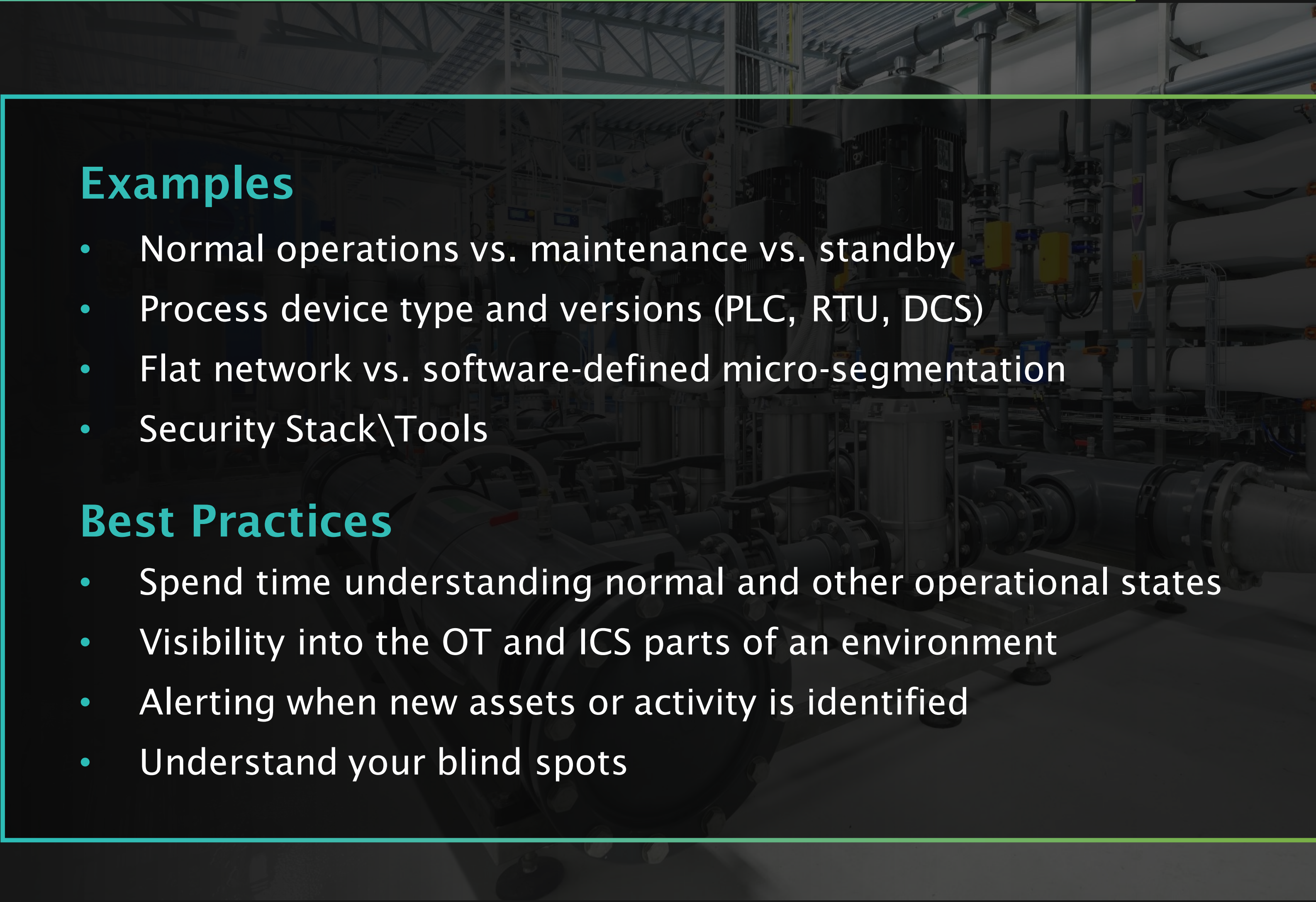
DRAGOS

10 Ways Asset Visibility Builds an Effective OT Cybersecurity Foundation

1 Understanding what “normal” looks like

NO TWO ENTITIES HAVE THE **SAME NORMAL**



Examples

- Normal operations vs. maintenance vs. standby
- Process device type and versions (PLC, RTU, DCS)
- Flat network vs. software-defined micro-segmentation
- Security Stack\Tools

Best Practices

- Spend time understanding normal and other operational states
- Visibility into the OT and ICS parts of an environment
- Alerting when new assets or activity is identified
- Understand your blind spots

2 Not just identifying, but verifying assets

TRUST BUT VERIFY

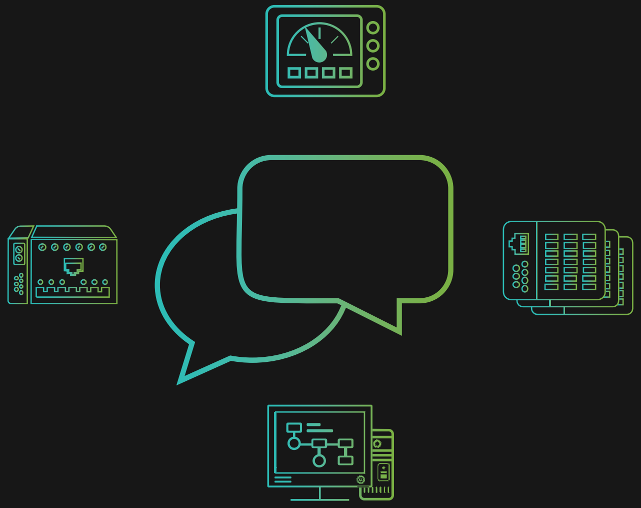
Examples

- Adding the needed context around the identified assets
- Validate that what I am seeing is supposed to be there
- Support security and operations goals

Best Practices

- Use information and sources you already have
- Validate installed software to known approved configurations
- Physical and logical verification when needed

3 Visualizing asset network communications



DEVICES **WILL TALK TO ANYONE**, THOSE SOCIAL BUTTERFLIES

Examples

- ARP and DNS requests
- ICS protocols
- Network zones and trust levels are not always well defined
- Vendors and operators will do what they need to get it working

Best Practices

- Confirm what is supposed to be communicating and how
- Ensure traffic visibility into ICS/OT North-South and East-West
- Conduct periodic reviews of the security devices that segment the environments
- Take a baseline of communications for future comparison

4 Improving change management with config detection

TRUST WHAT YOU'VE VERIFIED

Examples

- Configuration management is more common in IT-type systems
- Configuration detection can detect changes in real-time to ICS
- Automation can assist in maintaining supporting change management and compliance

Best Practices

- No news is *not* good news. Ensure tools are working or that the change took place.
- Look for outlining changes that don't fit.
- Leverage your solutions that provide configuration change tracking as part of your change processes and compliance

5 Minimizing the impact of compliance reporting

CONFIRMING THE HUMAN FACTOR

Examples

- Tools can handle year’s worth of asset information, including configurations for audit
- Daily reporting and alerting from A/V, SIEM, and asset configuration can identify issues such as services not running or out-of-date software
- Visibility tools can support other tools and gain visibility for compliance assurance where manual work would normally be required.

Best Practices

- Start with the output in mind and build or purchase a solution that fits
- Automate as much of the process as is possible
- Automation will have issues, so layer if its critical
- Periodic manual confirmation that tools are operating as required

6 Justifying security program investments

80% PAPERWORK, 20% TECHNICAL WORK

Examples

- The highest rate of security return on investment and effort
- Finding gaps in a program
- Compliance
  - 100 assets x (daily software validation + A/V check and update + Event Viewer reviews + Firewall review + IDS/IPS review) = Several employees
  - **Or** 1 report for software validation + 1 report for A/V status + Automated SIEM logging/alerting report + SIEM Firewall Report + IDS/IPS Report = 2-3 hours.

Best Practices

- Use visibility to determine the low-hanging fruit to improve security
- Use what you already have to enhance security
- Compare times between human verification and technology. Compare times for audit report retrievals as well as compile reports monthly. There's more than just running scans in an effective visibility program.
- Consider the stress and boredom of continuous report running and archiving, especially in a regulated entity.
- Automate the tasks that take the most time and that have the least value. Using the gained free time to execute higher value activities such as threat hunts.

7 Effective vulnerability mitigation

Examples

- Tools such as Microsoft WSUS\SCCM can tell you patches needed within 24hr of release
- Asset baselining tools can compare currently installed software to a list of known CVEs
- On-demand and scheduled scans can confirm patching removed vulnerable software
- Visibility tools can provide you with a list of vulnerabilities

Best Practices

- Understand the vulnerabilities in your environment
- Prior to patching, understand why you are patching
- Vulnerability management is not just patching but mitigations
- After a patching cycle, look for assets that might have been missed or failed to install software

COMBINING SUPERPOWERS

8 Threat detection in an ocean of noise

RIDE THE WAVES

Examples

- Native functionality of systems and devices
- Automated tools and collections solution
- Centralized SIEMs and storage locations
- Regular updates will provide new IoCs, vulnerability indicators, and other threat definitions/hashes for automated detections

Best Practices

- Alert fatigue is real. Make sure they add value
- Know the environment’s schedule (pigging, weather, installs)
- Focus on high-value alerts
- Trust but verify your tools
- Perform investigations based on the alerts or drive alerts based on investigations

9 Stopping rogue assets in their tracks

DEFCON 1

Examples

- Visibility baselines will show new devices which may be rogue
- Asset inventories can be used to validate visibility
- Integration into SIEM or other alerting solutions

Best Practices

- Develop a network baseline and asset inventory
- Proper switch port identification and configuration
- SIEM alerting and network visibility will help in the identification and investigations

10 Incident response when the heat is on

USING HISTORY TO SOLVE THE PROBLEM

Examples

- IR relies on knowing what should be there and what is normal
- Visibility can be used for tracking threats in the environment
- Increases the speed of IR steps

Best Practices

- IR requirements should be an input to what you collect for asset information and where you have visibility
- Practice using the solutions you have in your IR exercises

To find out more …

1 Grab a copy of *this whitepaper*

DRAGOS WHITEPAPER

HOW TO GET STARTED

Before starting, make sure a plan is established through a structured approach like Dragos's Col lay the foundation for a successful outcome that Visibility program.

Typically the planning and implementation stage Framework will be a continuous process that loo

Remove unneeded requirements, update changes, disseminate/ communicate
Update Collection Plan
Measure and understand
Test

As organizations go through the journey of esta potential stages of the maturation process.

DRAGOS, INC.

DRAGOS

Whitepaper

10 WAYS ASSET VISIBILITY BUILDS THE FOUNDATION FOR OT CYBERSECURITY

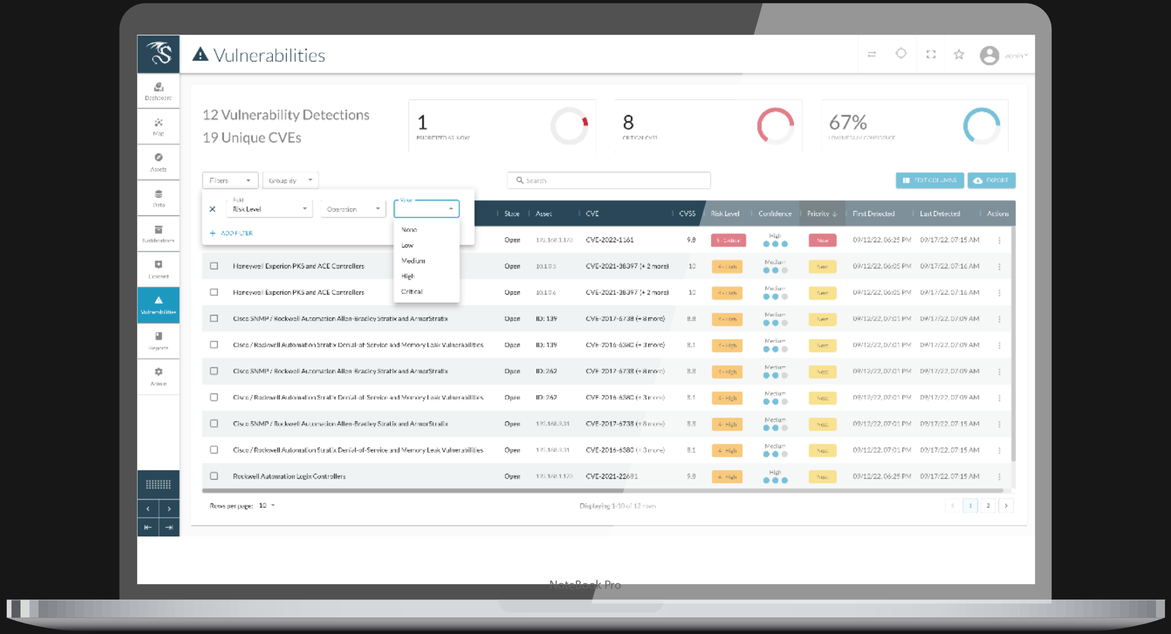
KNOWING THE DATA YOU NEED TO COLLECT ISN'T ENOUGH IF YOU DON'T HAVE FULL ASSET VISIBILITY

August 2022

info@dragos.com
@DragosInc

and

2 Learn how the Dragos Platform can improve your Asset Visibility



Vulnerabilities

12 Vulnerability Detections
19 Unique CVEs

1 PRIORITIZED AS NOW

8 CRITICAL CVSS

67% LOW/MEDIUM CONFIDENCE

Filters ▾ Group By ▾ Search EDIT COLUMNS EXPORT

Field: Risk Level ▾ Operation ▾ Value ▴
+ ADD FILTER

Value: None, Low, Medium, High, Critical

		State	Asset	CVE	CVSS	Risk Level	Confidence	Priority ↓	First Detected	Last Detected	Actions
		Open	192.168.1.173	CVE-2022-1161	9.8	5 - Critical	High ●●●	Now	09/12/22, 06:25 PM	09/17/22, 07:15 AM	⋮
□	Honeywell Experion PKS and ACE Controllers	Open	10.1.0.5	CVE-2021-38397 (+ 2 more)	10	4 - High	Medium ●●○	Next	09/12/22, 06:05 PM	09/17/22, 07:16 AM	⋮
□	Honeywell Experion PKS and ACE Controllers	Open	10.1.0.6	CVE-2021-38397 (+ 2 more)	10	4 - High	Medium ●●○	Next	09/12/22, 06:05 PM	09/17/22, 07:16 AM	⋮
□	Cisco SNMP / Rockwell Automation Allen-Bradley Stratix and ArmorStratix	Open	ID: 139	CVE-2017-6738 (+ 8 more)	8.8	4 - High	Medium ●●○	Next	09/12/22, 07:01 PM	09/17/22, 07:09 AM	⋮
□	Cisco / Rockwell Automation Stratix Denial-of-Service and Memory Leak Vulnerabilities	Open	ID: 139	CVE-2016-6380 (+ 3 more)	8.1	4 - High	Medium ●●○	Next	09/12/22, 07:01 PM	09/17/22, 07:09 AM	⋮
□	Cisco SNMP / Rockwell Automation Allen-Bradley Stratix and ArmorStratix	Open	ID: 262	CVE-2017-6738 (+ 8 more)	8.8	4 - High	Medium ●●○	Next	09/12/22, 07:01 PM	09/17/22, 07:09 AM	⋮
□	Cisco / Rockwell Automation Stratix Denial-of-Service and Memory Leak Vulnerabilities	Open	ID: 262	CVE-2016-6380 (+ 3 more)	8.1	4 - High	Medium ●●○	Next	09/12/22, 07:01 PM	09/17/22, 07:09 AM	⋮
□	Cisco SNMP / Rockwell Automation Allen-Bradley Stratix and ArmorStratix	Open	192.168.2.31	CVE-2017-6738 (+ 8 more)	8.8	4 - High	Medium ●●○	Next	09/12/22, 07:01 PM	09/17/22, 07:15 AM	⋮
□	Cisco / Rockwell Automation Stratix Denial-of-Service and Memory Leak Vulnerabilities	Open	192.168.2.31	CVE-2016-6380 (+ 3 more)	8.1	4 - High	Medium ●●○	Next	09/12/22, 07:01 PM	09/17/22, 07:15 AM	⋮
□	Rockwell Automation Logix Controllers	Open	192.168.1.173	CVE-2021-22681	9.8	4 - High	High ●●●	Next	09/12/22, 06:25 PM	09/17/22, 07:15 AM	⋮

Rows per page: 10 ▾ Displaying 1-10 of 12 rows ‹ 1 2 ›

dragos.com/platform/

THANK YOU

DRAGOS