OT Security | What Why How?

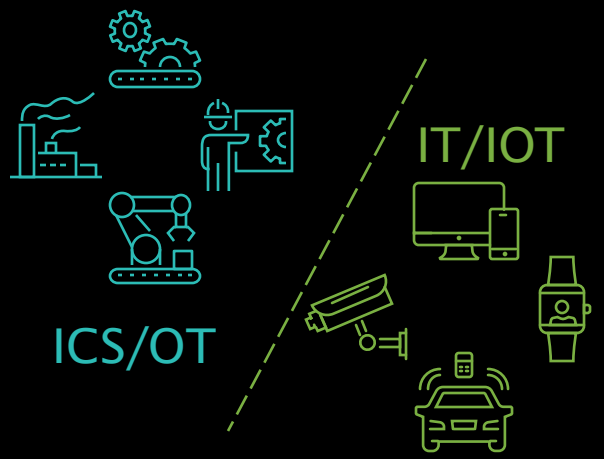
Serene Siow
Territory Manager | ASEAN

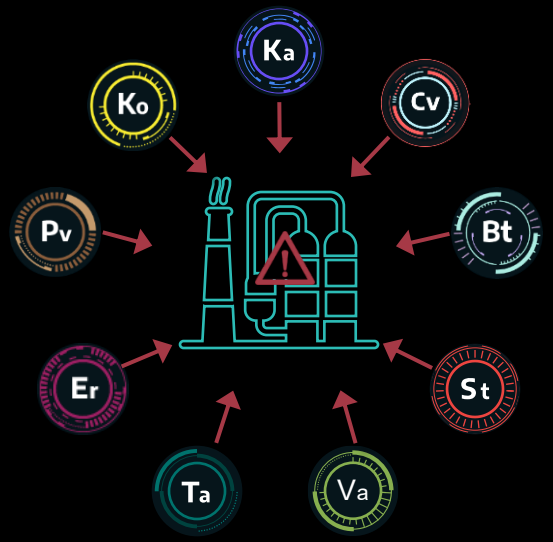
Hi, I'm Serene!

- 10 months in Dragos and 17 years in the cybersecurity scene
- From a generalist cybersecurity enthusiast to a mission focus member in OT security at Dragos, safeguarding civilization
- No technical engineer but I get to help customers think about
  - how to be an ENABLER to the business
  - consider tools to better assess risks in the organization
  - how to upskill the People, Process and Technology aspects

WHAT IT IS &
WHAT IT IS NOT

ICS/OT CYBER SECURITY ISSUES





ICS/OT Systems, Networks, & Vulnerabilities are Very Different from IT/IOT

Specialized Threat Groups Target ICS/OT Systems With TTPs Specific to the Environments

There Can Be Significant Impacts to Public Safety, Environment, & Revenue

ICS/OT SECURITY INVESTMENTS SIGNIFICANTLY LAG IT SECURITY

WHY IT MATTERS

CHEMICAL MANUFACTURING: Cybersecurity Challenges

Systems and Facilities

- Proprietary embedded systems and outdated technologies
- Lack of OT asset inventories and network visibility

Regulatory Environment

- Complex environmental, safety, and security regulations
- Current regulatory framework may not be applicable or out of date

Organizational Alignment

- OT skills gap and workforce shortages, expert attrition
- IT cybersecurity strategies do not address OT environments

POTENTIAL IMPACTS

- Potential for injury, loss of life, and environmental damage
- Community impact due to evacuate or shelter-in-place orders

- Operational disruption and downtime resulting in lost revenue
- Loss of intellectual property and competitive advantage

HOW TO START
What to look for?

Effective OT Security

5

SANS

THE FIVE ICS CYBERSECURITY CRITICAL CONTROLS

01
ICS Incident Response Plan

02
Defensible Architecture

03
ICS Network Visibility & Monitoring

04
Secure Remote Access

05
Risk-based Vulnerability Management

01 ICS INCIDENT RESPONSE PLAN

OT's incident and response plan is distinct from IT's.

Different

Device types	Communication protocols
Tactics	Techniques and procedures

Managing the potential impact of an incident is different for OT's. Create a dedicated plan as well as thought-out next steps for specific scenarios

More importantly, test the plan!

02 A DEFENSIBLE ARCHITECTURE

The resources and technical skills required to adapt to new vulnerabilities and threats should not be underestimated.

Network segmentation & traffic filtering (zones & conduits)

Removing extraneous OT network access points & managing access

Maintaining strong policy control at IT/OT interface points

Defenders & Responders - The people and processes to manage it

03 ICS Network Visibility & Monitoring

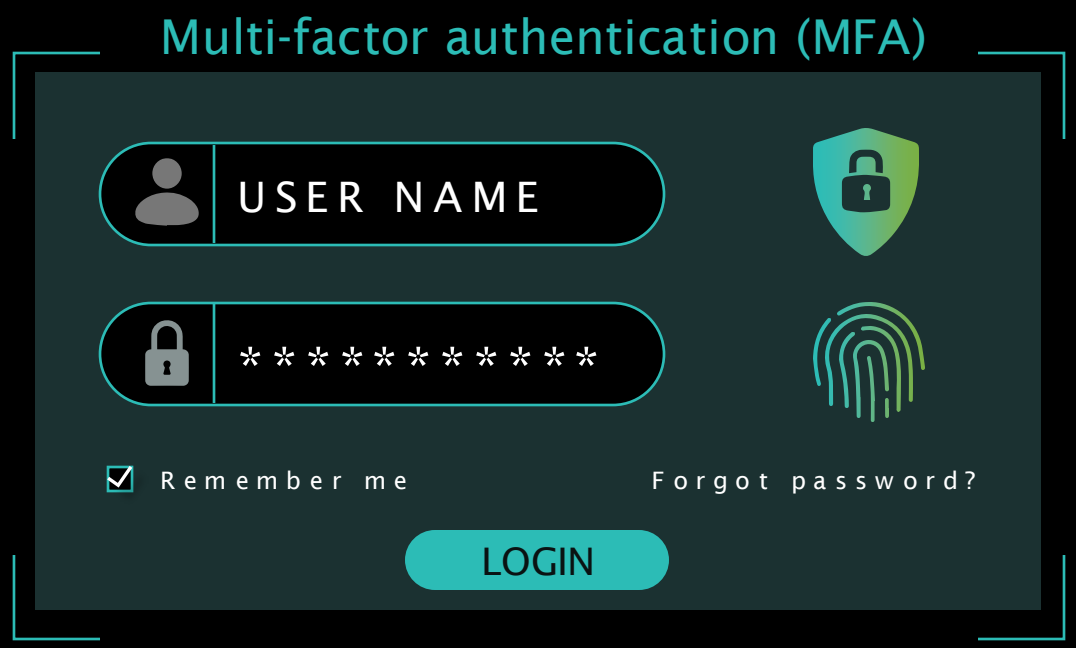
You can't protect
what you can't see.

IN 2022
80%
of Dragos services customers had limited to no visibility in their OT environments

A Successful OT Security Posture

- Maintains an inventory of assets
- Maps vulnerabilities against those assets
- Actively monitors traffic for potential threats
- validating the security controls implemented in a defensible architecture

04 SECURE REMOTE ACCESS

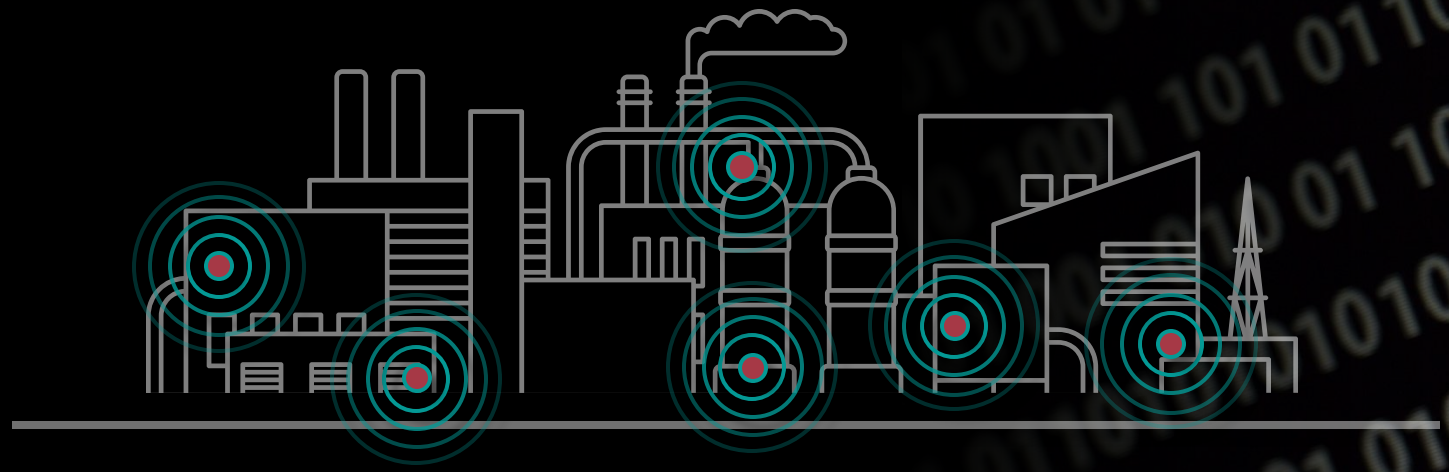


Implement MFA across your systems of systems to add an **extra layer of security** for a relatively small investment.

Add key policies to limit access; use jump hosts between OT and IT; separate OT and IT access credentials

Monitor ICS Networks to identify external remote access sessions & validate security controls

05 Risk-Based Vulnerability Management



Knowing your vulnerabilities
and having a plan to manage them is a critical component to a defensible architecture.

Check Alternative Mitigation & Accurate CVSS info
CNA's often mischaracterize OT risk and fail to provide risk management outside of patching

Working Together

Bring In The Best Of The OT & IT Side

- Form a cross functional team
- Bring in people from IT and OT backgrounds
- Leverage operations and process/electrical/control engineers - they are MVPs for understanding what's important and what needs to be secured
- OT Security is a journey, not a project