SANS ICS SUMMIT APAC

Protect Power Plant and Industrial Infrastructure from Cyber Attack!

How to mitigate the risk based on case study in Japan

Takashi Amano

General Manager, Cyber Security Center, **Toshiba Corporation**

Technology Executive and CISO, **Toshiba Digital Solutions Corporation**

TOSHIBA

Mitigating Risk

Earthquakes, typhoons, Flood, Tsunami etc.

Building resilience to natural disaster

Trend of recent cyber incidents in Japan

IT security

Increase **sophisticated cyberattacks**

target defense industry by nation state industrial espionage

Product security

Supply chain issues

vulnerabilities in generalized software embedded in products

Control systems security

Factory shut down, serious damage in the world.

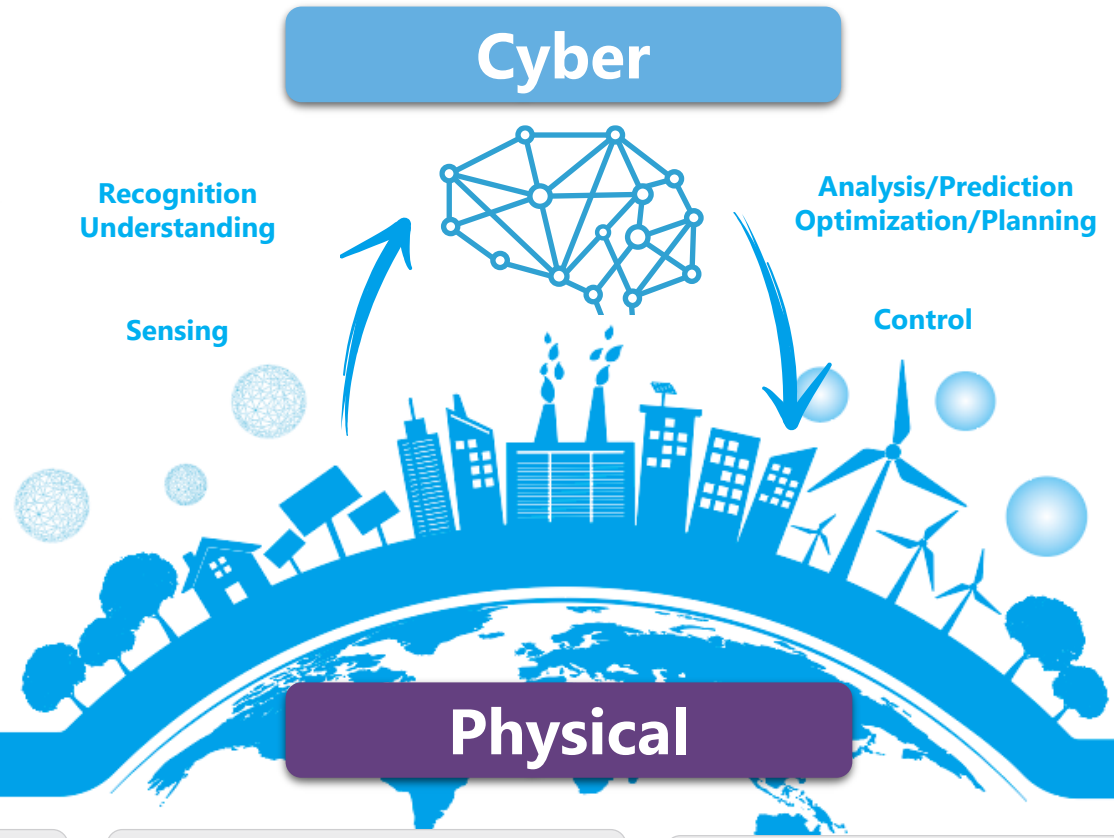
Targeted automobile plants and control systems

Creating new value by taking full advantage of CPS technology

Make full use of CPS technologies and Solve the problems facing society and our customers

Digital Technology

Product and System Technology



- AI・Data Analysis
- IoT Solution
- Cyber Security
- Edge Solution
- Edge Device
- Embedded Software Development
- Development Tool Solution

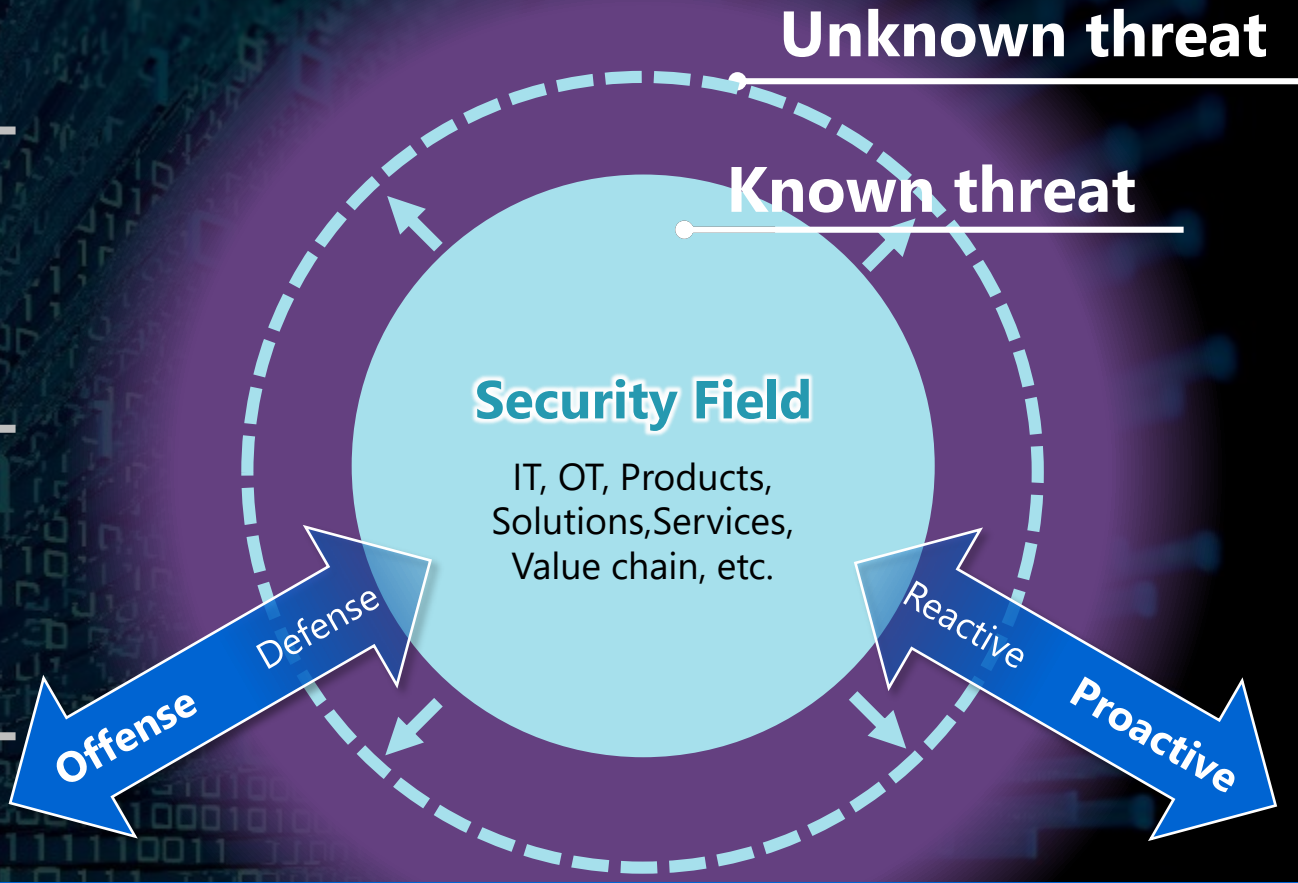
Social Infrastructure | Energy System | Manufacturing | Electronic Component

Digital Risk is increasing to CPS

1 Targets of Cyber attacks

2 Cyber threats intrusion

3 Methods of Cyber attacks



To respond to unknown threats,
we have to change from Defense to Offense, from Reactive to Proactive

What is Cyber Resilience?

Ability to Prepare, Mitigate impact, and Response & Recover

Japan Business + IT	Cyber resilience refers to the mechanisms and ability to **minimize the impact of a system's** cyber-attack and **restore it to its original state as soon as possible.**

Ref: https://www.sbbit.jp/article/cont1/35866

NIST SP800-160 Vol.2	"the ability **to anticipate, withstand, recover** from, and **adapt** to adverse conditions, stresses, attacks, or compromises on systems that use or are enabled by cyber resources."

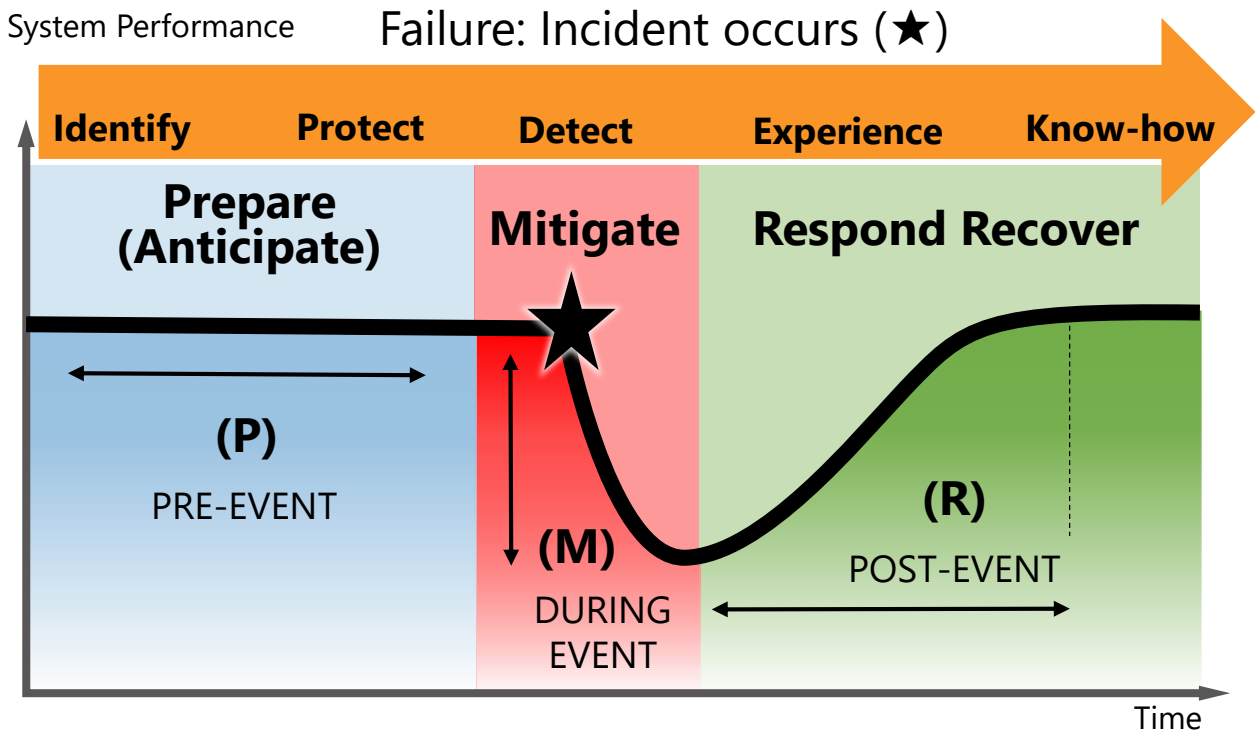
Ref：Developing Cyber Resilient Systems : A Systems Security Engineering Approach

UK IT Governance	Cyber resilience is the ability **to prepare for, respond to and recover from cyber attacks**.

Ref：https://www.itgovernance.co.uk/cyber-resilience

Identify key parameters of cyber resilience

Longer “P”, Minimize “M” and Shorter “R”



Parameters

P : Mean time between failures

M : Decrease in efficiency due to failure or incident

R : Mean time between Response & Recover

To minimize damage by incident

① Prepare

Longer system performance（Longer P）

② Mitigate

Minimize the impact of incidents (Minimize M)

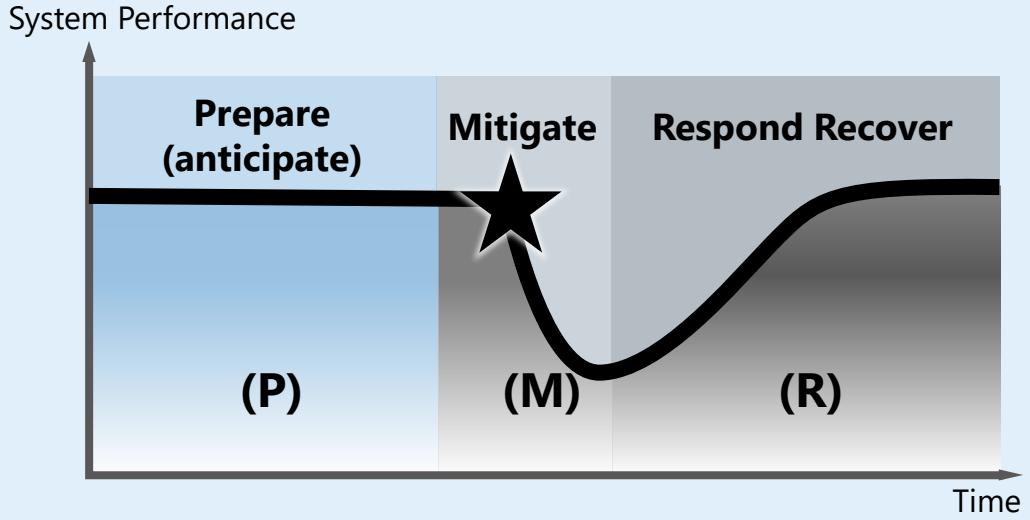
③ Respond & Recover

Shorter recovery time（Shorter R）

① Prepare->Longer system performance（Longer P）

Maintain system health（Cyber Hygiene）

- IT: Update OS/SW regularly and patch in a timely manner
- OT: Regular maintenance
- Security by design
- Visualize assets and continuous monitoring
- Collect the log for forensic analysis and store as knowledge



Strengthen deterrence and prevention measures

- Multi-layered protection at the system boundary between IT and OT
- OT: Unidirectional communication, Endpoint security to protect legacy devices
- System redundancy incase of the incident

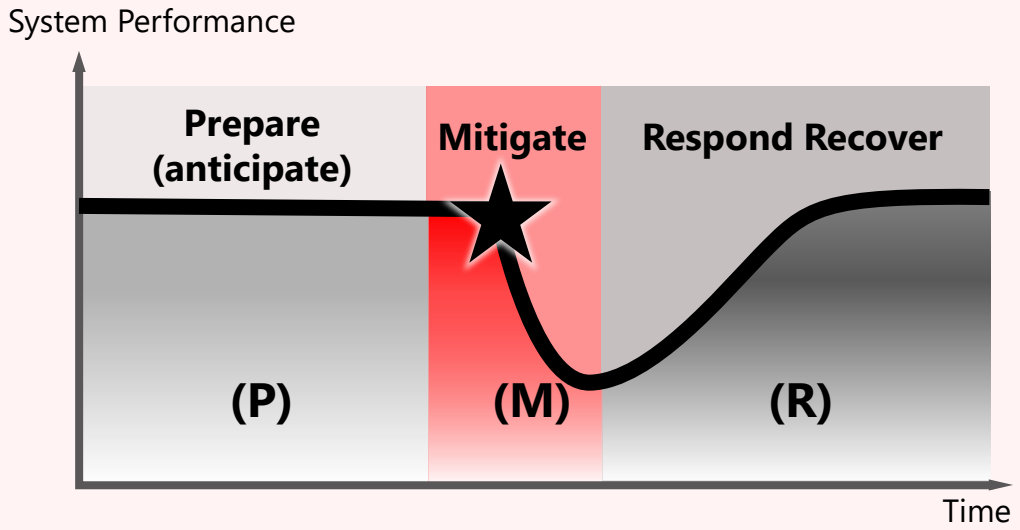
Use Threat intelligence, anticipate the risk

- Predict most likely paths of attack vector chains

② Mitigate->Minimize the impact of incidents（Minimize M）

Real-time detection of attacks

- Anomaly detection, Behavior detection
- Intrusion Detection System (IDS)
  → Detect OT unique protocol in passive way
- IT/OT continuous monitoring (SOC)
- Incidents and events correlation analysis (SIEM)
- Incident Visualization and Response Automation(SOAR)



Minimize impact and localization of damage by zoning

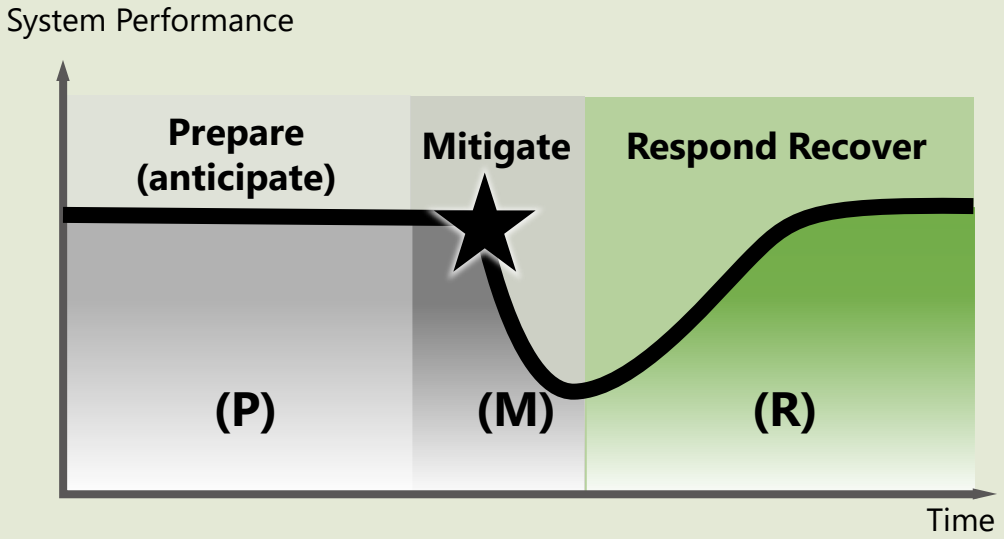
- Monitor conduit communications and detect anomalies
- Monitor the internal state of the zone and detect anomalies

③ Respond & Recover->Shorter recovery time（Shorter R）

IT: System shutdown, backup and recovery

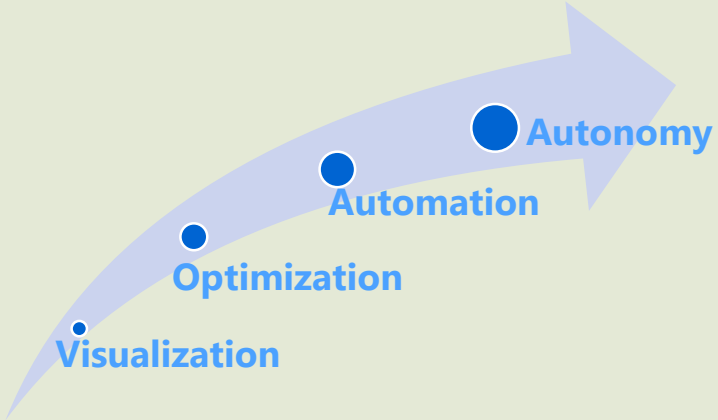
OT: Continue operating and recovering while compromised

- Zone by zone recovery（Multilayered）
- Switching between main and subsystems（Redundancy）
- Continuous monitoring while system maintenance and recovery



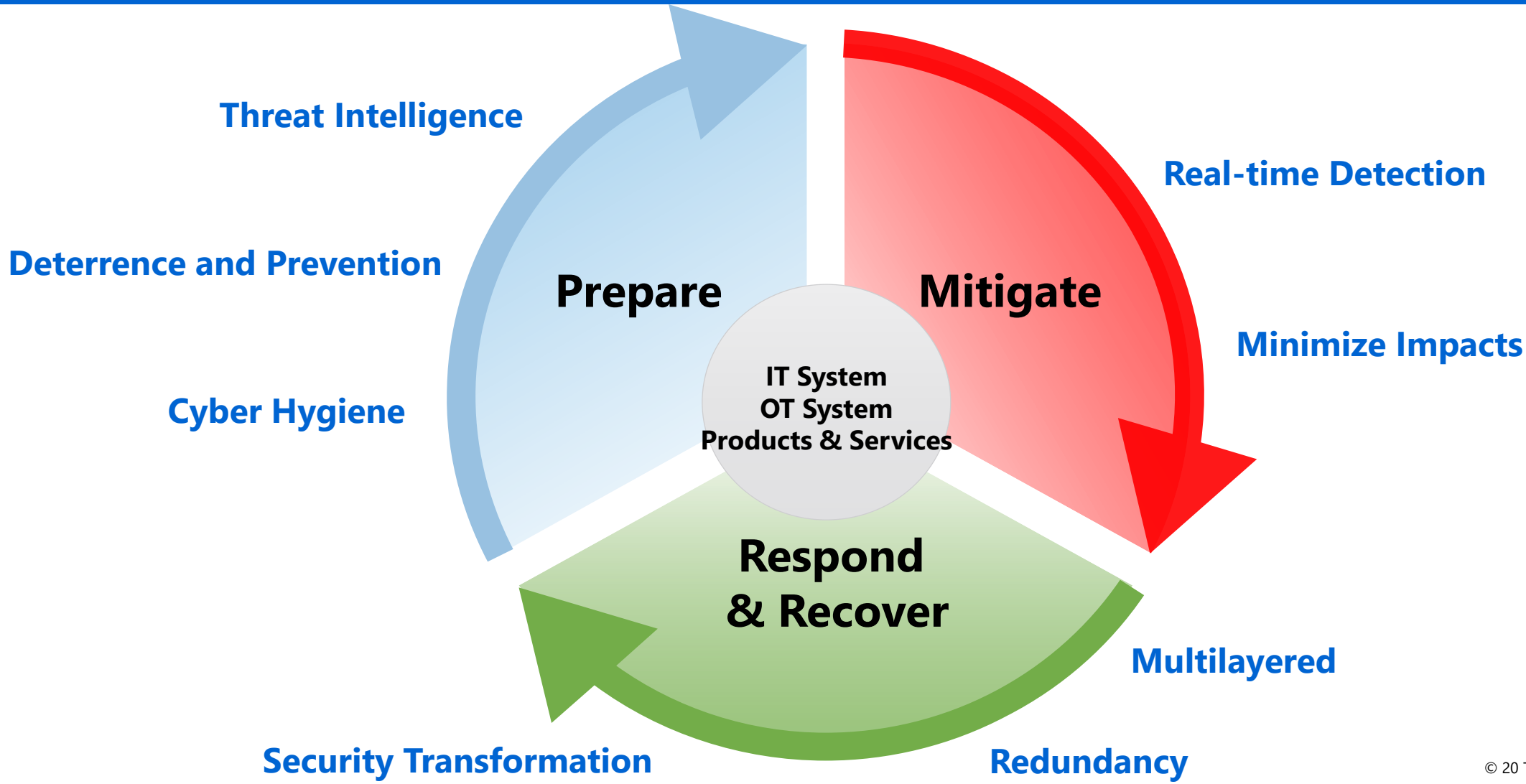
Support the person to make decisions by history log and experience

- Provide information（visualization）
- Recommend measures（Optimization）
- Partially Automate measures（Automation）



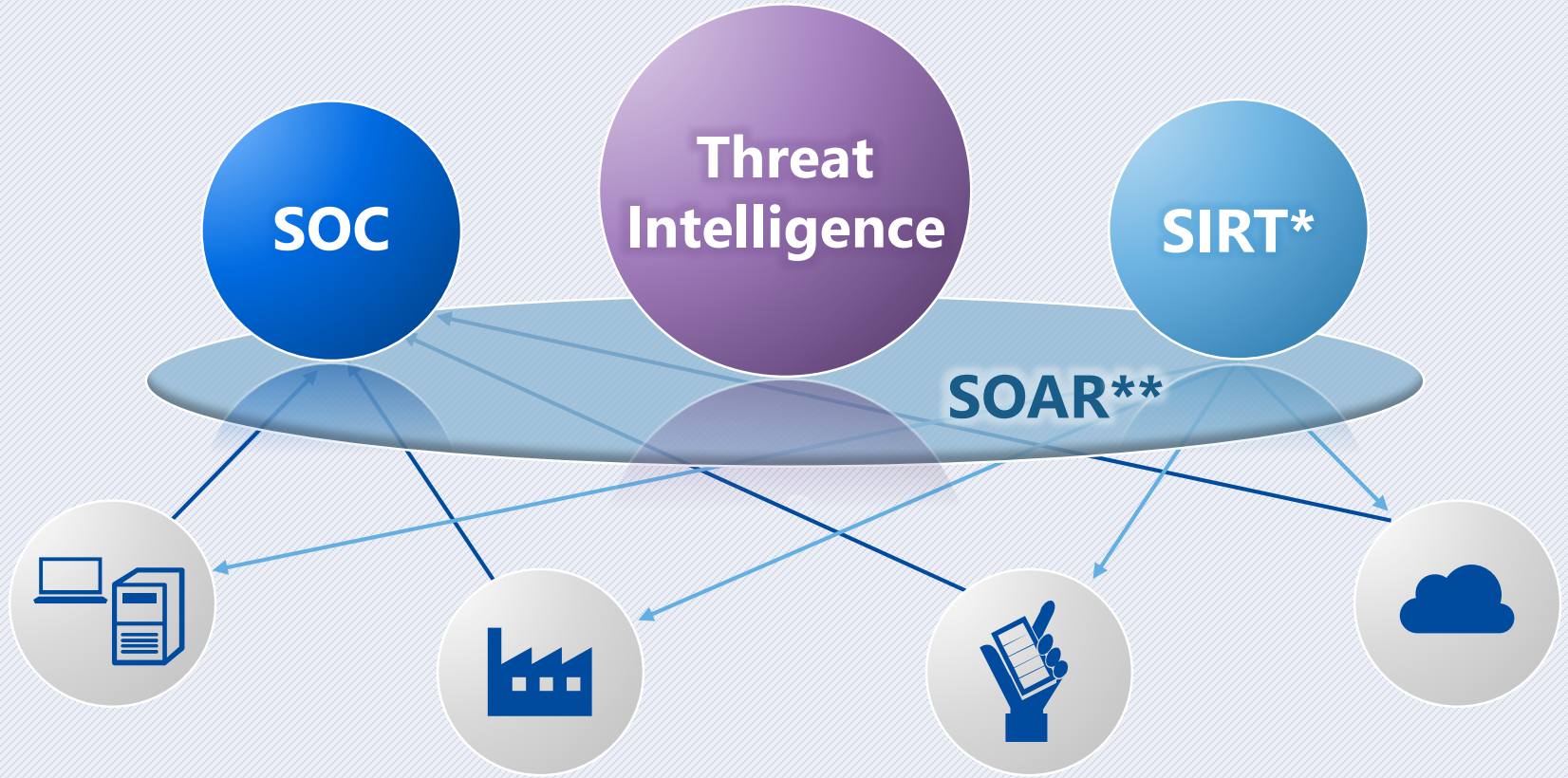
Cyber Resilience Lifecycle

Continuing the life cycle will strengthen cyber resilience



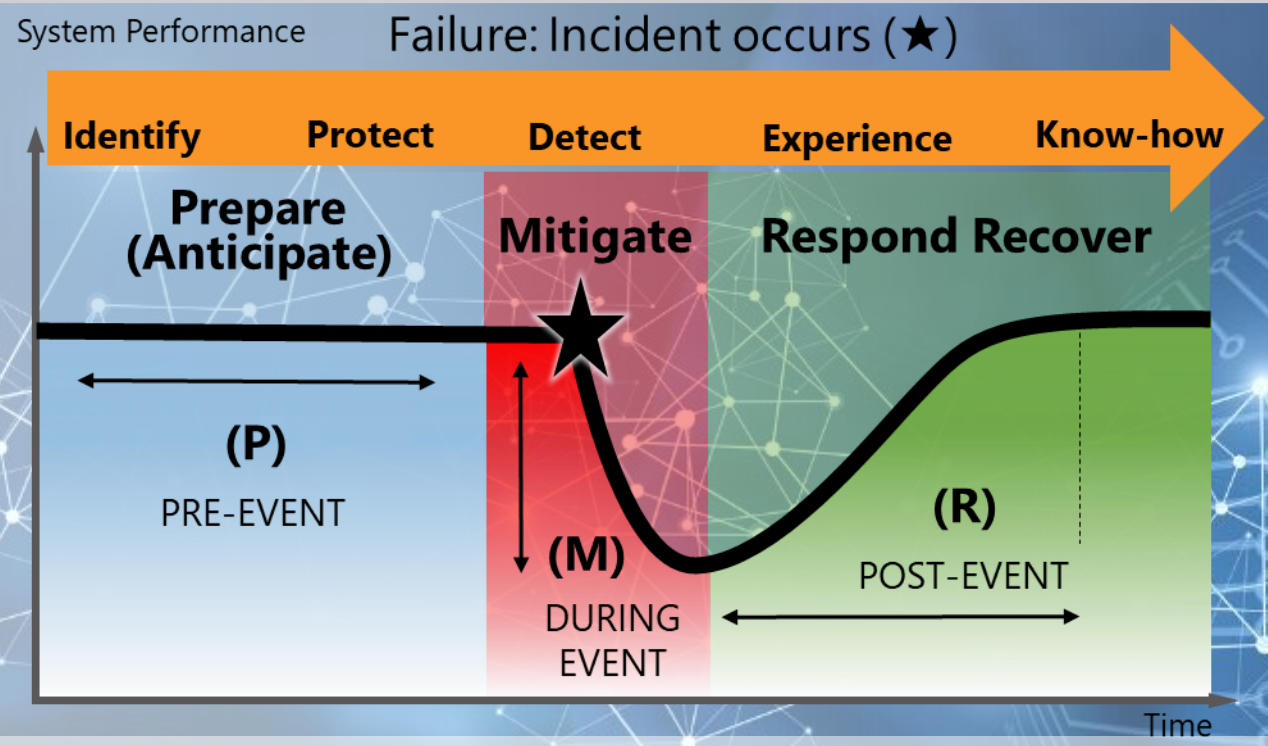
Cyber Resilience Operation Platform (CROP)

Logs from assets and threat intelligence are used as inputs to SOAR to automate operations with on-site experience and knowledge



*CSIRT：Computer Security Incident Response Team
*PSIRT：Product Security Incident Response Team
**SOAR：Security Orchestration, Automation and Response

Summary : Cyber Resilience at Power Plant and Industrial Infrastructure



- **Prepare** Longer system performance — Longer "P"
- **Mitigate** Minimize the impact of incidents — Minimize "M"
- **Response & Recover** Shorter response time — Shorter "R"

Committed to People,
Committed to the Future.

TOSHIBA