



# Protecting Your OT Environment with Dragos

[Dragos.com](https://www.dragos.com)

# AGENDA

- Market Trends
- Customer Panel
- Dragos Platform



# ENABLING SECURE DIGITAL TRANSFORMATION

WORLD  
ECONOMIC  
FORUM

“Industrial companies must balance investment in **digitizing operations** with **greater exposure to malicious cyberthreats.**” May 2021





# OT VULNERABILITY TRENDS

First 6 Months of 2021 Compared to FY 2020

- Vulnerabilities and advisories released at ~2X the rate of 2020
  - Vulnerabilities: 793 in first half '21 v 703 CY '20
  - Advisories: 230 in first half '21 v 253 CY '20
- Advisories with errors are lower so far in '21
  - 35% in first half '21 v 43% CY '20
- Advisories with or without a patch lack mitigation advice
  - 85% in first half '21 v 64% in CY '20

[www.dragos.com/year-in-review/](http://www.dragos.com/year-in-review/)

# Customer Panel

# Customer Panel

- **James Sumpter**
  - VP of IT Operations and Security, Boardwalk Pipelines
- **Shon Gerber**
  - CISO, INVISTA, a subsidiary of Koch Industries
- **Michael Ball**
  - VP and CSO, Berkshire Hathaway Energy



# THE DRAGOS DIFFERENCE – OUR PEOPLE



## DRAGOS PLATFORM



ASSET  
VISIBILITY  
& INVENTORY



THREAT  
DETECTION



INVESTIGATION  
& RESPONSE



VULNERABILITY  
MANAGEMENT

# Dragos Experts (video)





# Dragos Platform Release Updates

# THE DRAGOS PLATFORM

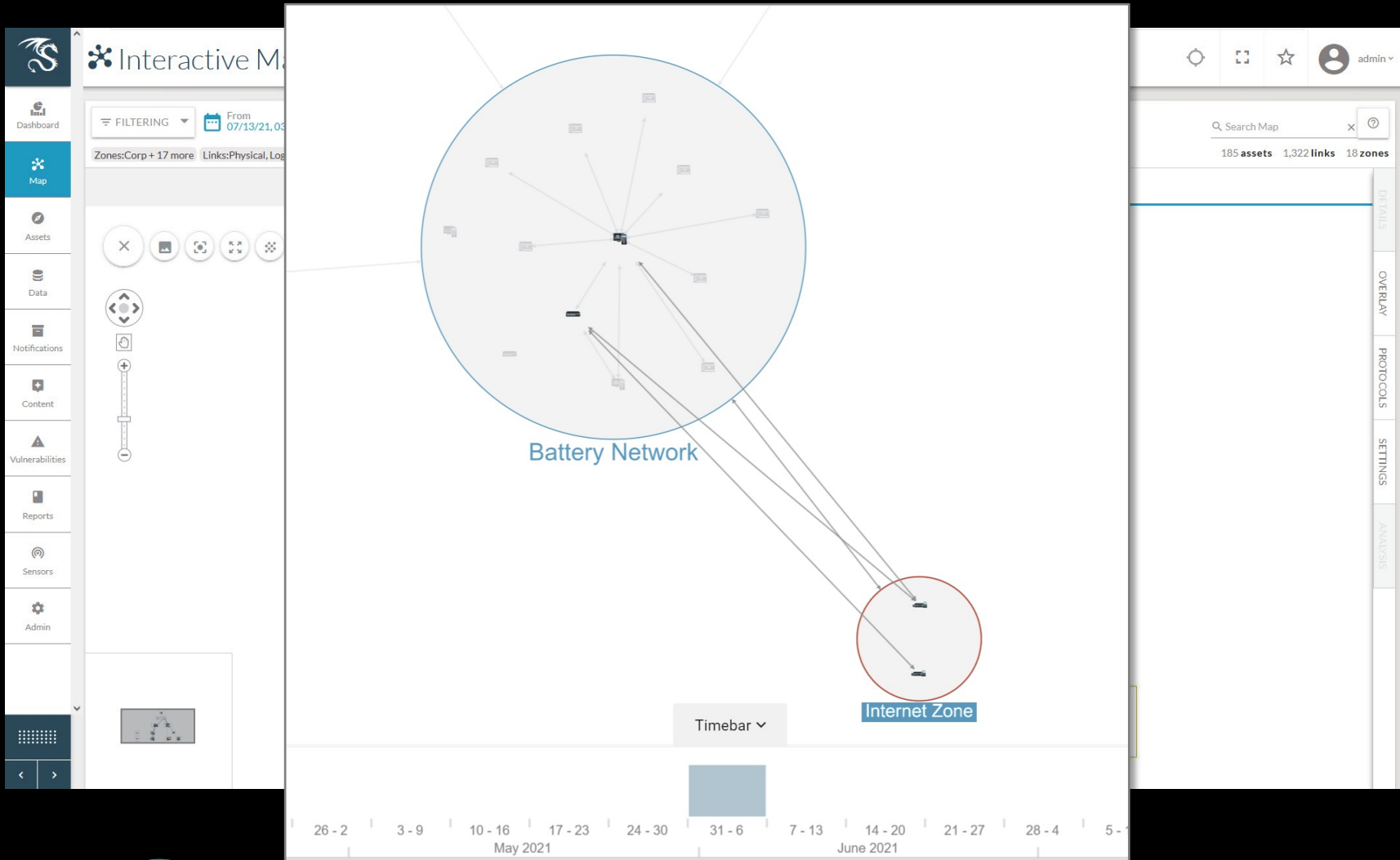
## FOR INDUSTRIAL CYBERSECURITY



# WHAT'S NEW IN THIS RELEASE

- Visual Map Performance Updates
- Asset Explorer → Asset Inventory Management
- Vulnerability Management – new!
- UI/UX updates to:
  - Asset Inventory
  - Vulnerability Management
  - includes improved Searching, Filtering, and Group By

# PLATFORM INTERACTIVE MAP/TIMELINE VIEW



- ✓ Scales to 100,000s of Assets
- ✓ Cross-Sensor and Cross-Site visibility
- ✓ Timeline and historical views for investigations
- ✓ Highly customizable zoning

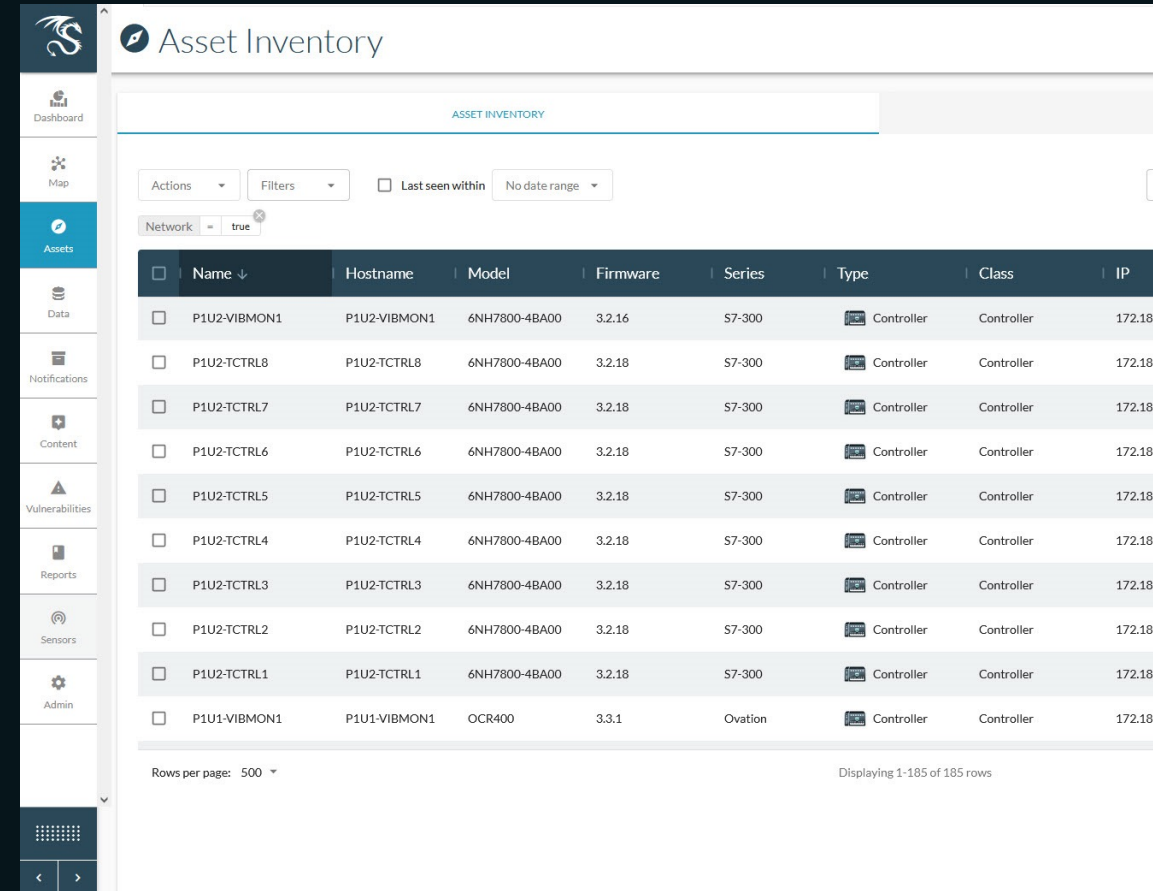
# ASSET INVENTORY LIFECYCLE MANAGEMENT

New UX - Asset Inventory, Asset List, and Asset Summary/Details view

Assets will be represented as persistent objects, not bound by time

User Import of assets, attributes, and non-discoverable data

New Asset Bulk Edit workflows



The screenshot displays the 'Asset Inventory' management interface. It features a sidebar with navigation options: Dashboard, Map, Assets (selected), Data, Notifications, Content, Vulnerabilities, Reports, Sensors, and Admin. The main content area shows a table of assets with the following columns: Name, Hostname, Model, Firmware, Series, Type, Class, and IP. The table contains 185 rows of data, with the first 10 rows visible. The assets are categorized as 'Controller' and include details such as model numbers (e.g., 6NH7800-4BA00) and IP addresses (e.g., 172.18.0.1).

Name	Hostname	Model	Firmware	Series	Type	Class	IP
P1U2-VIBMON1	P1U2-VIBMON1	6NH7800-4BA00	3.2.16	S7-300	Controller	Controller	172.18.0.1
P1U2-TCTRL8	P1U2-TCTRL8	6NH7800-4BA00	3.2.18	S7-300	Controller	Controller	172.18.0.2
P1U2-TCTRL7	P1U2-TCTRL7	6NH7800-4BA00	3.2.18	S7-300	Controller	Controller	172.18.0.3
P1U2-TCTRL6	P1U2-TCTRL6	6NH7800-4BA00	3.2.18	S7-300	Controller	Controller	172.18.0.4
P1U2-TCTRL5	P1U2-TCTRL5	6NH7800-4BA00	3.2.18	S7-300	Controller	Controller	172.18.0.5
P1U2-TCTRL4	P1U2-TCTRL4	6NH7800-4BA00	3.2.18	S7-300	Controller	Controller	172.18.0.6
P1U2-TCTRL3	P1U2-TCTRL3	6NH7800-4BA00	3.2.18	S7-300	Controller	Controller	172.18.0.7
P1U2-TCTRL2	P1U2-TCTRL2	6NH7800-4BA00	3.2.18	S7-300	Controller	Controller	172.18.0.8
P1U2-TCTRL1	P1U2-TCTRL1	6NH7800-4BA00	3.2.18	S7-300	Controller	Controller	172.18.0.9
P1U1-VIBMON1	P1U1-VIBMON1	OCR400	3.3.1	Ovation	Controller	Controller	172.18.0.10

# DRAGOS PLATFORM OVERCOMES OT/ICS VULN MANAGEMENT CHALLENGES

Public vulnerability sources (ICS-CERT/NVD) have incomplete or inaccurate data

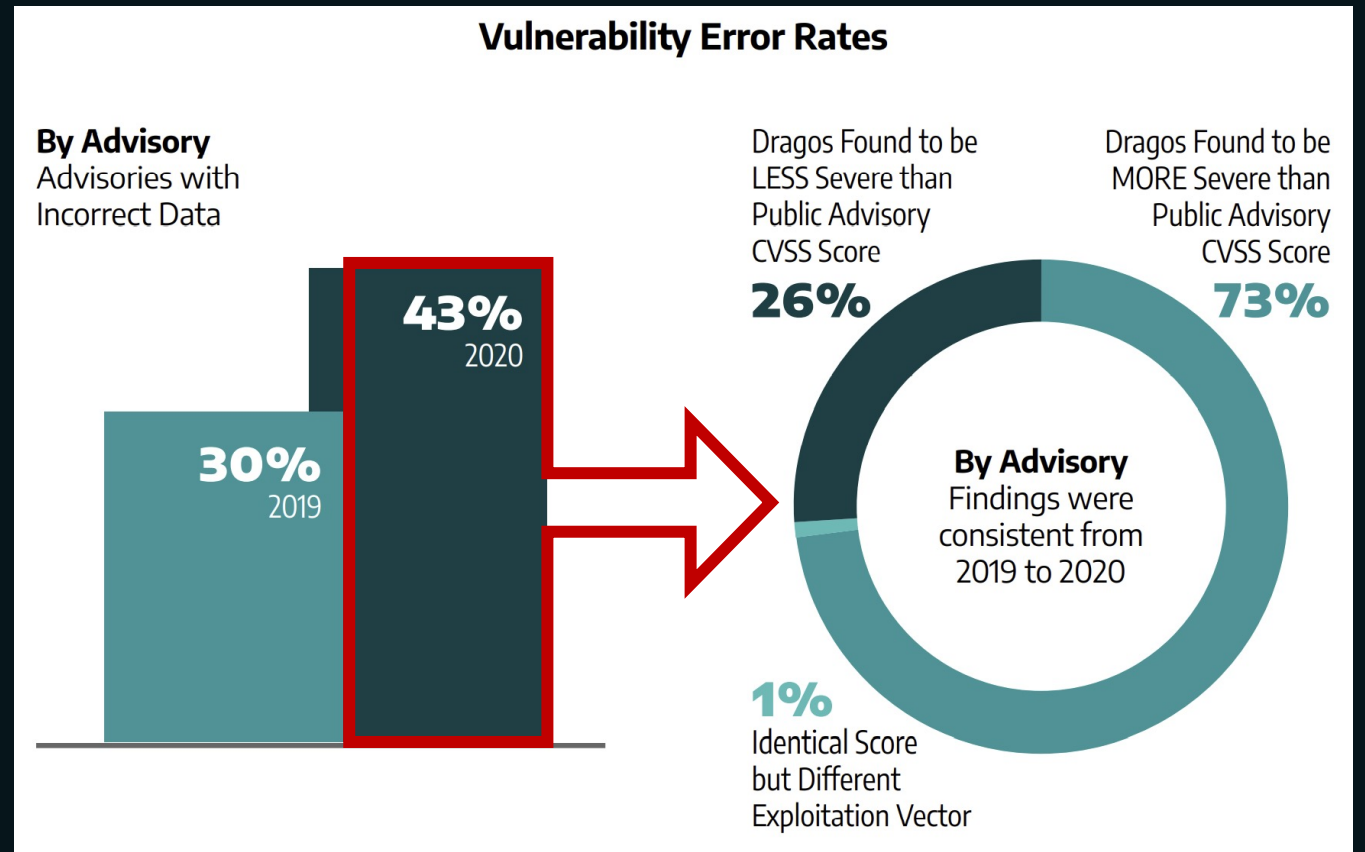
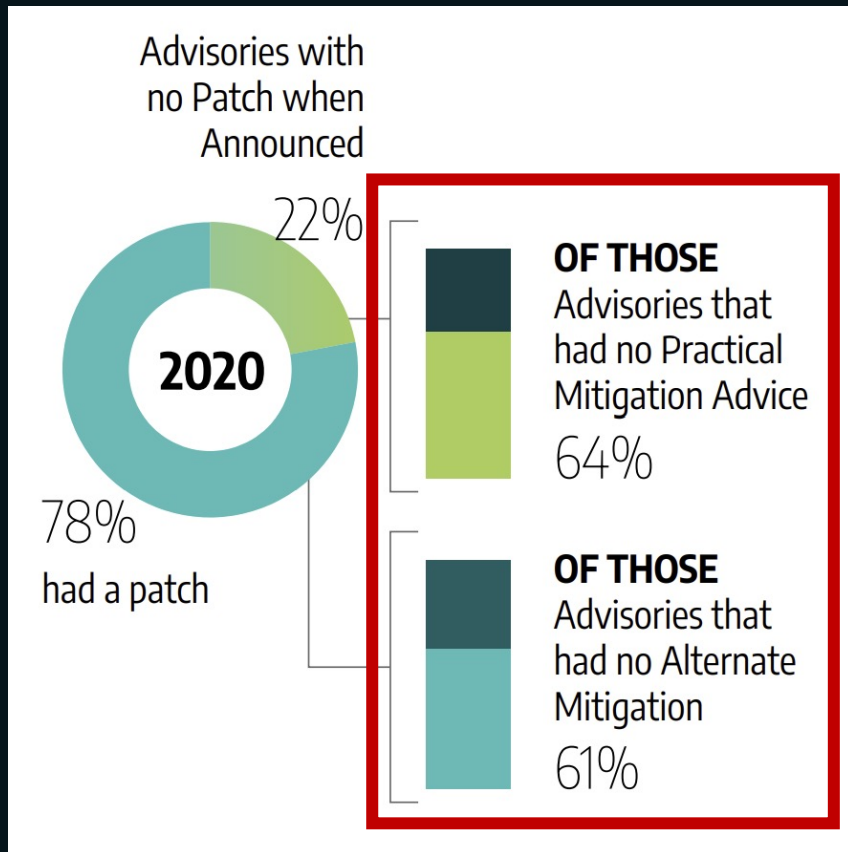
OEM Vendors often do not provide mitigation guidance

IT-style active scanning is not suitable for production / critical OT systems

Vulnerability assessment without management leaves issues untracked and attack points

# DRAGOS VULNERABILITY INTELLIGENCE

## YEAR IN REVIEW 2020



# EXAMPLE: DRAGOS FOUND CVE LESS SEVERE

## ROCKWELL AUTOMATION LOGIX CONTROLLERS

### CISA ICS Advisory – CVSS 10.0 Critical

**ICS Advisory (ICSA-21-056-03)** [More ICS-CERT Advisories](#)

**Rockwell Automation Logix Controllers (Update A)**

Original release date: March 18, 2021

[Print](#) [Tweet](#) [Send](#) [Share](#)

---

Legal Notice

All information products included in <https://us-cert.cisa.gov/ics> are provided "as is" for informational purposes only. The Department of Homeland Security does not endorse any commercial product or service, referenced in this product or otherwise. Further information regarding any information contained within. DHS does not endorse any commercial product or service, referenced in this product or otherwise. Further information regarding any information contained within. DHS does not endorse any commercial product or service, referenced in this product or otherwise. Further information regarding any information contained within. For more information about TLP, see <https://us-cert.cisa.gov/tlp/>.

**1. EXECUTIVE SUMMARY**


- CVSS v3 10.0
- ATTENTION:** Exploitable remotely/low skill level to exploit
- Vendor:** Rockwell Automation
- Equipment:** Studio 5000 Logix Designer, RSLogix 5000, Logix Controllers
- Vulnerability:** Insufficiently Protected Credentials

**Note:**  
**CVE-2019-19790**  
 9.8 => 7.5  
 AV:N/AC:L/PR:N

### Dragos – Limited Threat – Priority “Next”

**Rockwell Automation Logix Controllers**

Date: Feb 25, 2021  
 Source: ICS-CERT  
**CVE-2021-22681**

**Dragos Assessment** 

Attributes	
Proof of Concept Exists	No
Active Exploitation	No
Skill Level Required	Low

**Access Level Required**

Remotely Exploitable	✓
Access Required	
Insufficiently Protected Credentials	
Remote Action	
Remote DoS	
Remote Service	✓
Exposure	
Configuration/Modify App	✓
...s	
<b>be:</b>	✓
	✓
	✓

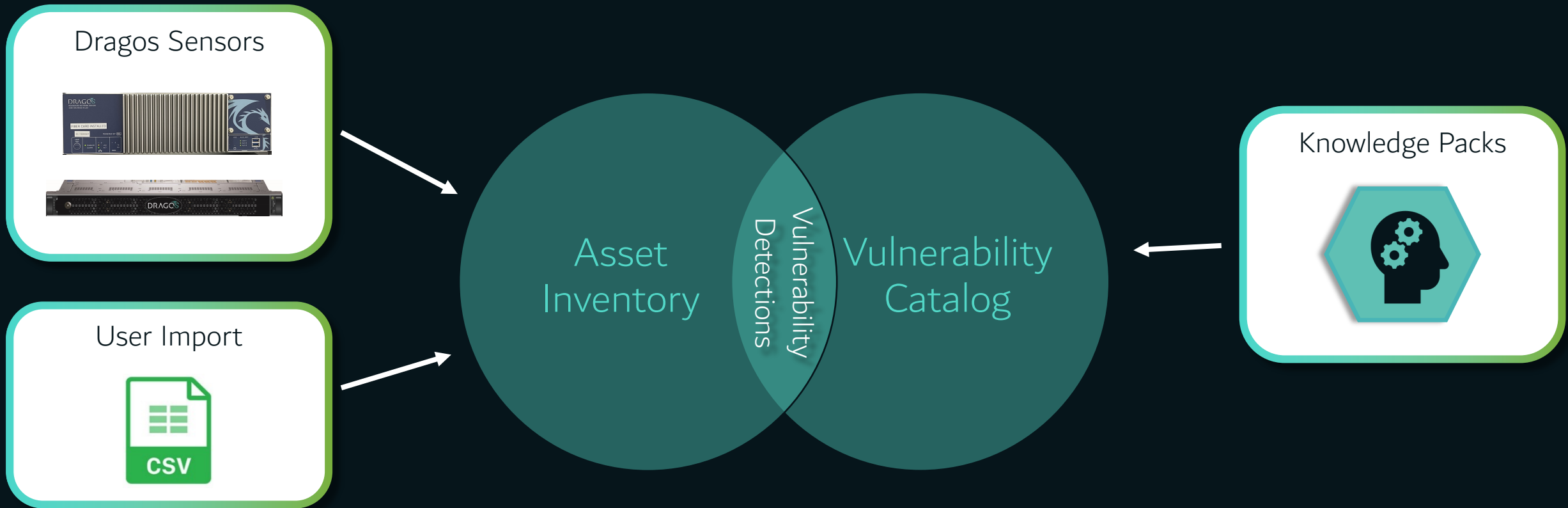
Dragos does agree that an attacker could leverage the private key to mount an attack. However, when determining the scope of the threat, we took the following mitigating factors into mind:

- Controllers in RUN mode are not affected.
- Controllers using CIP Security are not affected.
- Controllers are found at Level 1 of the Purdue model. Unauthorized access to Level 1 of an ICS network should either be impossible or limited.
- The private key has not been leaked.
- No public proof of concept exists. Any PoC would be a significant undertaking as it would require the attacker work out all of the crypto algorithms and require the attacker to implement their own version of the Logix Designer to Controller Ethernet/IP communications.
- This vulnerability has not been known to be exploited in the wild.

With all of that in mind, Dragos does not believe this issue requires immediate action.



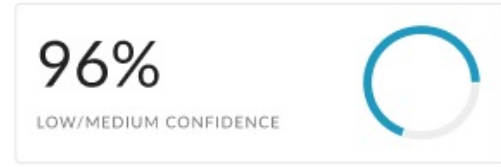
# INVENTORY-BASED VULN ASSESSMENT





- Map
- Assets
- Data
- Notifications
- Content
- Vulnerabilities
- Reports
- Sensors
- Admin

10 Vulnerability Detections  
5 Unique CVEs



Title	CVE	CVSS	Risk Level	Confidence	Priority	First Detected	Last Detected	Asset
<input type="checkbox"/> Treck TCP/IP Stack	CVE-2020-25066	9.0	High - 4	High	Next	2020-12-18	2020-12-21	proc-hmi 10.50.7.99
<input type="checkbox"/> Schneider Electric Easergy T300	CVE-2020-7561	8.6	High - 4	High	Next	2020-11-19	2020-12-11	seleasergyfrt 10.50.6.32
<input type="checkbox"/> Siemens Embedded TCP/IP Stack Vulnerabilities (AMNESIA:33)	CVE-2020-13988	7.5	Medium 3	Low	Never	2020-12-11	2020-12-16	svr180frt 10.50.6.180
<input type="checkbox"/> GE UR Series Relays Denial of Service	CVE-2018-5475	6.3	Critical - 5	High	Now	2018-02-26	2021-01-06	ge-ur-001 10.50.7.200
<input type="checkbox"/> SEL AcSElerator Architect	CVE-2018-10604	5.1	Low - 2	Low	Next	2020-11-25	2020-11-30	selsvrftA 10.49.6.44
<input type="checkbox"/> OSIsoft PI Interface for OPC XML-DA	CVE-2013-0006	4.2	High - 4	Medium	Next	2013-01-09	2020-11-20	historian-frt 10.41.0.10
<input type="checkbox"/> WECON PLC Editor	CVE-2020-25177	4.1	High - 4	Medium	Next	2020-12-01	2020-12-02	plc-svr-ft 10.41.0.11
<input type="checkbox"/> Netlogon Vulnerability 'ZeroLogon'	CVE-2020-1472	3.8	Critical - 5	High	Now	2020-08-17	2020-12-24	winsvr0456 10.41.1.12
<input type="checkbox"/> HMS Networks Ewon Flexy and Cosy	CVE-2020-16230	2.1	Medium 3	High	Never	2020-09-18	2020-12-23	hms88frt-a 10.11.48.9
<input type="checkbox"/> Cisco IOS XR Software DVMRP Memory Exhaustion	CVE-2020-3566	2.0	High - 4	High	Next	2020-08-29	2020-09-04	router-frt-prod 10.0.0.1

Rows per page: 10



## Rockwell Automation CompactLogix 5370 and ControlLogix 5570 Controllers

Successful exploitation could allow an adversary to send a malicious CIP pack...

Priority - Next Risk Level - High

Confidence ●●●

Highest CVSS Base: 7.5

State Open

### Asset Details

Name	PLC-1
Hostname	-
FQDN	localhost
MAC	5C:88:16:EE:7C:47
IP	192.168.20.30



Source	Intelligence	Published	03/02/21, 00:00 UTC
First Seen	06/14/21, 15:26 UTC		
Last Seen	06/14/21, 15:30 UTC	CVE-2020-6998	



### Summary

## Summary



### Links

### Description

Successful exploitation could allow an adversary to send a malicious CIP packet, causing a DoS condition and interrupting communication between the controller and other products.

### Affected Products

Hardware: Rockwell Automation, ControlLogix, 5570, <=33

Current:

Hardware: Rockwell Automation, ControlLogix, 1756-L71/B LOGIX5571, 32.11

OS:



### Threat

### Dragos Guidance

Update to a patched version, [v33.011 or later](#).

Restrict access to ports UDP/2222, TCP/44818, and UDP/44818. Ensure controllers are not directly connected to the internet.

### Product Summary

Rockwell Automation's CompactLogix and ControlLogix are controllers deployed worldwide and commonly seen in the critical manufacturing industry.



### Impacted Assets 2

Port	# Source IPs	Actions
2222	7 ?	⋮
44818	12 ?	⋮

← Validate that network mitigations are in-place and working correctly



### History



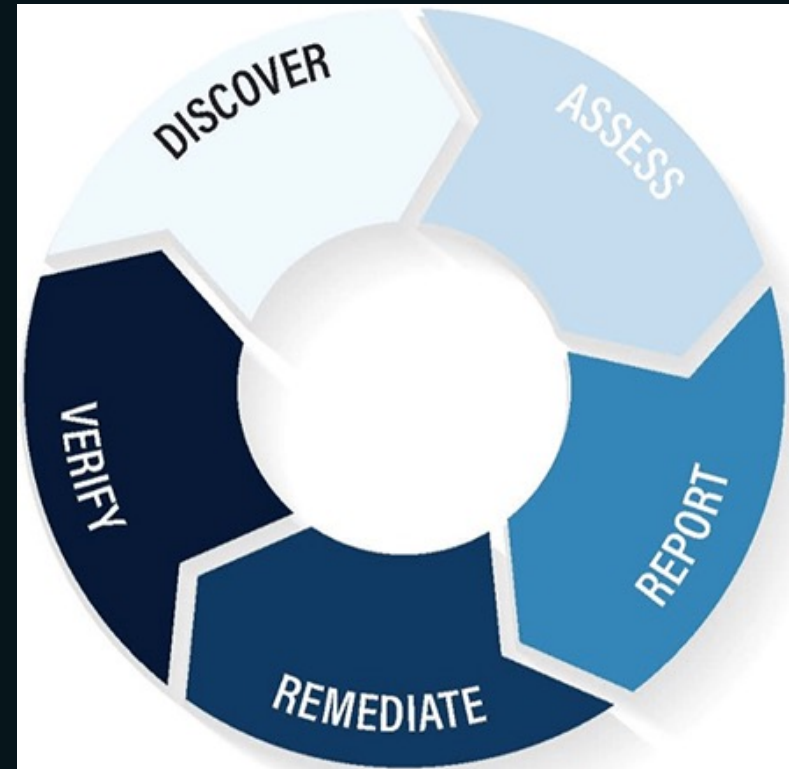
### CVEs



# VULNERABILITY MANAGEMENT

## FUNCTIONALITY AND PROCESSES TO:

- + **Identify** Vulnerabilities in asset firmware, operating systems, applications
- + **Prioritize** the Vulnerabilities based on active attacks, adversarial tactics, exploits
- + **Recommend** remediations and mitigations
- + **Allow** for manual severity changes, asset/process criticality, context definition
- + **Track** remediations over time, verify fixed remediations, including reopened vulnerabilities
- + **Report** on current, historical, trends



# DISPOSITIONING A VULNERABILITY

**Remediation** – The vulnerability no longer exists

+ Examples: Patching, uninstalling, reconfiguring, decommissioning

**Mitigation** – The vulnerability is no longer reasonably exploitable

+ Examples: Compensating controls such as network firewalls, app firewalls, data diodes, network segmentation, air gap

**Risk Acceptance** – The organization has accepted the risk of this vulnerability

+ Examples: Dragos prioritized as “Never,” Operational Risk outweighs Vulnerability Risk

# DISPOSITIONING IS KEY TO VULN MANAGEMENT

True Vulnerability Management requires that all vulnerabilities are tracked, not just hidden.

If you aren't tracking disposition, you are only performing Vulnerability Assessment.

The screenshot displays a vulnerability management interface. At the top, a yellow badge indicates 'Risk Level 4 - Limited'. Below it, 'Confidence' is shown with three blue dots and 'Highest CVSSv3 Base: 7.2 (High)'. A 'State' dropdown menu is open, showing options: 'Open', 'Risk Accepted', 'False Positive', and 'Close Vulnerability' (highlighted in red). To the right, an 'Asset' sidebar lists fields: Host, FQDN, Class, Type, IP, and Asset Ris. Below the dropdown, a modal titled 'Vulnerability Resolution' is open. It contains a 'State' dropdown set to 'Closed - Mitigated' and a 'Reason' text box containing 'Mitigated by updating to latest version.' (highlighted in red). At the bottom right of the modal are 'CANCEL' and 'SAVE' buttons.

# DRAGOS VULNERABILITY DIFFERENTIATORS

1. We have the most accurate and corrected ICS Vulnerability intelligence in the industry (See: Year in Review 2020)
2. Dragos Prioritization and Guidance for all detected vulnerabilities
3. Complete vulnerability lifecycle tracking—can be used to track risk acceptance, compensating controls
4. Confidence Rating – filter out the noise allowing users to focus on what is most impactful to their operations



# THANK YOU

## Resources

- Year In Review Report : [dragos.com/yir](https://dragos.com/yir)
- Vulnerability management: [dragos.com/platform/vulnerability-management/](https://dragos.com/platform/vulnerability-management/)
- Asset management: [dragos.com/platform/asset-visibility/](https://dragos.com/platform/asset-visibility/)

Schedule a demo: [dragos.com/request-a-demo/](https://dragos.com/request-a-demo/)

Webinar on July 29 - MITRE Engenuity ATT&CK® Evaluations for ICS  
[dragos.com/webinars](https://dragos.com/webinars)