



DO NO HARM APPROACH

OT Native Cybersecurity for OT Environments

Yesterday's OT

Isolated

Serial based connections.
Local physical access was
main method to control

Obscure

Home grown system, highly
specialized comms

Safe

High cost, custom,
expert attack

Today's OT

Connected

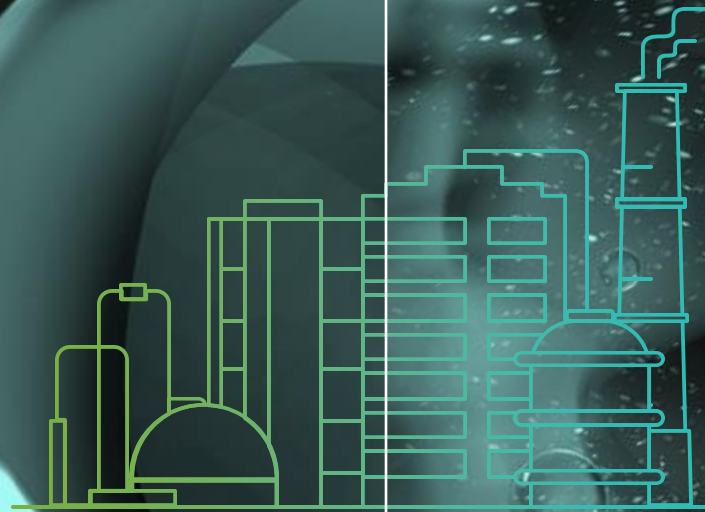
Modernization,
digital transformation,
remote & 3rd party access

Homogenous

Common software across automation
systems widens target
list for given attack method

Targeted

Nation states & common
ransomware gangs motivated
by malice & money



IT and OT Security is Different

A man wearing a white hard hat and a high-visibility yellow safety vest over a light-colored shirt and jeans is holding a tablet. He is standing in an industrial environment with yellow railings and large pipes in the background.

Informational Technology

Systems & Data
Confidentiality
Integrity

Operational Technology

Systems of Systems
Physical Safety
Operational Continuity

The SANS 5 Critical Controls

SANS

5

ICS CYBER
SECURITY
CRITICAL
CONTROLS

01 ICS Incident Response Plan

02 Defensible Architecture

03 ICS Network Visibility & Monitoring

04 Secure Remote Access

05 Risk-based Vulnerability Management

SANS Critical Control #3

Implement **continuous network security monitoring** of the ICS environment



Requires a
protocol-aware
toolsets



Provides system of
systems interaction
analysis



Informs operations
of potential risks
to control



Unique Challenges in Monitoring OT Environments

OT Systems and Protocols Differ from IT

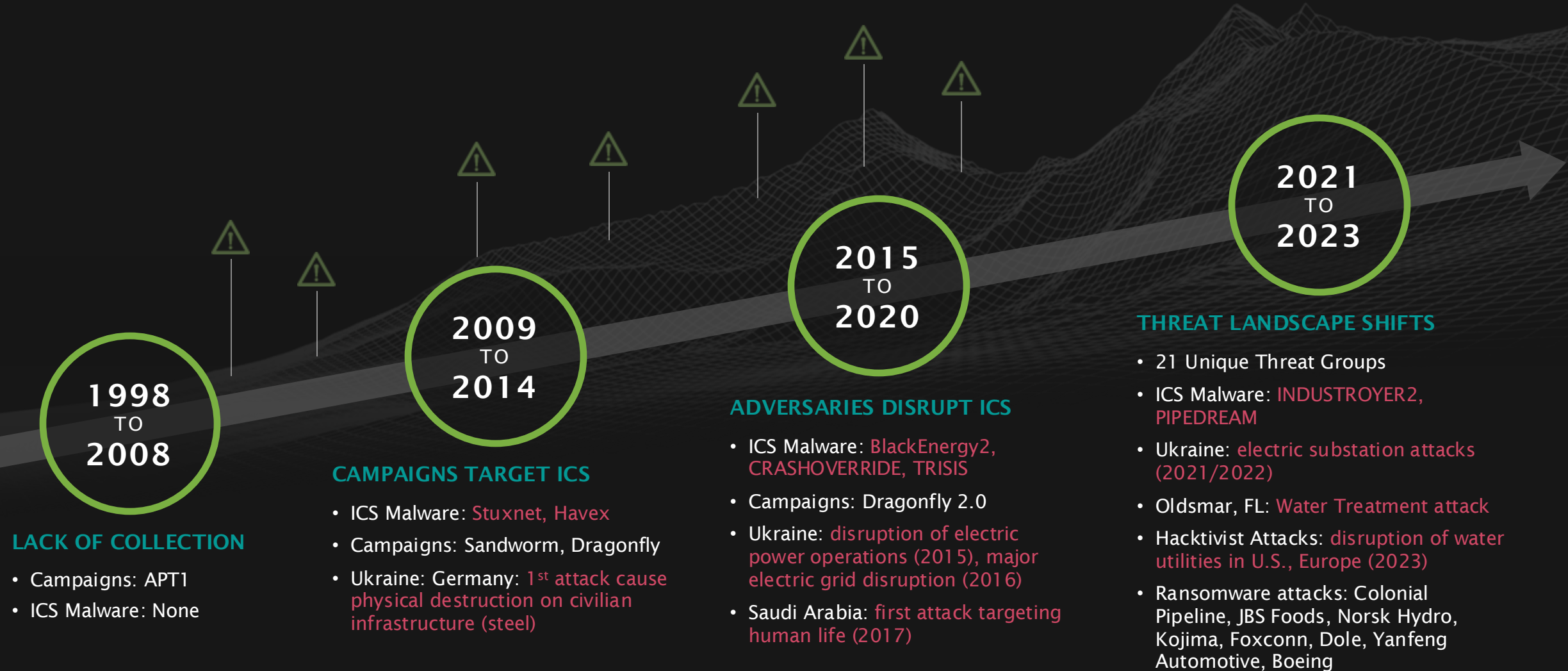
Diverse Devices - OT, IT, IOT and IIOT

100% Uptime – Availability Requirements

Increase in OT Specialized Adversaries and Tools



More Frequent & Sophisticated Threats to OT



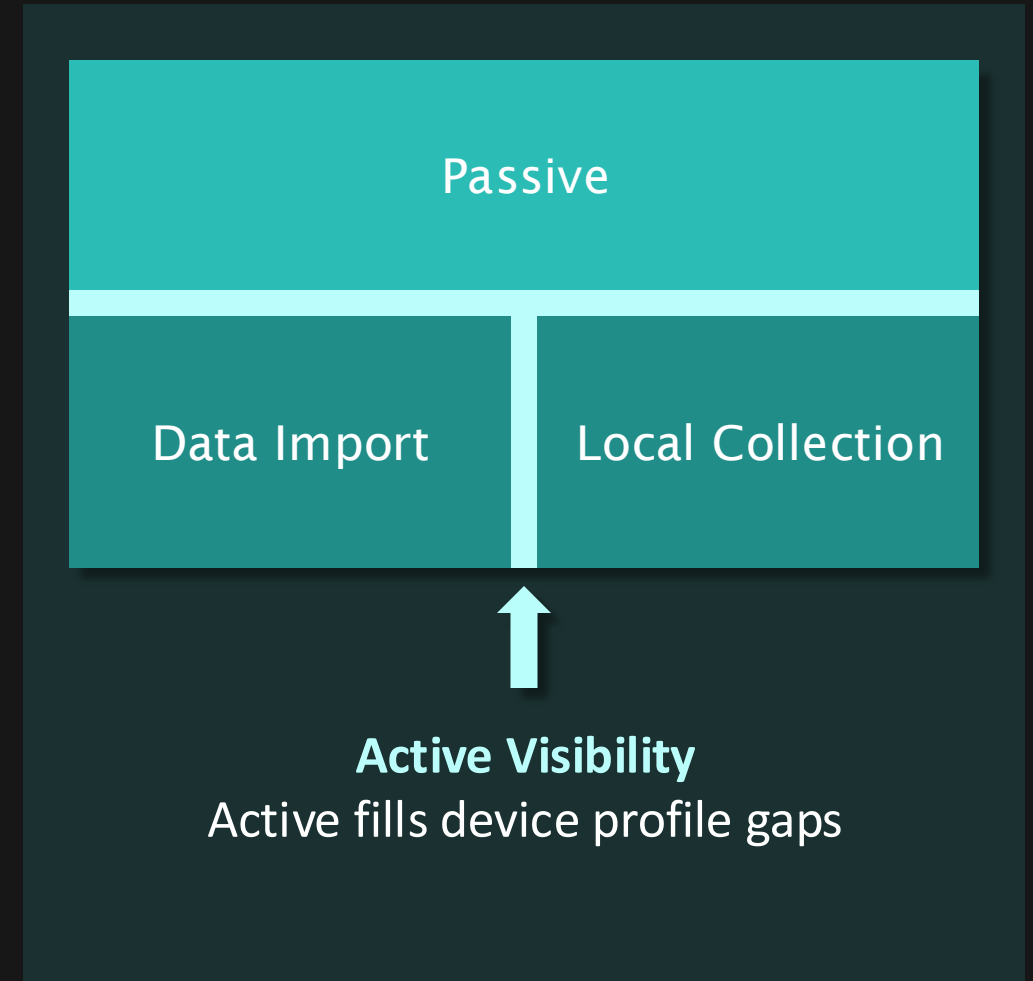
The background is a dark, industrial scene, possibly a factory or data center, with various pipes, cables, and machinery. Overlaid on this is a network diagram consisting of green lines and nodes, suggesting a complex network structure. The text is centered within a dark rectangular box with a thin green border.

Do No Harm: OT Native Network Monitoring

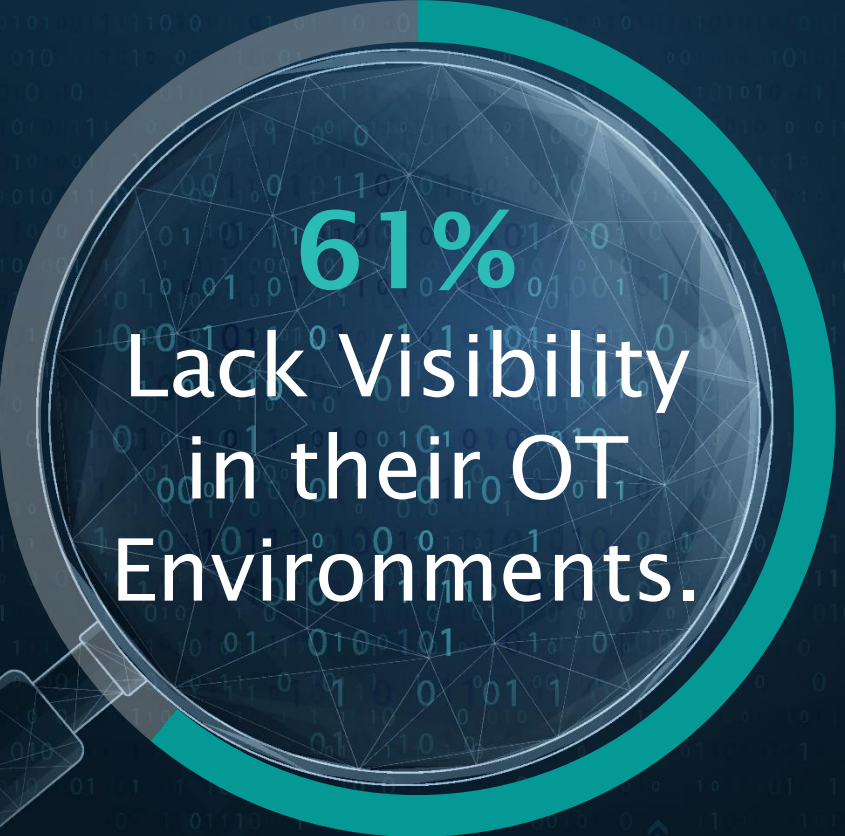
Passive First and Active to Fill Gaps

Support the goal of 100% uptime with minimal operational interruptions

- ✓ Monitor at the IT/OT boundary and deep into OT environment
- ✓ Lead with **passive** and utilize info you already have.
- ✓ Use **controlled active** methods to fill gaps or enhance profiles without disturbing to operation.



Build Visibility Foundation



61%
**Lack Visibility
in their OT
Environments.**

*YIR 2023, Dragos Services Customers

Ensure coverage across the common and proprietary ICS/OT protocols

Capture detailed logs of OT traffic

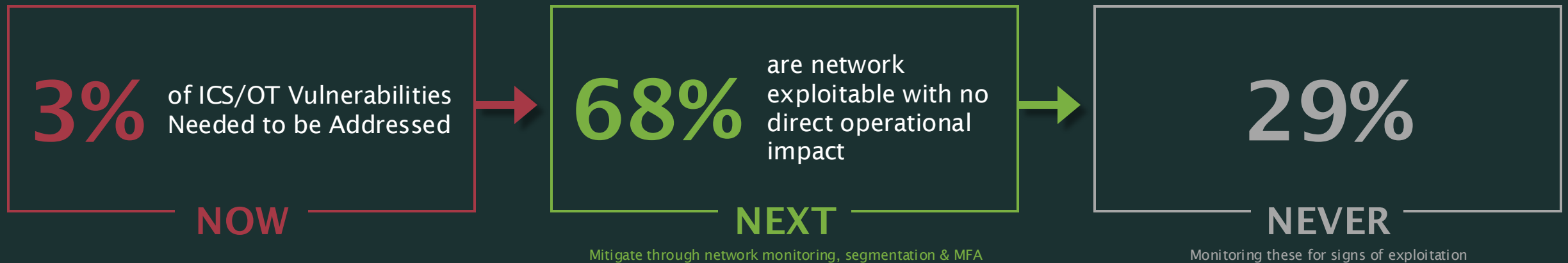
Identify OT assets, IT, IoT and IIOT devices

Beyond an Inventory – understand the role that the asset plays in the system

Establish normal behavior – in order to ID unusual or unexpected.

Practical Vulnerability Management: Alternatives to Patching

OT native required practical solutions not just “patch the device”



Understand the actual potential impact of the vulnerability

Utilize alternative mitigation to the risk that allows the process to safely continue

If necessary, provide a patch at the next maintenance window

Catch the Threat: OT Focused Threat Detection

IT tools often rely on anomaly detection



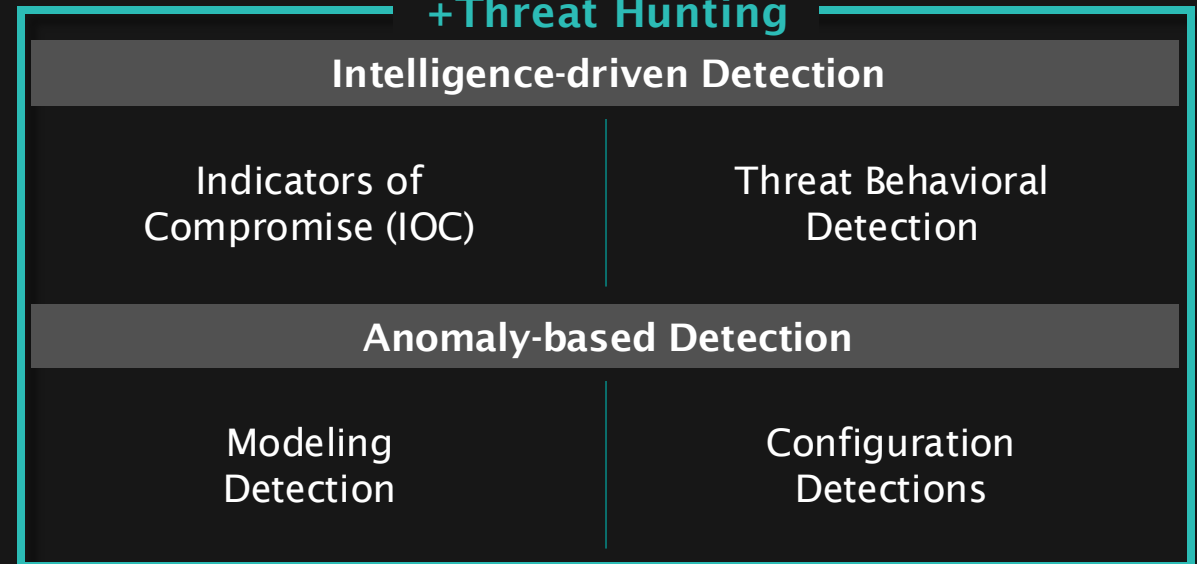
20+ threat activity groups directly target OT and ICS with specialized TTPs

OT Native to reduce false positives and improve accuracy

OT Cyber Threat Intelligence



+Threat Hunting



Value to Operations: Insights and Root Cause Analysis



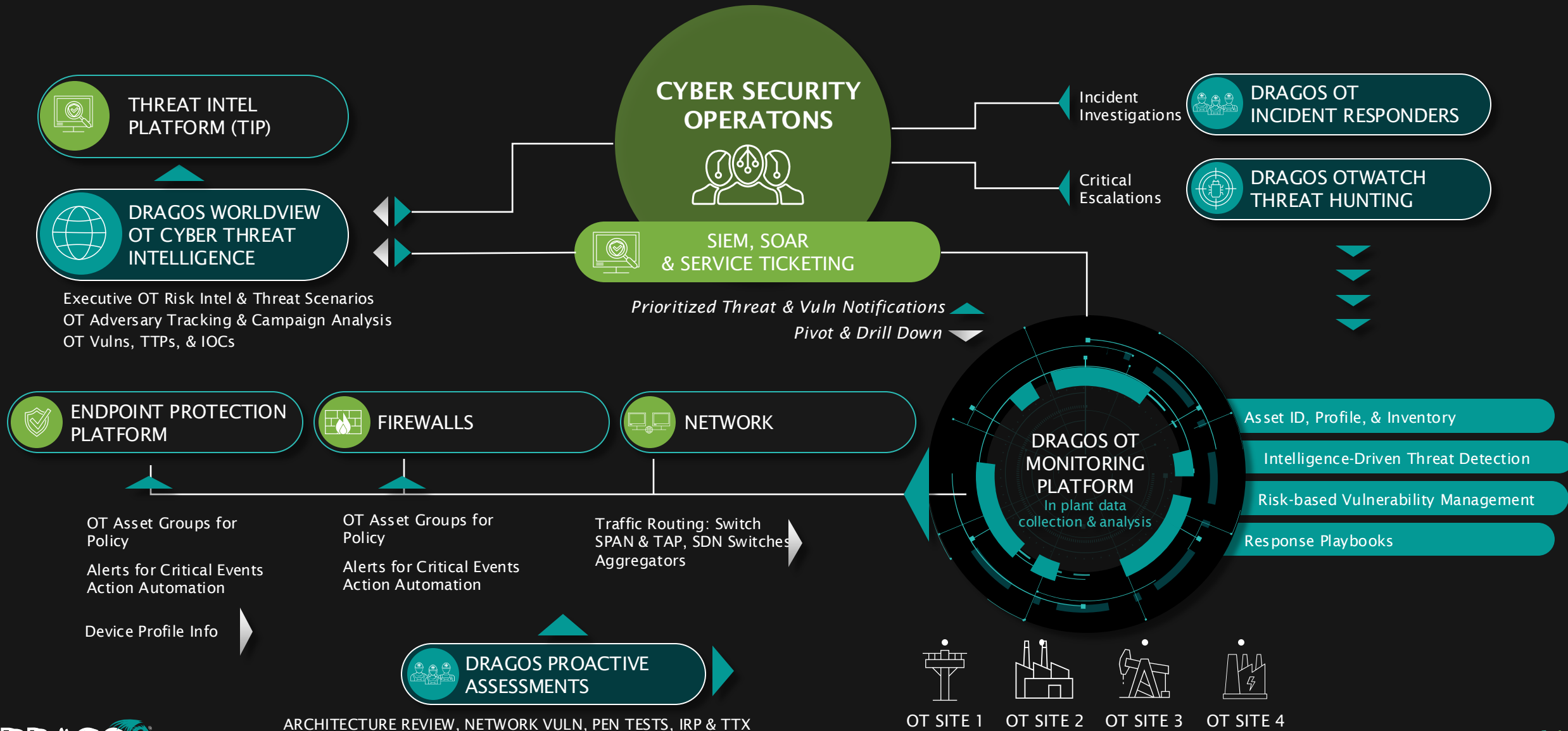
Identify misconfigurations

Root cause analysis

Non-disrupting monitoring

Mitigate vulnerabilities
without shutdown

IT + OT: Integrate with IT Security Operations



Dragos Platform

OT-Native Network Visibility & Monitoring



Boston Beer Company - Manufacturing



Iconic Brands


Samuel Adams, Dogfish Head, Truly and More

111 Million Cases
of Beer Produced

1.9 Million
Visitors to Properties

Drivers: Rise in ransomware targeting manufacturing and risk to physical damage, downtime, financial loss and safety hazards.

Need: Modernize IT security, build OT security for OT environments and improve overall infrastructure.



"We're not just a beer company, we're a manufacturing company. If we lose the ability to brew, bottle, and can, then we're out of business."

— Brandon Catalan, CISO

OT Native Network Visibility and Monitoring

Solution:

Dragos Platform Across 4 Sites

Ransomware Tabletop Exercises

OT Cyber Threat Intelligence

Dragos OT Watch for OT Threat Hunting

Outcome:

Visibility into OT networks and assets

Significant reduction in cybersecurity risk

Support operations with root cause analysis, troubleshooting and misconfiguration identification

IT, OT, leadership alignment on OT Security priority

100% investment ROI in first year

15% reduction in cyber insurance premiums

“When you really want to make a difference
and you’re not willing to gamble, you go
with the Cadillac. That is Dragos.”
– Brandon Catalan, CISO

Key Take Aways

- 1 Acknowledge Your Program Maturity

- 2 Align Plan to the Five Critical Controls

- 3 Build the Foundation: OT Native Network Monitoring

- 4 Become an Operations Ally

- 5 Secure Your Organization

The background is a dark, industrial scene, possibly a factory or warehouse, with various metal structures, pipes, and equipment. A large, dark rectangular box with a thin green border is centered on the image. Inside this box, the text "Thank You" is written in a large, white, sans-serif font. The overall tone is professional and technical.

Thank You