What’s Really Happening in OT Cyber-attacks (in 2025!)

Seth Enoka, Lesley Carhart

Principal Incident Responders, Dragos Australia

Seth Enoka

Principal Incident Responder

linkedin.com/in/sethenoka

- Dragos: Industrial DFIR
  - Before: Middle East, Cisco, Clayton Utz, Klein & Co.
- SANS Instructor: FOR508 Advanced Incident Response and Threat Hunting
- GSE #320
- No Starch Press Author
  - Cybersecurity for Small Networks

GIAC SECURITY GSE EXPERT
GIAC SECURITY GSP PROFESSIONAL
GIAC CERTIFIED GCFE FORENSIC EXAMINER
GIAC CERTIFIED GCFA FORENSIC ANALYST
GIAC NETWORK GNFA FORENSIC ANALYST
GIAC REVERSE ENGINEERING GREM MALWARE
GIAC PENETRATION GPEN TESTER
GIAC EXPLOIT RESEARCHER & GXPN ADVANCED PENETRATION TESTER
GIAC WEB APPLICATION GWAPT PENETRATION TESTER
GIAC SECURITY ESSENTIALS GSEC CERTIFICATION
GIAC CERTIFIED GCIA INTRUSION ANALYST
GIAC RESPONSE AND GRID INDUSTRIAL DEFENSE
GIAC STRATEGIC PLANNING GSTRT POLICY & LEADERSHIP
ISC2 CISSP

Lesley Carhart

Technical Director, Incident Response

@hacks4pancakes
linkedin.com/in/lcarhart

- 7+ Years at Dragos, Inc
  - Previously - Motorola Solutions, United State Air Force (Retired)
- 17+ years in Critical Infrastructure Cybersecurity Incident Response
- SANS Instructor: ICS515 - ICS Visibility, Detection, and Response
- Conference and Clinic Organiser

GIAC REVERSE ENGINEERING GREM MALWARE

GIAC PENETRATION GPEN TESTER

GIAC RESPONSE AND GRID INDUSTRIAL DEFENSE

GIAC CERTIFIED GCFA FORENSIC ANALYST

GIAC CERTIFIED GCFE FORENSIC EXAMINER

GIAC CERTIFIED GCIH INCIDENT HANDLER

DMA DIFFERENCE MAKERS AWARDS

OT Incident Response is a Unique Space

- Life / Safety / Process Consequences
- Legacy Systems and Topologies
- Low-Level Process Devices
- Vendors, OEMs, and Operations Staff
- Low Cybersecurity Maturity
- Criticality of Uptime

70% of vulnerabilities **reside deep within the network**

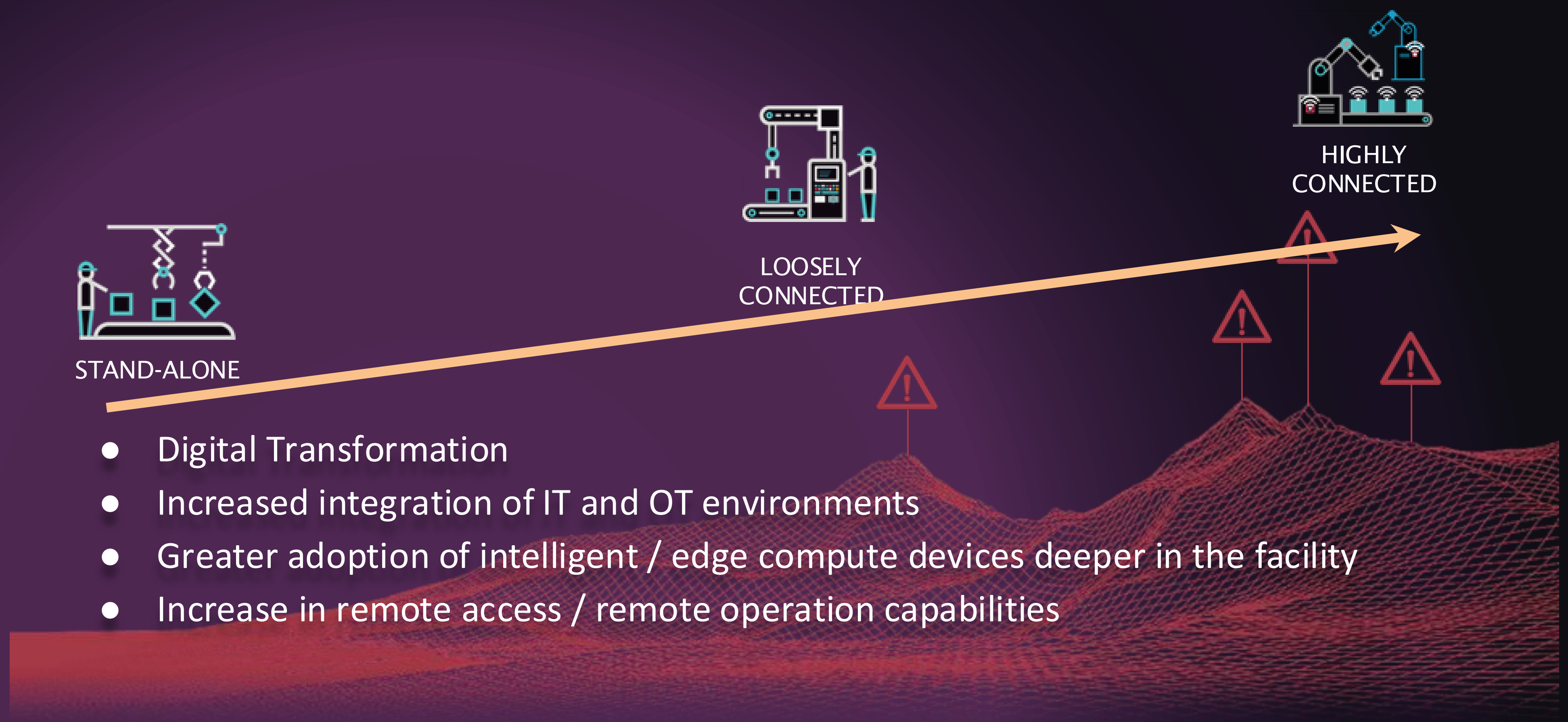
22% of advisories **had incorrect data** in 2024

39% of advisories analysed **could cause both a loss of view and loss of control**, down from 53% in the previous year

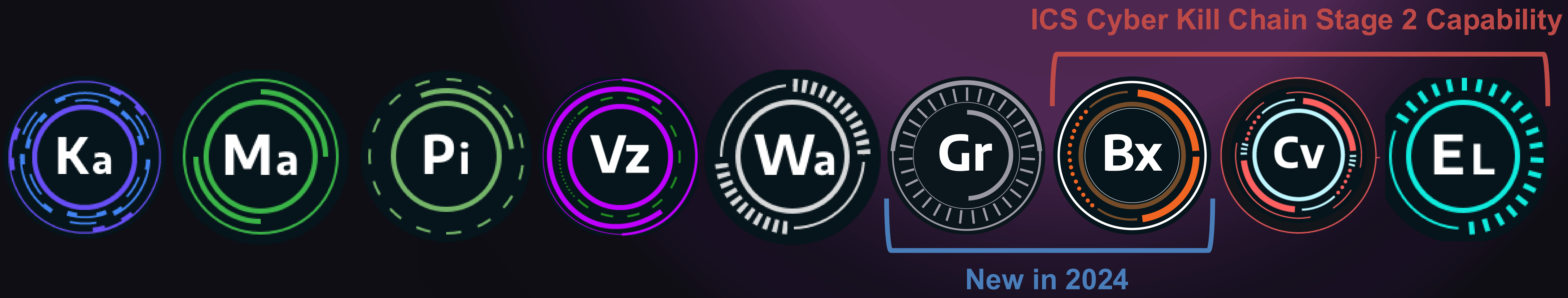
22% of advisories were **network exploitable and perimeter facing** in 2024

The Changing OT Threat Landscape

- IT / OT Technology Convergence
- Remote Access and Telemetry
- Attacker Awareness and Maturity
- Regulation
  - SOCI / SLACIP, IPART
- Homogenisation of Industrial Tech Deployments



- Digital Transformation
- Increased integration of IT and OT environments
- Greater adoption of intelligent / edge compute devices deeper in the facility
- Increase in remote access / remote operation capabilities



Five Misconceptions & Assumptions Impair OT Cybersecurity

1. Cybersecurity teams rely on **incorrect assumptions:**
   - Network maps
   - Asset inventories
   - Security controls
   - Monitoring
   - Backups
   - Remote access
2. Leadership **incorrectly assume enterprise plans, tools, and procedures transfer** to OT
3. IT teams incorrectly assume lack of modern systems, updates, and contemporary enterprise security tooling is **due to apathy or poor maintenance**
4. Organisations **assume they are either the best** or **the worst** at OT cybersecurity and avoid tackling the challenges head-on
5. Cybersecurity personnel prioritise **"cyber stuff"** over **process consequences**

Categories of Attack to Which We Respond

Commodity / Criminal

Insider (Intentional, Unintentional)

State / Terrorist (Sabotage, Espionage)

Not Every Outage or Event is Cyber-Related

Most events are caused by maintenance or human operational errors

Number of cyber-related events is **increasing meaningfully**

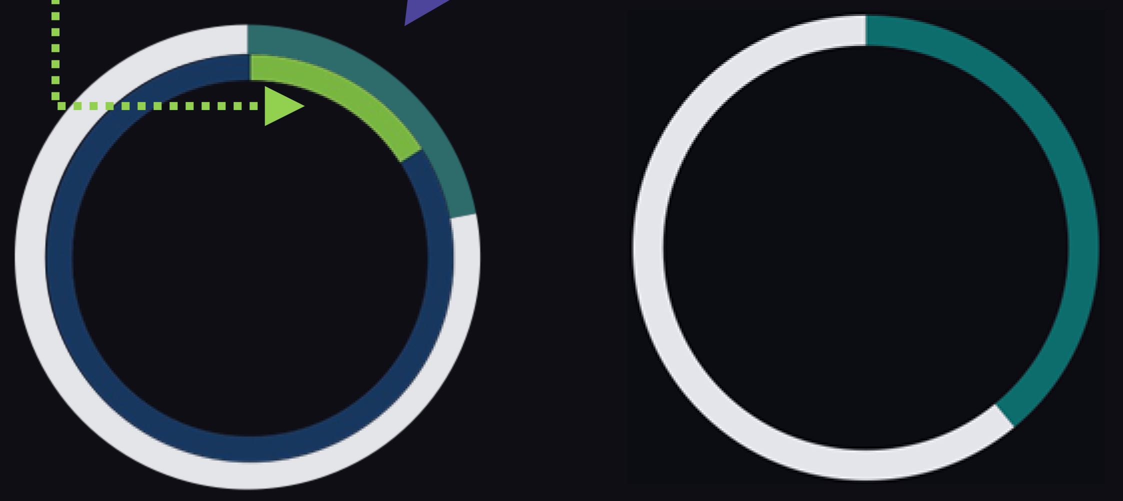
Understanding and **identifying** cyber-caused events is important for everyone

Intrusion Vectors

- **Lowest barrier** / cost to entry to accomplish goal
- **Least chance of detection** using traditional, automated tools
- Attacks of **opportunity** by initial access brokers
- Networks are **rarely air-gapped** and rarely use textbook **Purdue Model DMZ segmentation** today
- OT networks are **increasingly exposed**

This growth is due in part to the number of perimeter devices being actively exploited in industrial organisations related to hacktivism, ransomware, and threat groups.

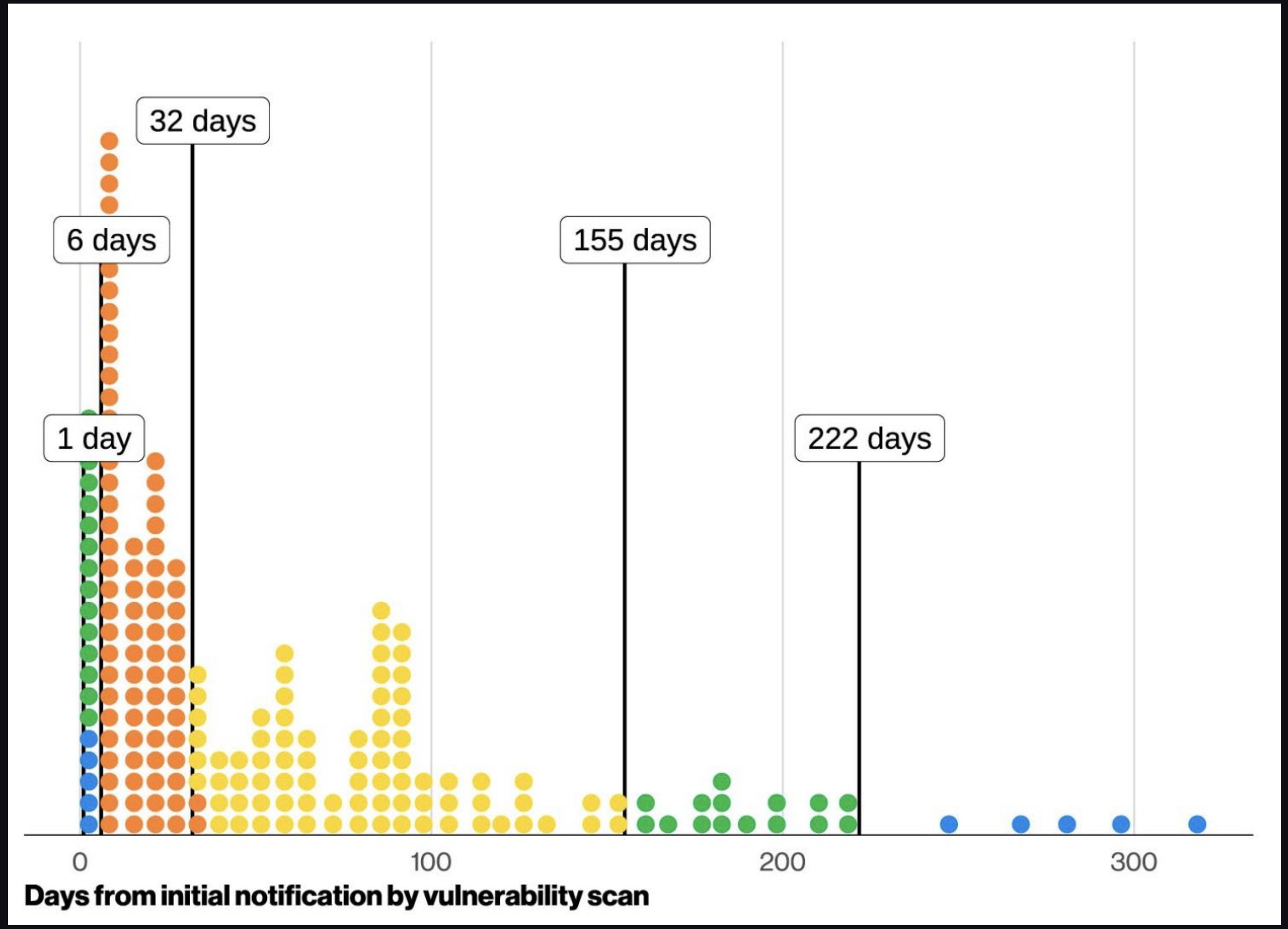
16%
in 2023



22%
of advisories were network-exploitable and perimeter-facing

39%
of vulnerabilities could cause both a loss of view and a loss of control

Vulnerabilities: Time to Patch



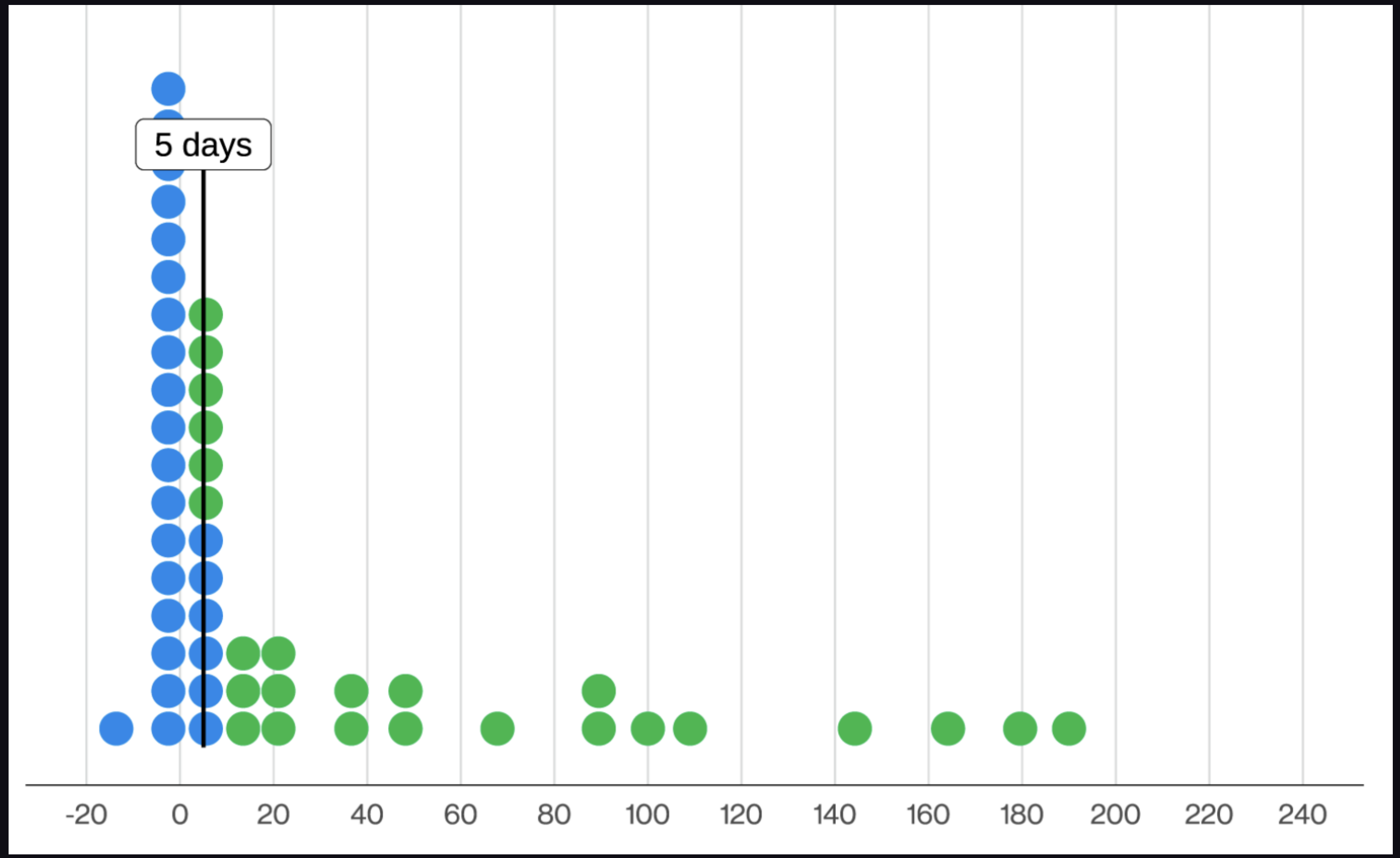
Ref: Verizon, 2024 DBIR

- CISA Known Exploited Vulnerabilities (KEV) catalogue
- These are **only KEV vulnerabilities**
- On average, organisations patch KEV vulnerabilities at **38 days**
- On average, organisations patch **edge device** KEV vulnerabilities at **36 days**

4.5%
of vulnerabilities had a proof-of-concept (POC) and were actively exploited

70%
of vulnerabilities were at lower levels within the ICS network

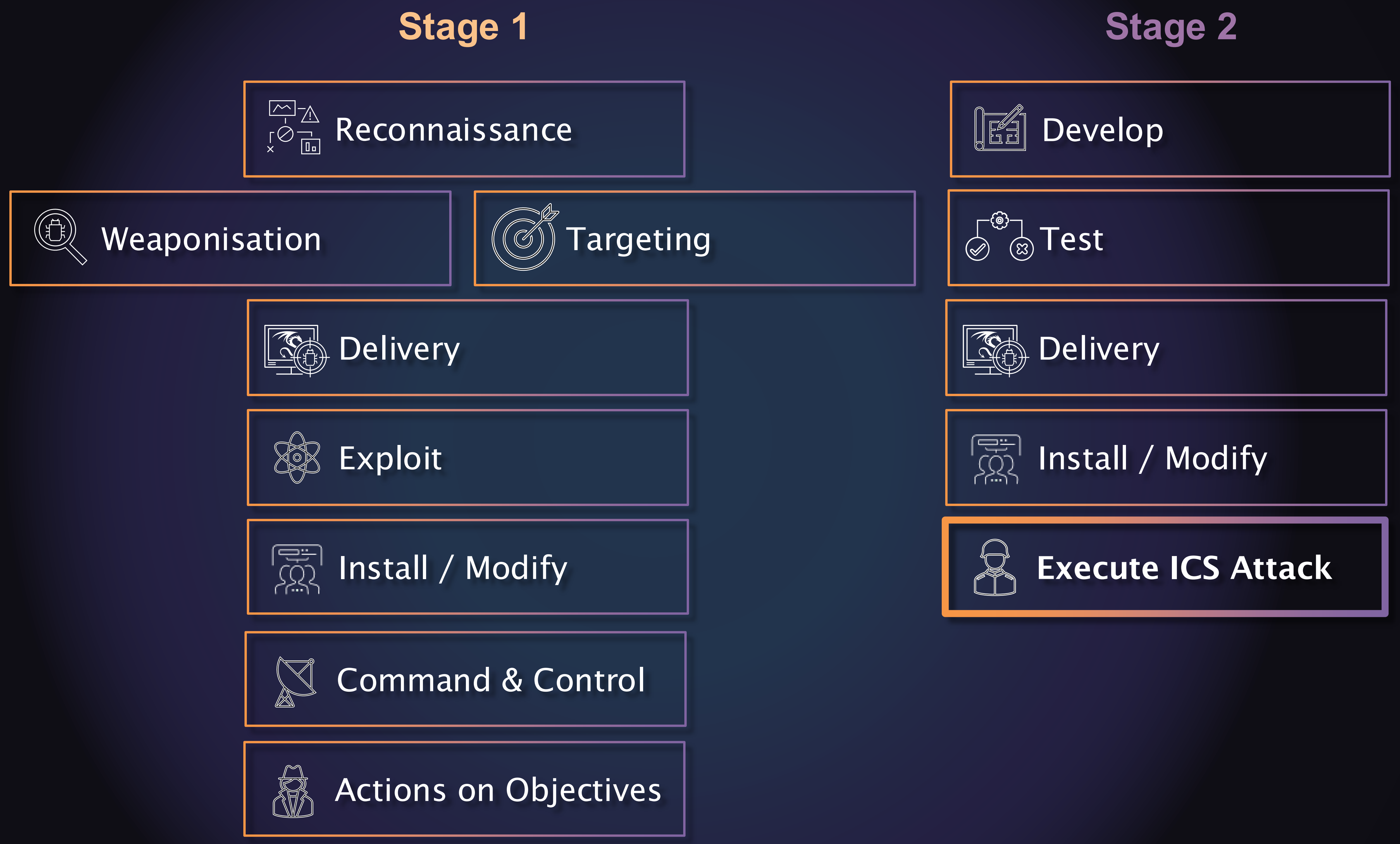
Vulnerabilities: Time to Exploit



- On average, adversaries **exploit for KEV-listed vulnerabilities after 5 days**
- On average, adversaries **exploit edge devices** listed on KEV **within 0 days**!
- Patch KEV-listed vulnerabilities first!

Adversary TTPs Inside OT Environments

- "**Living off the land**" and human-driven compromise is common
- Long **reconnaissance** periods
- No sense in using malware or hacking PLCs **when access to an operator's interface** will suffice
- Separate "**Stage 1**" and "**Stage 2**" intrusions, teams, and activities
- Stage 2 can require far more **resources and expertise** than Stage 1
- Criminal / low-skill actors also **make errors** that disrupt process systems



Stage 1

Reconnaissance

Weaponisation

Targeting

Delivery

Exploit

Install / Modify

Command & Control

Actions on Objectives

Stage 2

Develop

Test

Delivery

Install / Modify

Execute ICS Attack

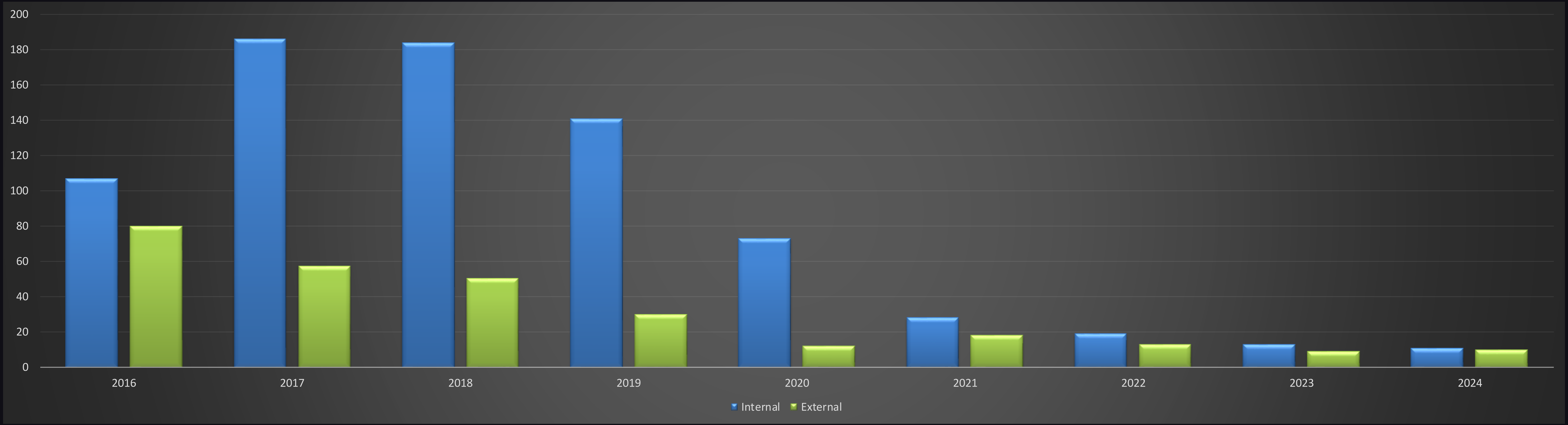
https://www.sans.org/white-papers/36297

Median Dwell Time: 2011 – 2024

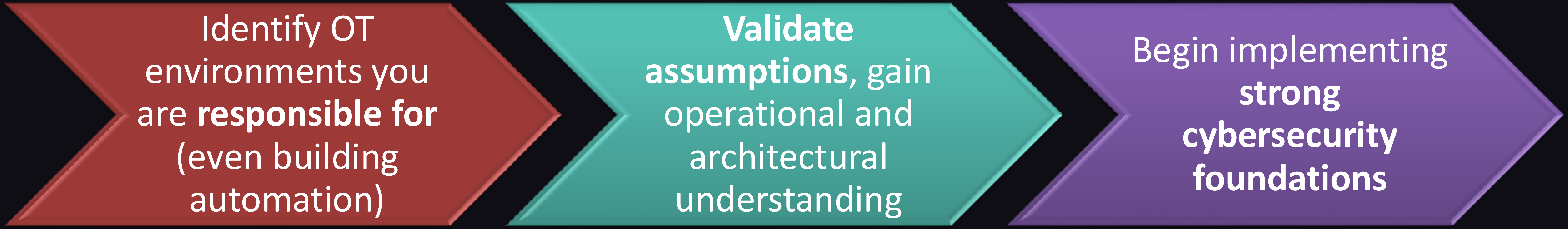
Ref: FireEye, M-Trends 2025

	2011	2012	2013	2014	2015	2016	2017	2018	2019	2020	2021	2022	2023	2024
All	416	243	229	205	146	99	101	78	56	24	21	16	10	11
External	–	–	–	–	320	107	186	184	141	73	28	19	13	11
Internal	–	–	–	–	56	80	57.5	50.5	30	12	18	13	9	10

An adversary is active for **11** days, before you detect them.



Solutions and Strategies We Recommend

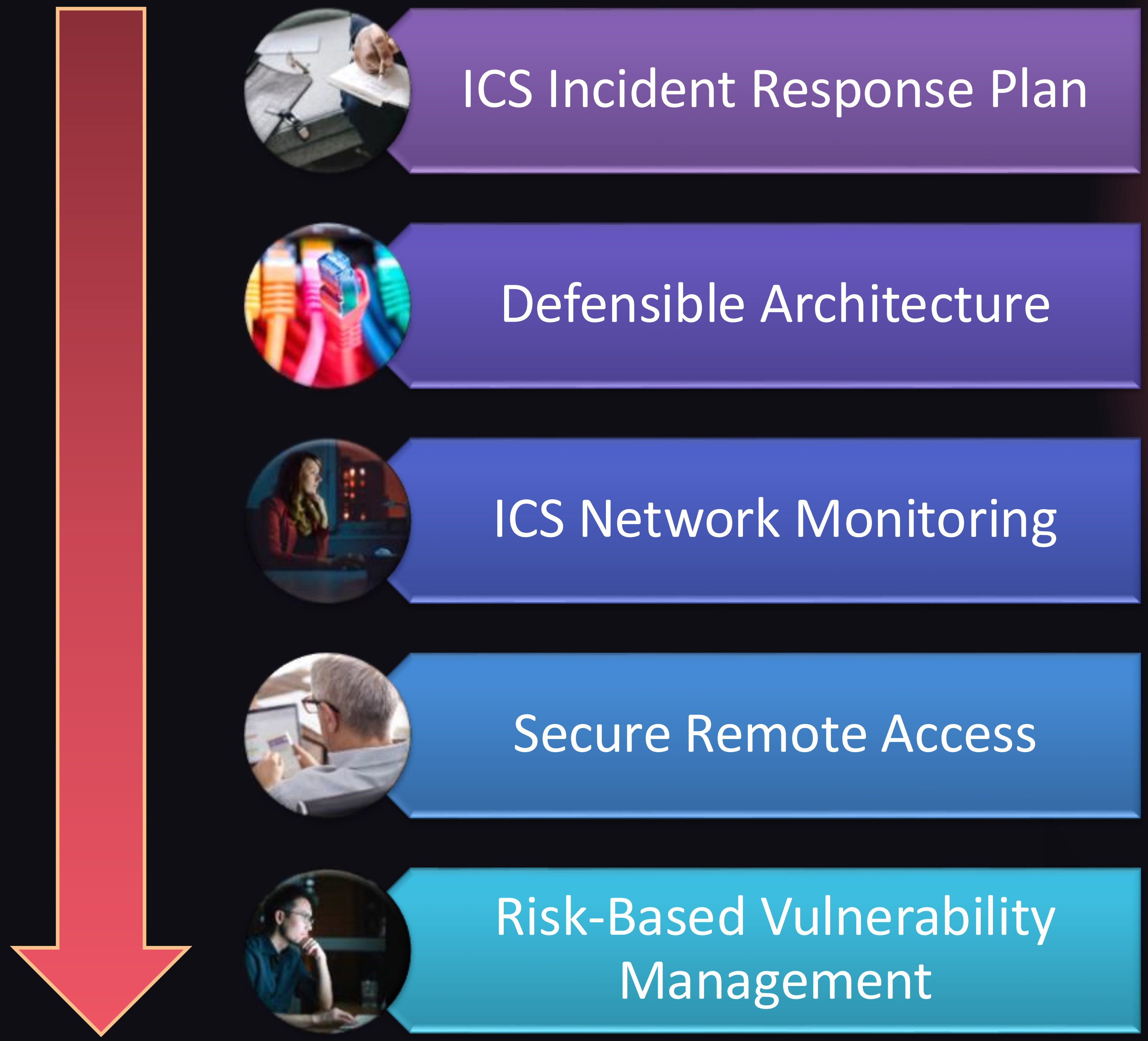


Identify OT environments you are **responsible for** (even building automation)

Validate assumptions, gain operational and architectural understanding

Begin implementing **strong cybersecurity foundations**

The Five Critical Controls for ICS Cybersecurity (Academic Whitepaper)



- ICS Incident Response Plan
- Defensible Architecture
- ICS Network Monitoring
- Secure Remote Access
- Risk-Based Vulnerability Management

https://www.sans.org/white-papers/five-ics-cybersecurity-critical-controls

Whitepaper

The Five ICS Cybersecurity Critical Controls

Written by **Robert M. Lee** and **Tim Conway**

October 2022

Looking Ahead: What We Expect in 2026 >

1. **Authentication Token and Cloud API Abuse**

2. **Supply Chain Attacks**
   - Who are your critical vendors for authentication and remote access?
   - What open-source software do you rely on?
   - Who has remote and physical access to your process environments?

3. **Attack toolkits with OT modules** and capabilities for common ICS deployments and architectures

Looking Ahead: What We Expect in 2026 >

4. AI-Enhanced Attacks

- Shorten an attacker’s path to compromise in unfamiliar environments
- Understanding of process and device function

5. Abuse of Common Software to Hide

- RMM Tools, living-off-the-land

6. Evasion of EDR

- Disabling and tampering EDR is becoming routine
- Beach Heads on non-monitored devices

Contact

Seth Enoka
senoka@dragos.com
linkedin.com/in/sethenoka

Lesley Carhart
lcarhart@dragos.com
linkedin.com/in/lcarhart - @hacks4pancakes