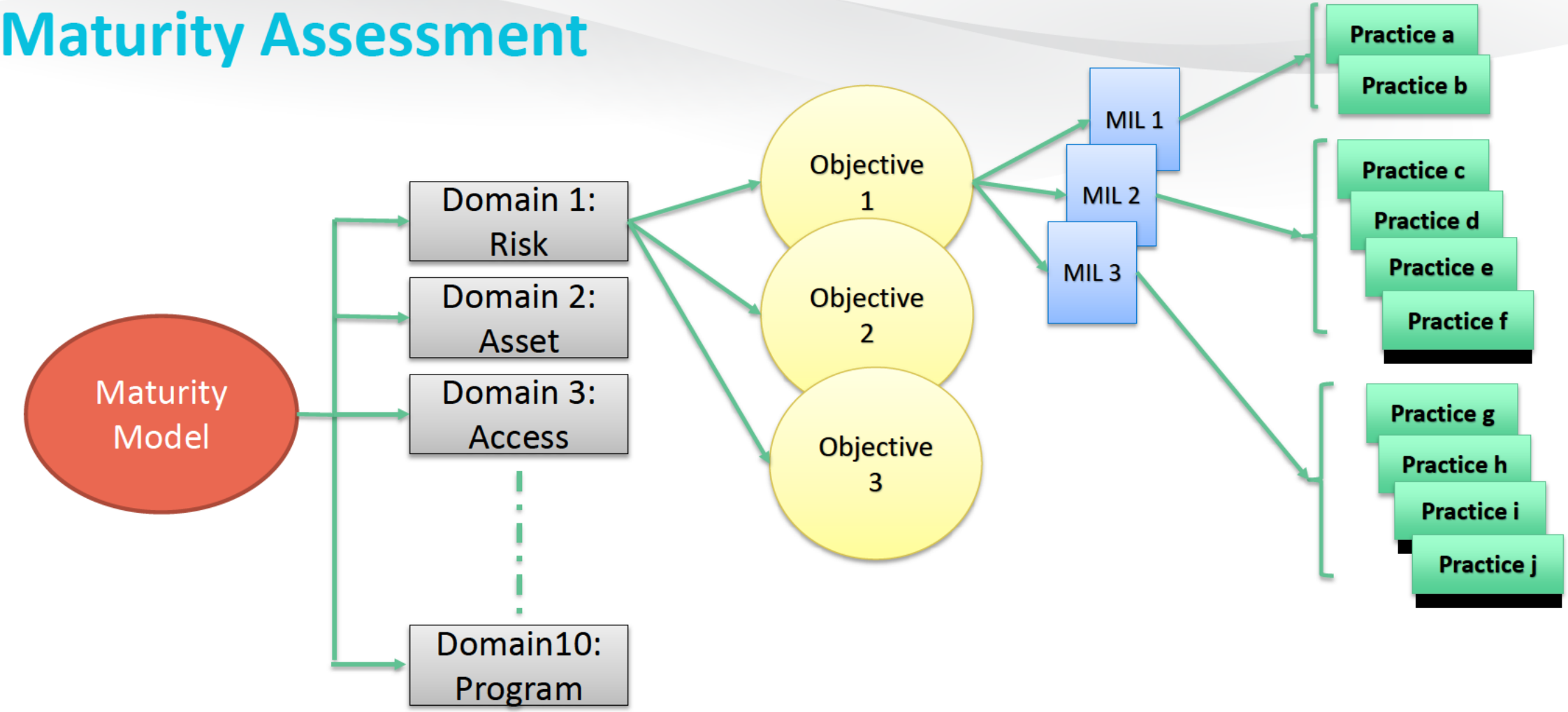


Domain + MIL level

Ex. THREAT 2d indicates maturity level 2d of the Threat domain.

https://www.energy.gov/sites/prod/files/2019/08/f65/C2M2%20v2.0%2006202019%20DOE%20for%20Comment.pdf

Maturity Assessment

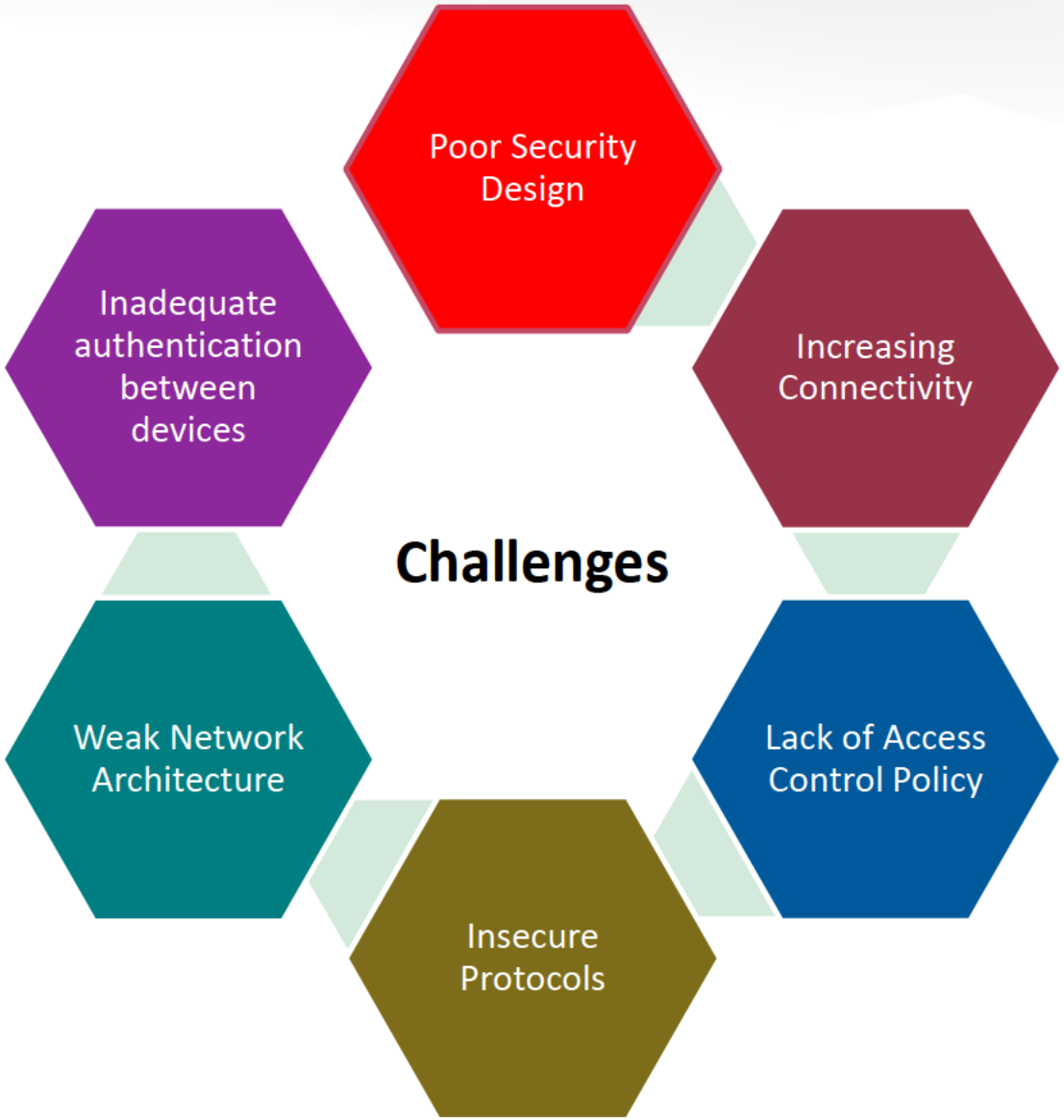


Example: Assessment Rating is specified as [Domain]-[Objective][Practice]
RISK-1d means for RISK Domain Objective 1 practice d is noted.
It will get a rating of MIL 2 (Maturity Indicator Level 2).

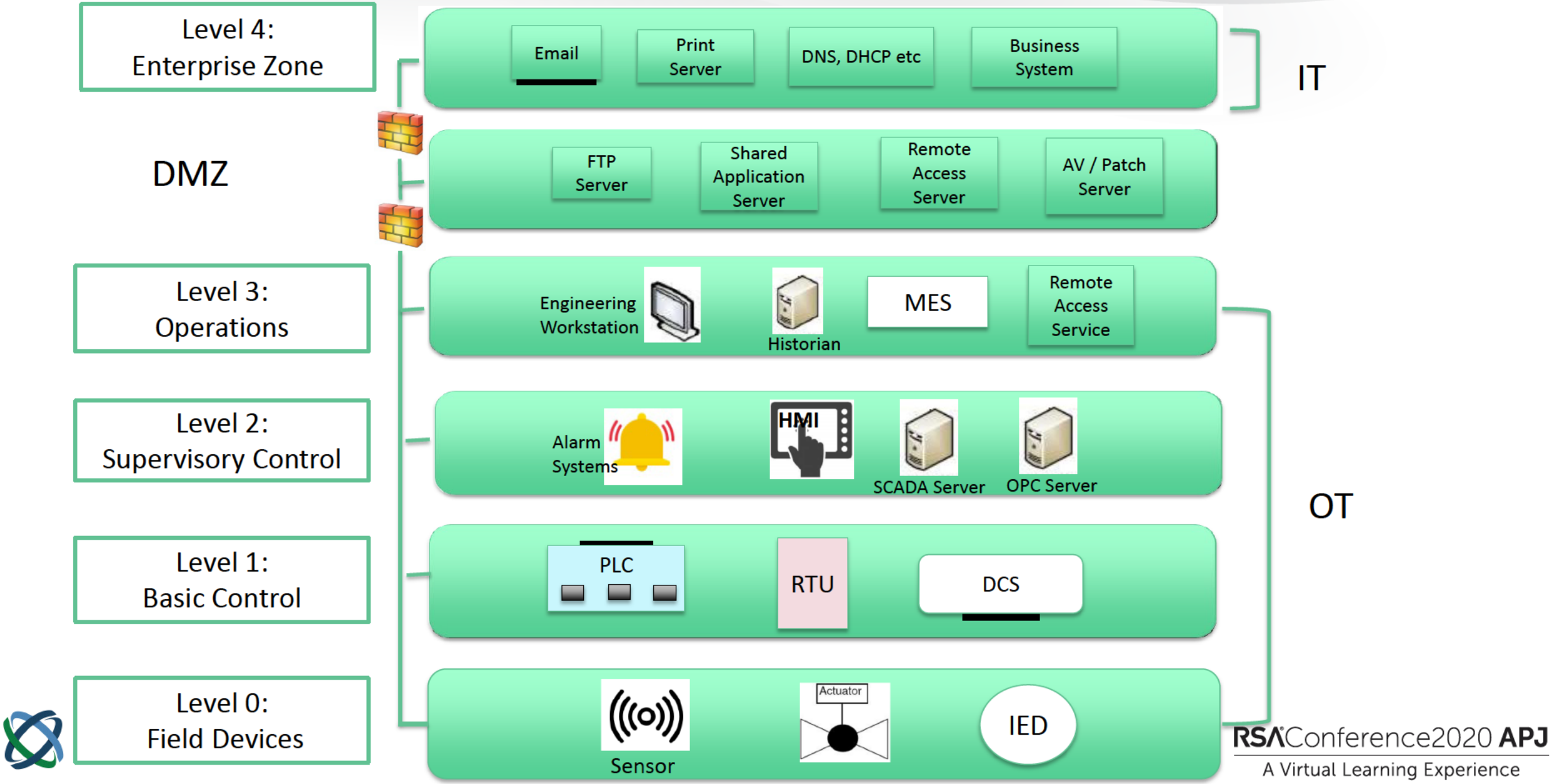
RSAConference2020 APJ
A Virtual Learning Experience

Securing Operational Technology

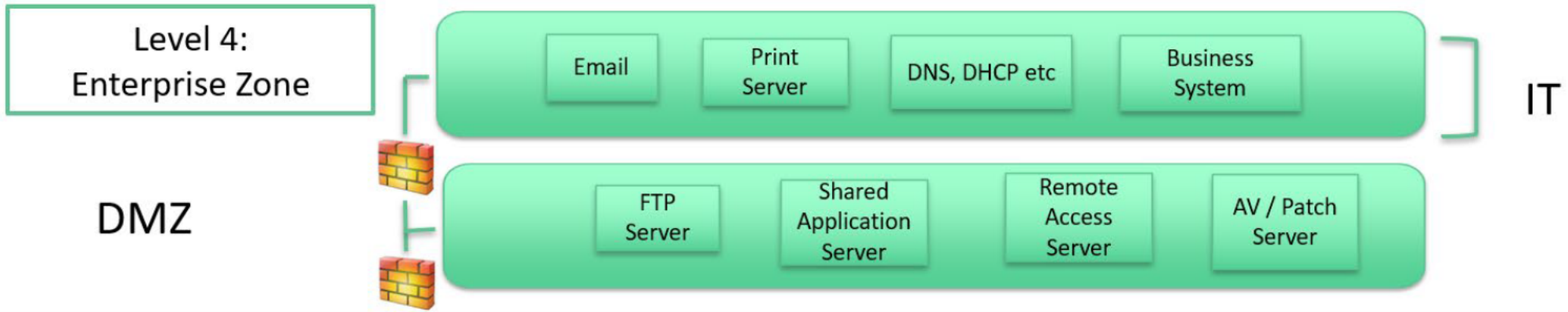
Common ICS Vulnerabilities



Industrial Network Architecture (Purdue Model)



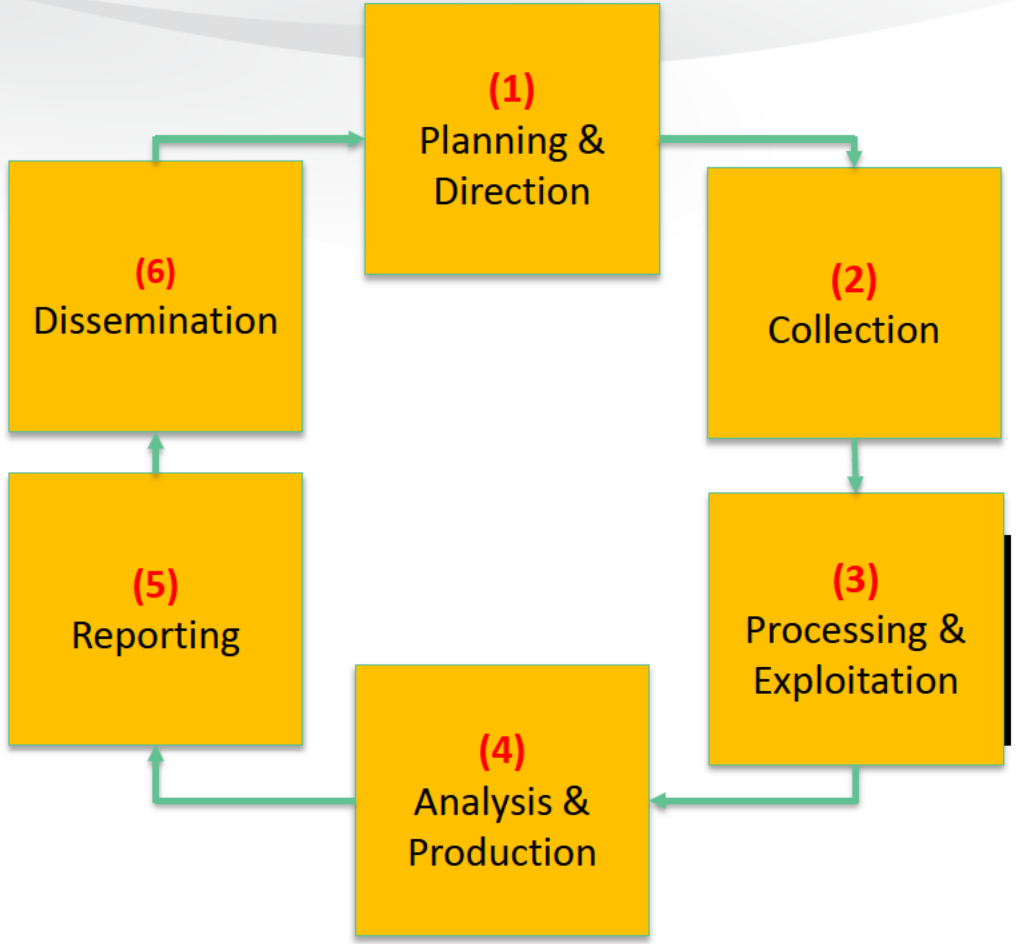
Industrial Network Architecture (Purdue Model)



LACK OF VISIBILITY IN THE OT NETWORK POSES SECURITY CHALLENGES.

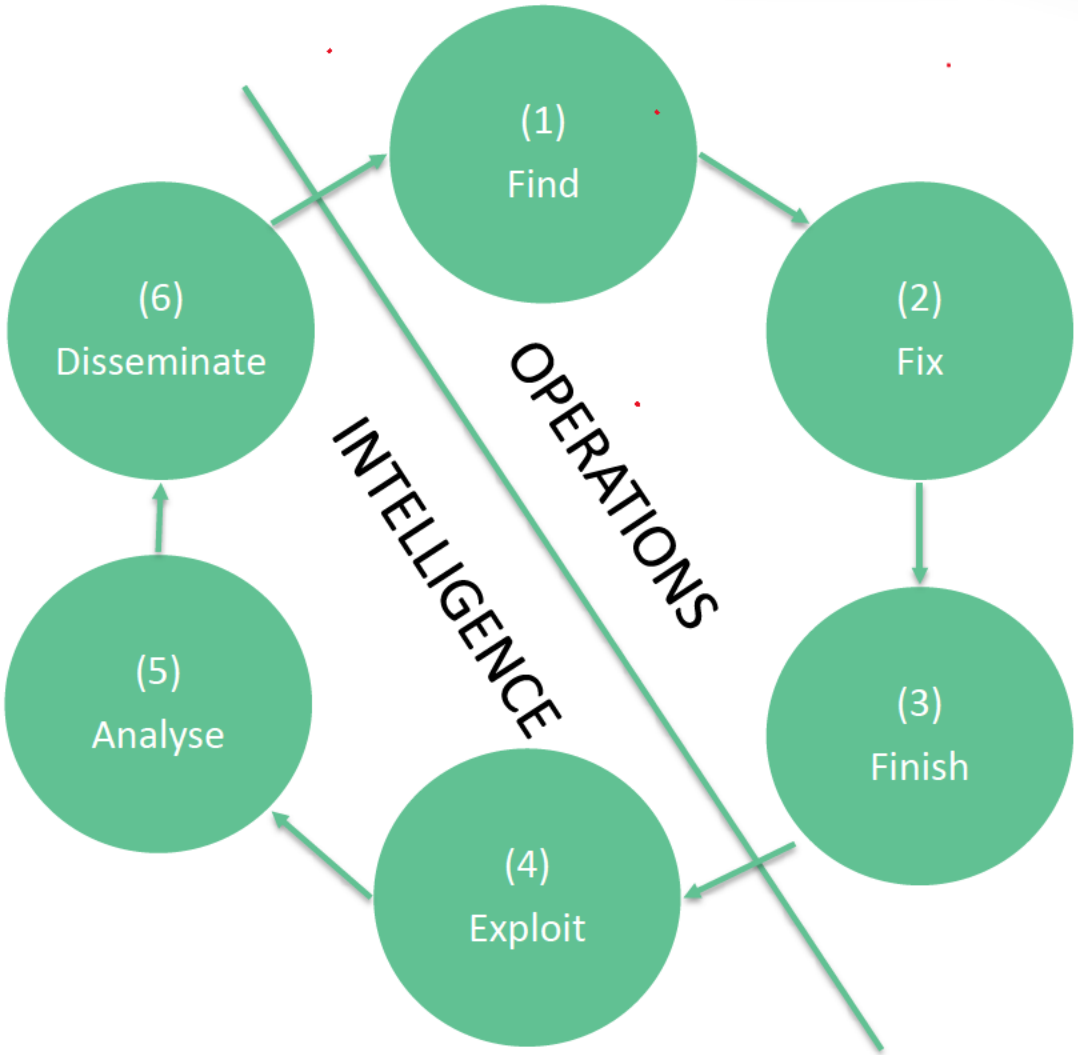
Threat Intelligence Cycle

Intelligence Pyramid



Actionable Threat Intelligence can increase cyber security and resilience.

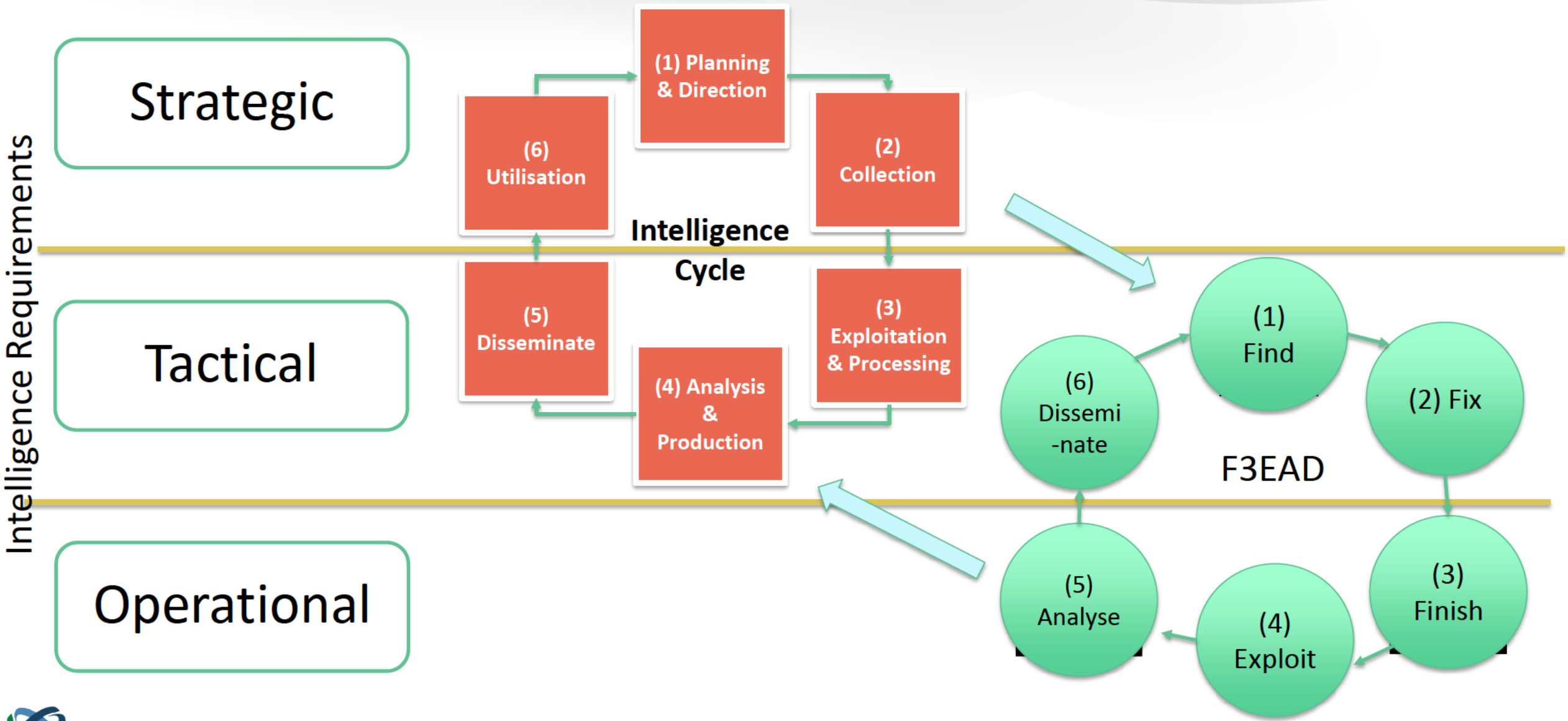
F3EAD Framework (complementary to Intelligence Cycle)



Focus on the tactical and operational aspects of Intelligence requirements

FIND	What is the threat
FIX	What is the solution
FINISH	Deploy the solution
EXPLOIT	Collect and enhance information of the threat
ANALYSE	Analyse and enrich the collected information
DISSEMINATE	Share the Intelligence with stakeholders

Threat Intelligence Cycle & F3EAD Integration



RSAConference2020 APJ

A Virtual Learning Experience

Case Discussion:
Information (Intelligence) Sharing

OT-ISAC Information Sharing Pathways

PUBLIC SOURCES
- CERT ALERTS
- REGULATORS
- LAW ENFORCEMENT
- AGENCIES

Members Sharing
- Incidents
- Forums
- RFIs

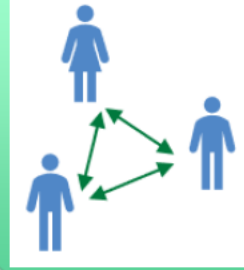
PRIVATE SOURCES
- GOVERNMENT
- THREAT INTEL VENDORS
- DARK WEB VENDORS
- VULNERABILITY VENDORS

Cross Sector Sources
- Affiliated ISACs, ISAOs
- Partners

How Members Share Information

Workshops,
Training, Seminars

Participate in
member events



OT-ISAC
Members

Secure Sharing and
Receiving of Intelligence
(follow TLP)

Monthly
Threat Calls

Mobile
Platform

Web
Portal

Traffic Light Protocol

OT-ISAC Incident Sharing Process

The entire process can be completed within 1 or 2 days depending on the criticality of the threat. The members get early warning of the potential threats and can take action.

(1) Member share incident or threat information

Incident details, TTPs, IOCs etc

OT-ISAC Operation Centre

OT-ISAC Community

(4) Intelligence disseminated to/received from the community

Incident details, TTPs, IOCs etc

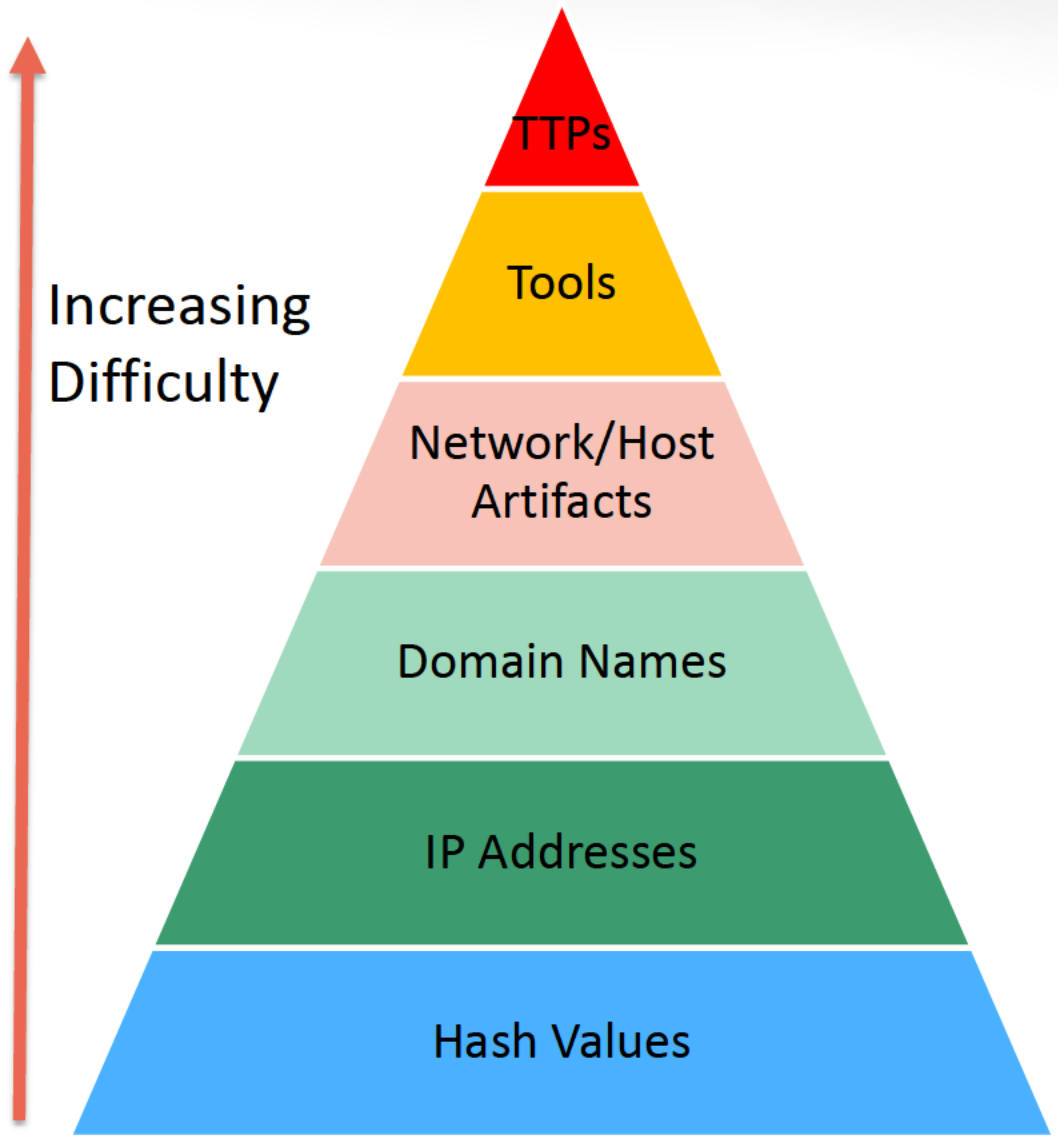
(3) Analyst may contact member to verify and gather more details

(2) Analyst redact, contextualise and anonymize details

GRF Cross Sectors

(5) If wider dissemination required, intelligence is sent to the GRF network. Feedback may be collected as input to the next intelligence cycle

Information Shared by Members in the ISAC



David Bianco "Pyramid of Pain"

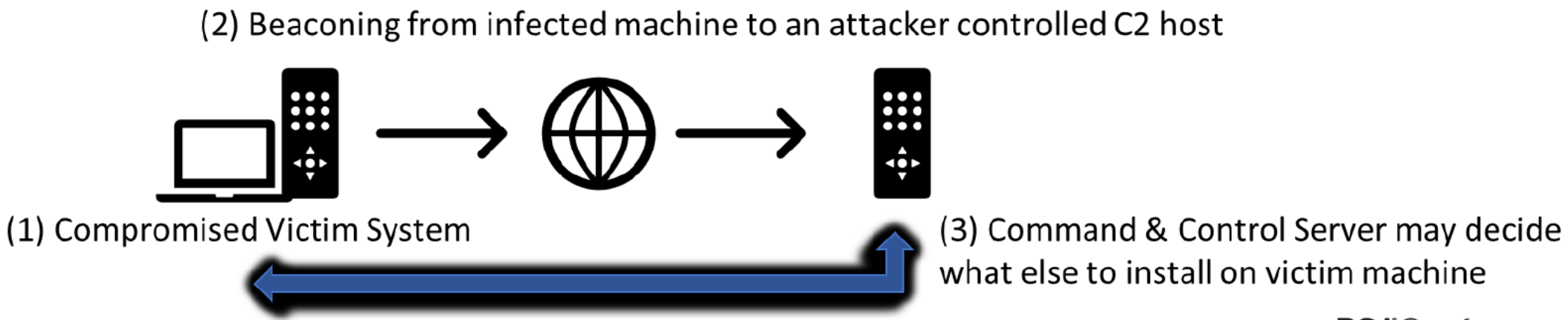
Members share:

- Cyber or Physical Threats or Incidents
- TTPs, Attack Vector, Context
- Indicators of Compromise (IOCs)
  - IP Addresses
  - Filenames
  - File Sizes
  - URLs
  - Domains
  - Hashes
  - Email Addresses
- Target/Impact Information
- Actions Taken
- Mitigation Strategies

Case: “Beacon Detection”

Case Facts

- A member reported an incident that happened in their infrastructure
- During a security assessment an internal server that was not authorized to external communication was discovered trying to do so
- Upon further analysis a compromised application was found on the server
- The application was trying to connect to an external machine over the internet



Case: “Beacon Detection”

MITRE TACTIC	TA0011	Command and Control
MITRE Technique	T1043	Commonly Used Port (80, 443)
	T1094	Use a common and control protocol
F3EAD		
FIND	Suspicious traffic detected browsing through fire wall log	“HTTP 403 error code” meaning forbidden access to requested resource
FIX	Remove offending application	The application was trying to send a beacon to a C2 server that it is “alive”
FINISH	Restriction on host on internet browsing	Otherwise the C2 server when contacted may try to install a payload
EXPLOIT	IOCs of the incident gathered.	Analyst anonymized the details
ANALYSE	Threat intel alert produced	TLP protocol followed
DISSEMINATE	Threat alert disseminated to the community.	Other members can take the precautions

Apply

Short Term (1-2 Weeks)

- Understand how the IT and OT security are managed in your organization (roles/functions/objectives)

Medium Term (1-2 Months)

- Recognize the critical assets, processes and systems of your organization (Asset Identification)

Longer Term (3-4 months)

- Conduct a security assessment and highlight 3 to 5 medium to high risks areas in your infra-structure to re-mediate

Summary

- We can minimize the impact to our organization if we **prioritize protection** of the most critical assets.
- **Sharing information and intelligence** will help us in our defense capability.

Global Resilience Federation

Global Resilience Federation (GRF) is a nonprofit corporation that develops and supports threat information sharing communities and coordinates cross-sector intelligence sharing among its members.

Global Resilience Federation

Thank you!

OT-ISAC

OPERATIONAL TECHNOLOGY INFORMATION SHARING AND ANALYSIS CENTER

Email: info@otisac.org