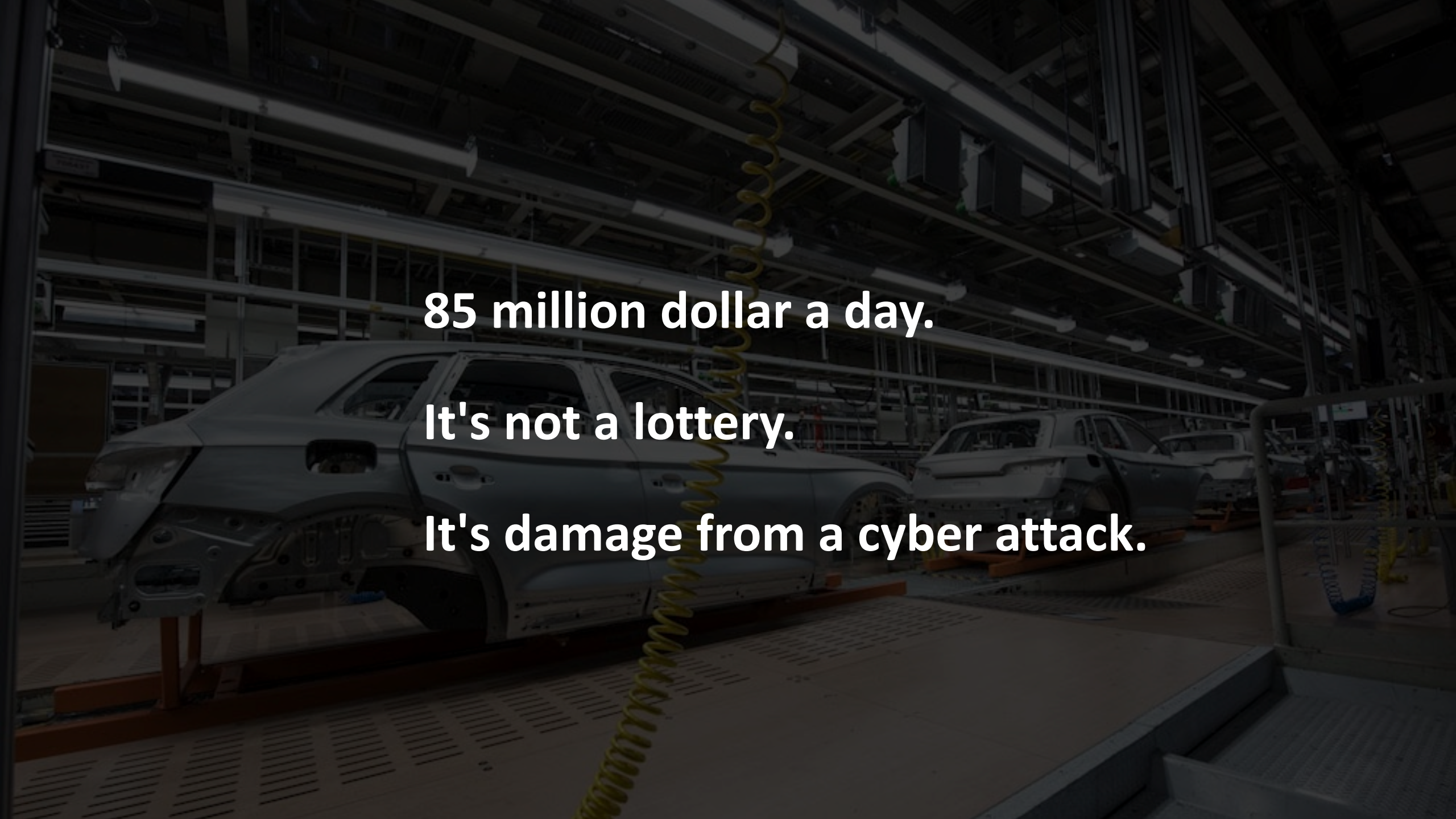




Introduction to Cyber Security Monitoring Service for OT System

Panasonic Cyber Security Team



85 million dollar a day.

It's not a lottery.

It's damage from a cyber attack.

Market Background

Market Background

Once an OT system is compromised by a cyberattack, its core functions can be severely disrupted—potentially halting production and causing significant damage to the business.



2018

Semiconductor company hit by ransomware

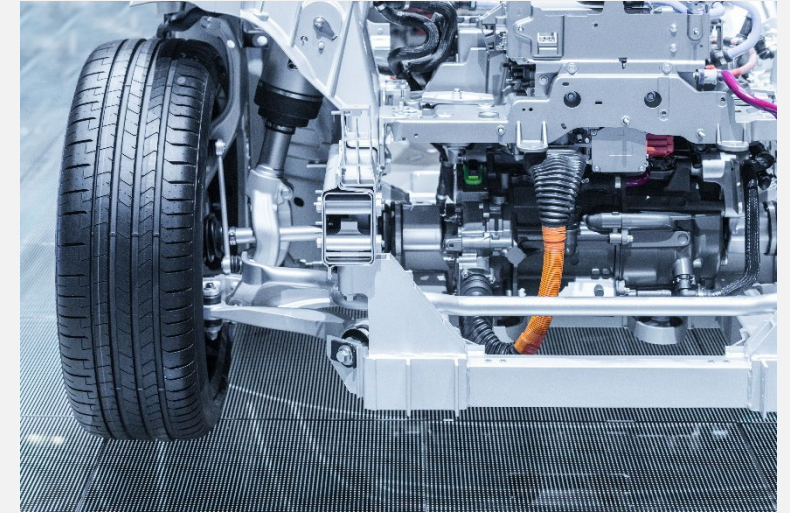
More than 10,000 PCs were infected with a variant of the ransomware "WannaCry", causing factory shutdown. The damage is said to be about \$256 million. The infection was caused by human error—new device was connected to the network without undergoing the required virus scan.



2020

Targeted Attack at automobile company

A targeted cyberattack brought global production to a standstill at a major automaker. As IT and OT become deeply integrated in manufacturing, this incident served as a wake-up call—cyber threats now have the power to shut down physical operations worldwide.

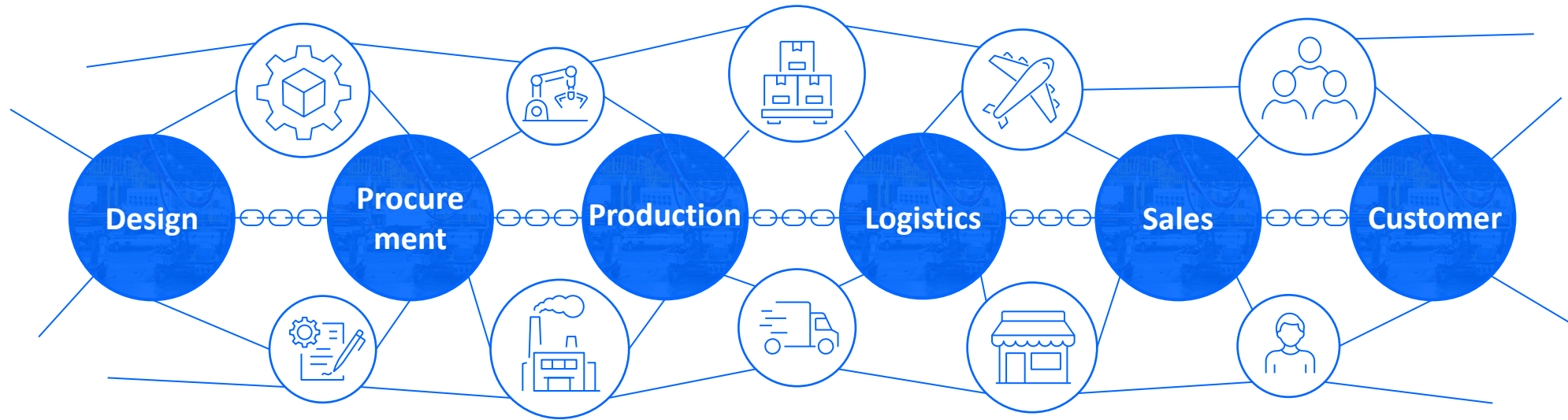


2022

Supply Chain Attack

A ransomware attack on a subsidiary parts supplier forced its parent company to halt operations at all domestic plants. This incident highlighted the vulnerability of supply chains to cyberattacks and sparked global awareness of the need for stronger cybersecurity.

In the coming era, securing the entire supply chain will be critical to ensuring operational stability and business resilience.



Today's supply chains are deeply interconnected, involving numerous companies and processes that depend on one another. This complexity increases the risk of cyberattacks, especially through suppliers and partners. Such attacks can have a widespread impact on business operations. To address this, it is essential to implement comprehensive security measures across the entire supply chain. Doing so not only reduces risk and ensures business continuity but also strengthens trust with customers and partners.

Among various international standards, security monitoring is required for Operational Technology.



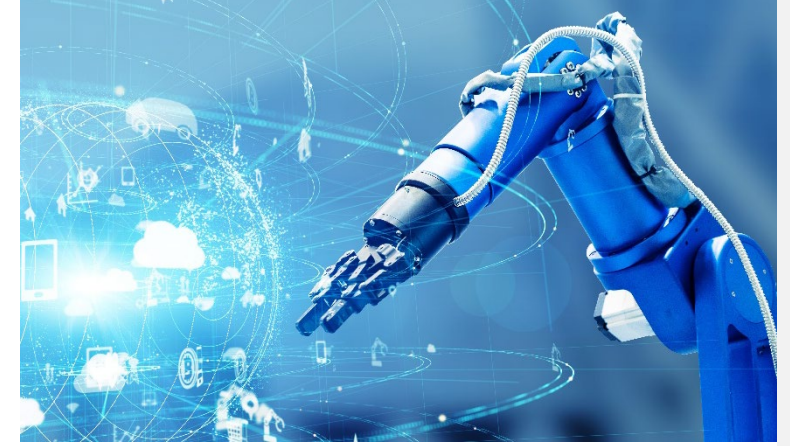
NIST SP800-82 Rev.3

NIST SP 800-82 Rev.3 provides cybersecurity guidance for Industrial Control Systems (ICS) and Operational Technology (OT). It emphasizes availability and safety, supporting risk management, defense-in-depth, network segmentation, continuous security monitoring, and anomaly detection.



NIST SP800-171

NIST SP 800-171 defines security requirements to protect Controlled Unclassified Information (CUI) in non-federal systems. It includes 14 control families and emphasizes not only prevention but also detection—such as logging and monitoring—to identify and respond to threats quickly.

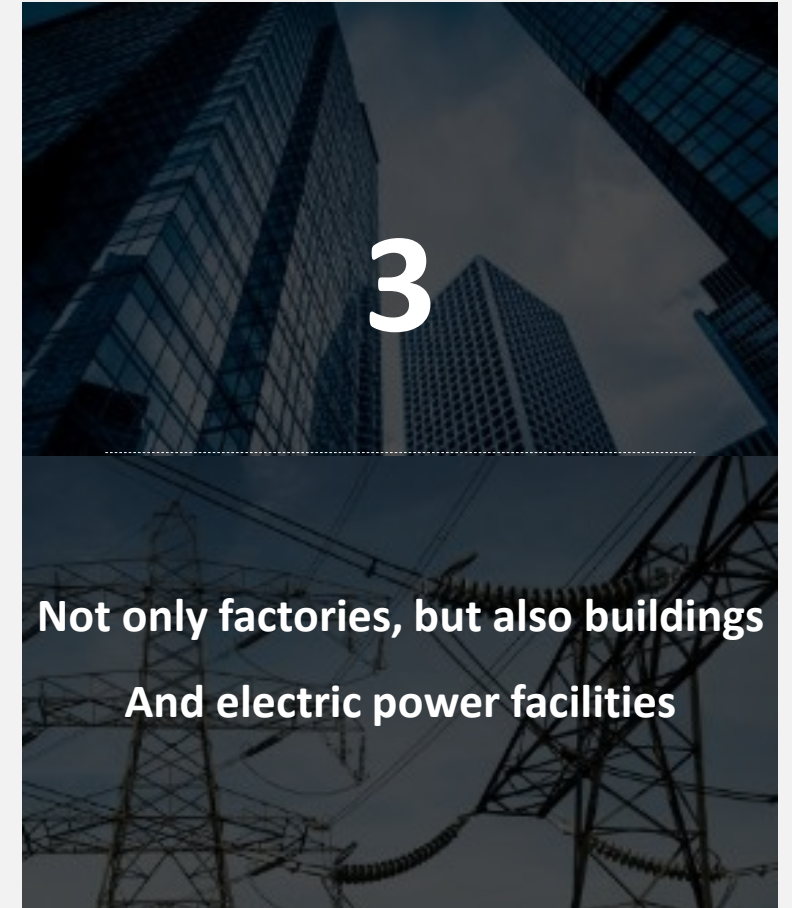
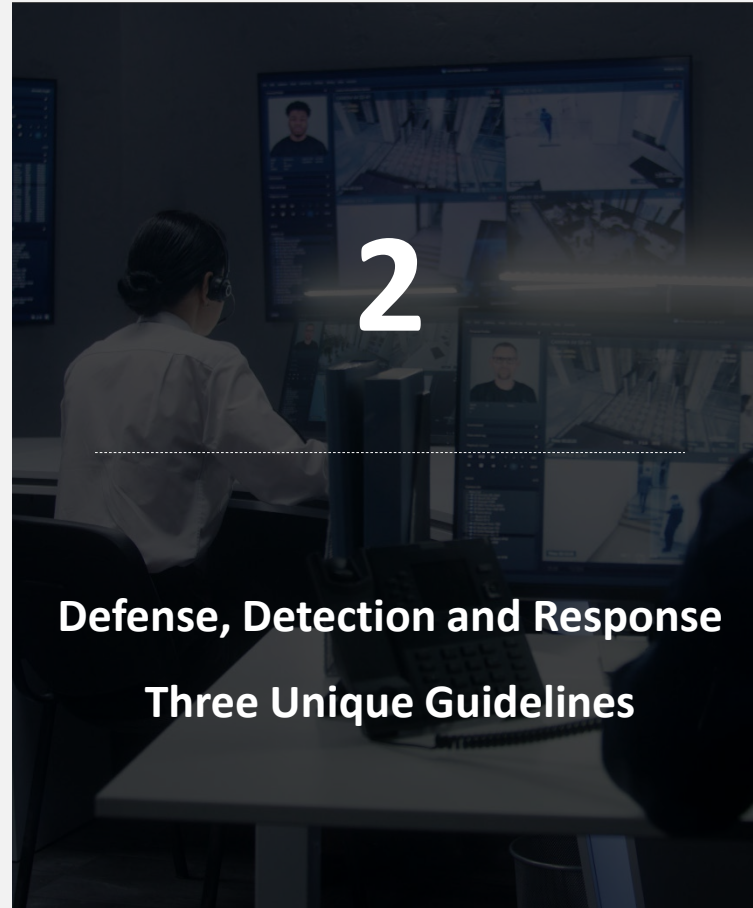
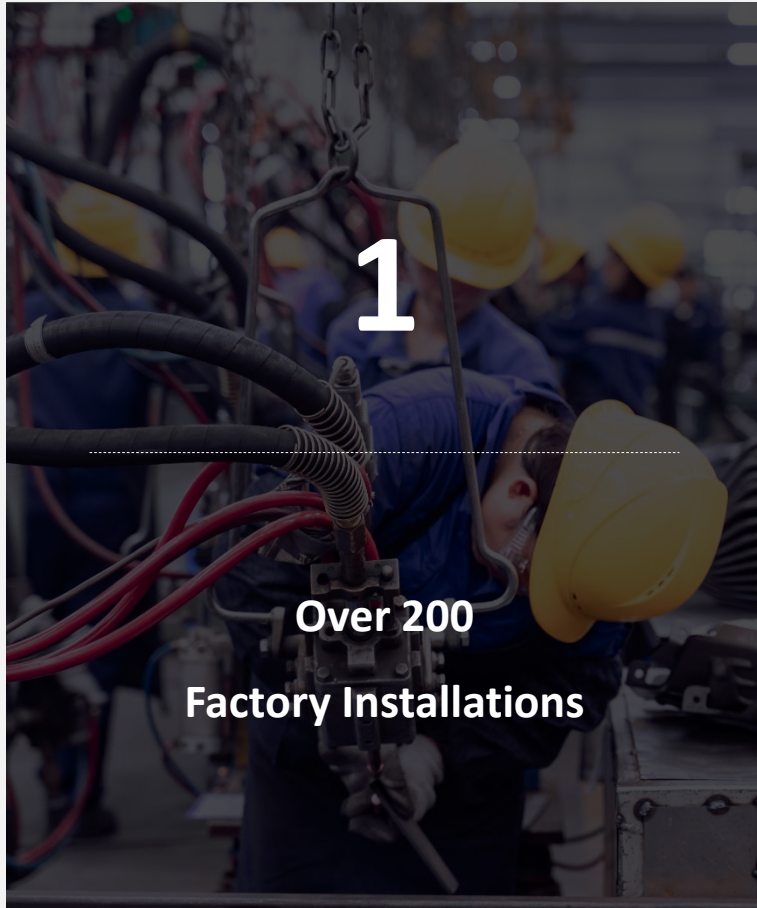


ISA/IEC62443

IEC 62443 is a global cybersecurity standard for industrial control systems. It defines a layered defense approach and mandates threat detection capabilities, such as network monitoring, to identify anomaly activities and enhance operational security and resilience.

Panasonic
Factory Security Initiatives

Three Initiatives Only Global Manufacturers Can Do



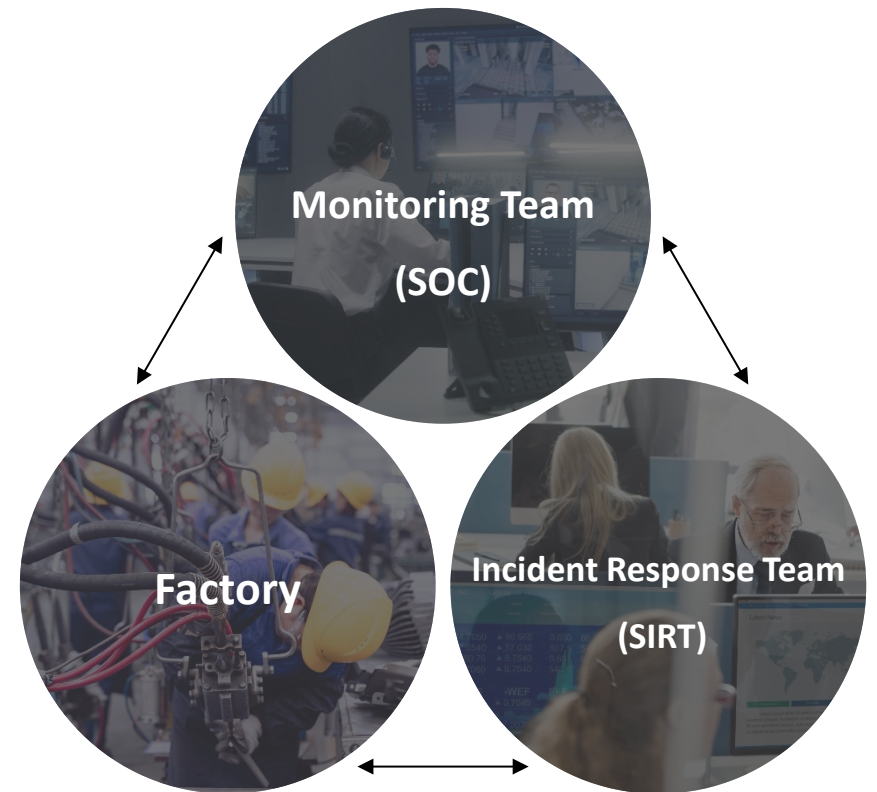
We conduct cybersecurity monitoring of over 200 diverse factories.

Panasonic operates approximately **300 manufacturing sites globally**. These factories produce a wide range of products—not only consumer electronics, but also chip resistors, housing materials, and more.

To date, we have implemented monitoring systems at over 200 of these sites, enabling tailored security monitoring based on the unique characteristics of each factory. Through this initiative, **we have accumulated valuable expertise in accurately identifying and managing the risks associated with diverse manufacturing operations.**

We have established a robust security framework through close collaboration between our factory teams, security monitoring teams, and incident response teams. This structure minimizes the impact on production activities in the event of an incident.

Building on these insights, we continue to enhance product safety and quality, enabling us to deliver products that earn the trust of our customers.



SOC: Security Operation Center

SIRT: Security Incident Response Team

Panasonic's Factory Security Initiatives

We have established three proprietary guidelines—Defense, Detection, and Response—to reinforce management and control. Through continuous improvement, we are constantly enhancing the security measures at our factories.



Protection

The Protection Guidelines Established in 2016

We enforce strict physical and network security measures, including security zoning, access control, equipment handling procedures, virus checks, firewalls, and network segmentation—ensuring robust protection against unauthorized access to our factories.



Detection

The Detection Guidelines Established in 2017

We mandate the implementation of detection systems that monitor network traffic, identify abnormal communications, and analyze threats, along with a dedicated security monitoring framework. This enables early detection of cyberattacks and minimizes potential damage to our factories.



Response

The Incident Response Guidelines Established in 2018

We have established clear protocols for communication, initial response, containment, investigation, recovery, and recurrence prevention in the event—or risk—of factory shutdowns or data breaches. These measures aim to minimize damage and prevent future incidents.

We are also expanding our service across various fields beyond factory



Panasonic's cybersecurity monitoring service is built on **cutting-edge technology and years of proven experience, protecting your manufacturing operations**. Leveraging expertise from our own factories, we are expanding into buildings, energy management system (EMS), and automotive fields—contributing to a safer society and a more prosperous future.

Cyber security for factories

Features of monitoring services

Panasonic provides end-to-end cybersecurity monitoring service —from risk assessment to incident response.



Risk assessment service

We identify critical assets and develop threat scenarios to visualize security risks in factories. Based on these insights, we propose countermeasures that prioritize factory availability.



Cyber security monitoring service

When an anomaly such as malware intrusion is detected, communication data is thoroughly analyzed to determine whether the affected device should be immediately isolated or if the impact would be minimal even without isolation. This approach helps minimize factory downtime. Panasonic offers a security monitoring service that prioritizes factory availability above all else.

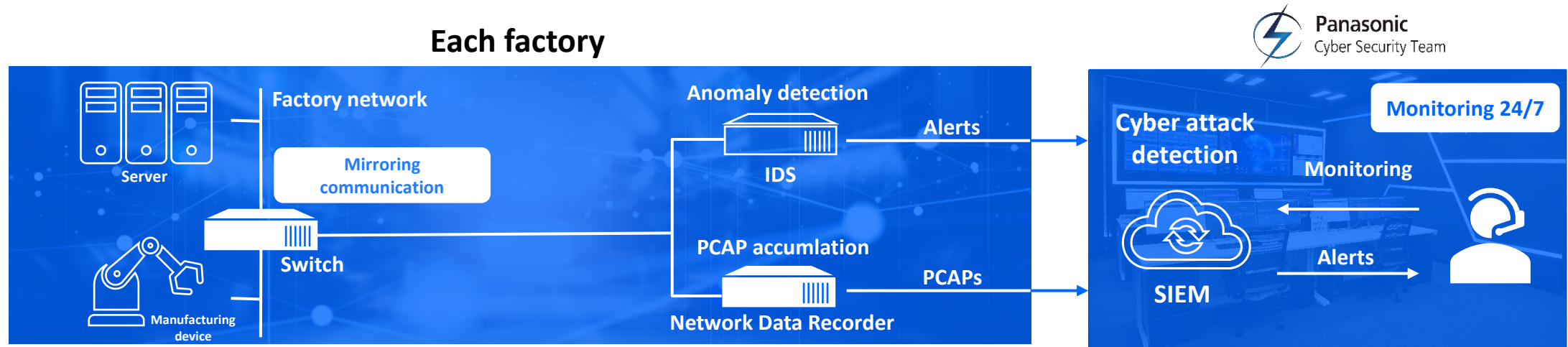


Incident response support service

We create use case scenarios and conduct training. In case of a real incident, we work closely with on-site teams for swift response—covering containment, investigation, recovery, and prevention.

Features of Cybersecurity Monitoring Service for Factories

Our security monitoring system enables early detection of anomalies and minimizes factory downtime.



Passive Monitoring That Doesn't Impact Factory Networks

Passive monitoring uses mirrored network traffic, ensuring no impact on the factory's existing network infrastructure.

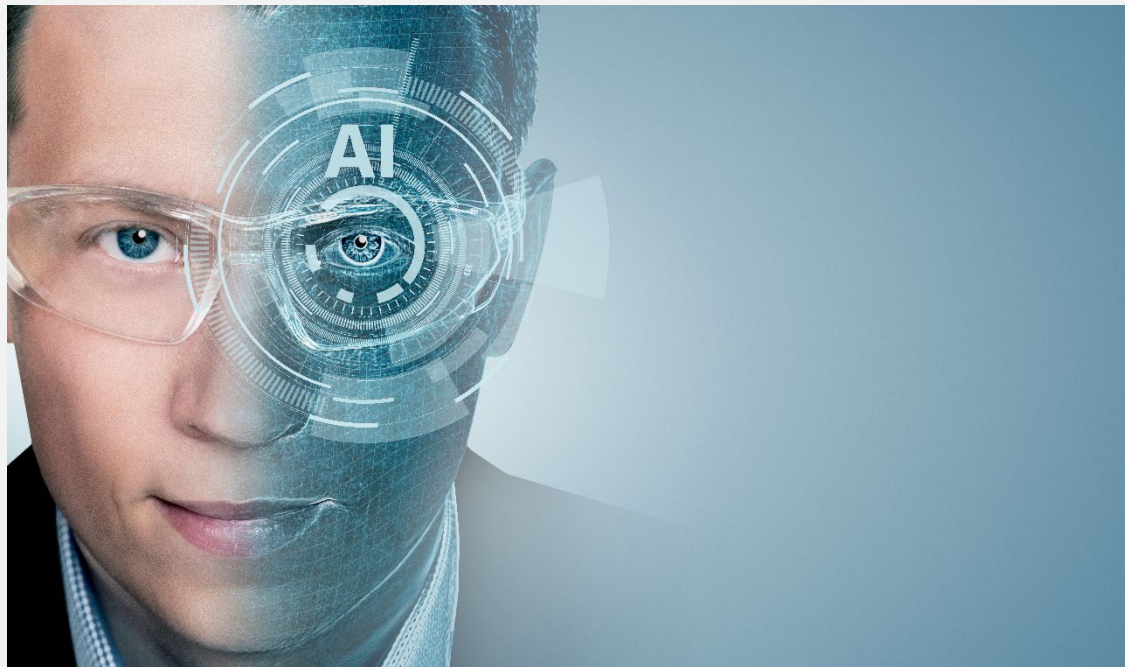
Anomaly Detection

IDS(Intrusion Detection System) functions as a sensor that issues alerts when it detects abnormal or suspicious activity within network traffic.

24/7 Security Monitoring System

We deliver 24/7 global security monitoring around the world. Our service enables early threat detection for industrial environments, helping protect factories from cyberattacks.

We focus on reporting only the alerts that truly matter to you.



Double check by attack detection engine and analyst

Automatically detected alerts often include a high number of false positives and over detections. Our team of certified security analysts—experts with extensive hands-on experience gained from monitoring over 100 of our own factories—carefully reviews and filters these alerts. By leveraging their deep expertise, they ensure that only the most critical and relevant alerts are reported, providing focused and effective monitoring for your factory.



Certified* and Experienced Analysts

*

Our monitoring sites

We have cybersecurity monitoring sites located in the United States, EU, Japan, China, and Southeast Asia. As a global manufacturing company, we are uniquely positioned to provide services to our customers' factories around the world.



Panasonic's Globally Recognized Cybersecurity Initiatives

Panasonic ranks **1st** In Japan* for cybersecurity patent applications

2,620 Patent applications related to cybersecurity

Panasonic holds the highest number of cybersecurity-related patents in Japan.

Panasonic Achieved the Highest Number of Cybersecurity-Related Patents in Japan.(2024) In the field of automotive security, Panasonic also demonstrates overwhelming patent strength across Japan, the United States, and Europe—holding 1,528 patents in Japan, 3,511 in the U.S., and 1,141 in Europe.

3.8 「防衛」、「検知」、「対策」でエンドポイントを守るトータルサイバーセキュリティ

【研究開発の目的】

【研究開発の内容】

Participation in Government R&D Projects and Publishing papers at Security Conferences

Panasonic has been selected for a government R&D project and is participating in an initiative led by the METI in Japan to enhance factory security. Panasonic is also actively involved in international conferences on cybersecurity.

World's Largest Cybersecurity Conference

OT Cybersecurity Conference

Automotive Cybersecurity Conference