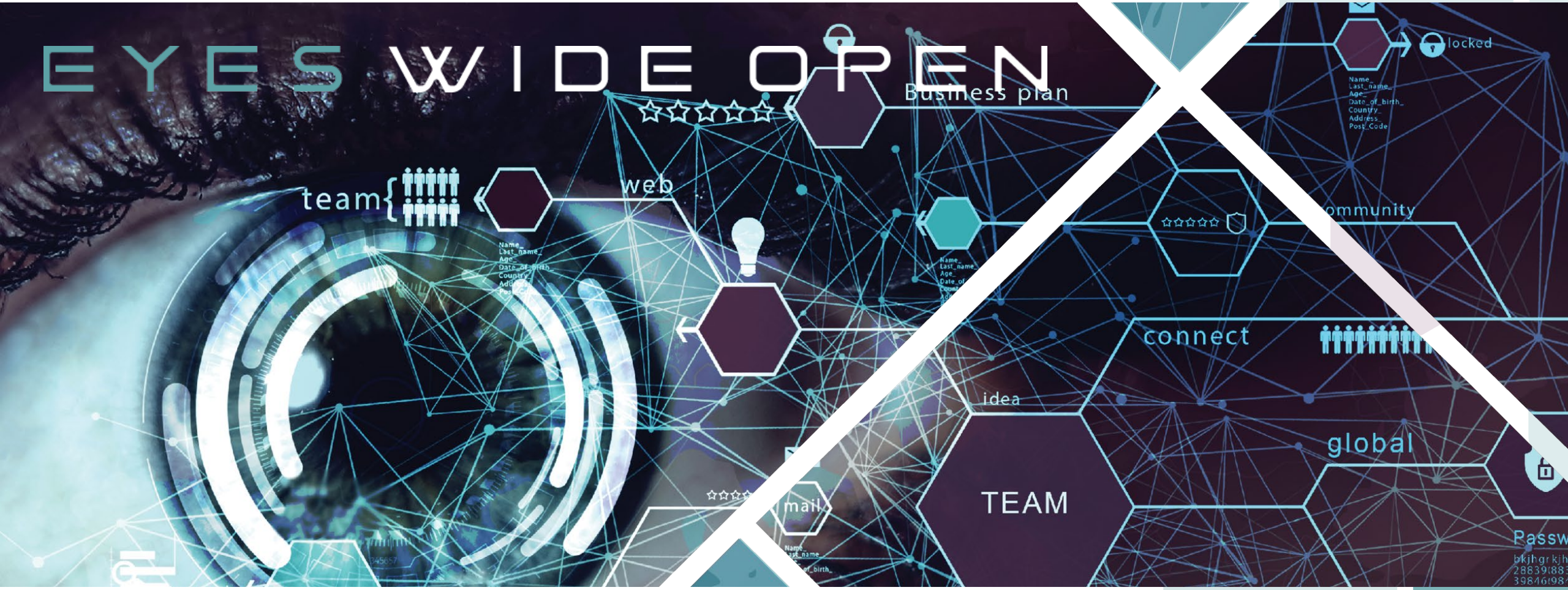
12TH ANNUAL LEADERSHIP EVENT

CYBER SECURITY SUMMIT

Security solutions through collaboration.™

TITLE SPONSOR

Island



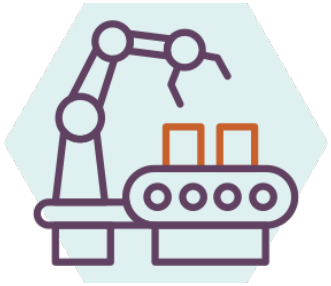
Securing IT and OT Convergence is a Team Sport

Bryan Gillson

Head of Vertical
Strategy, Ordr

Why Are We Here?

Secure Operational Environments Critical To The Way We Live

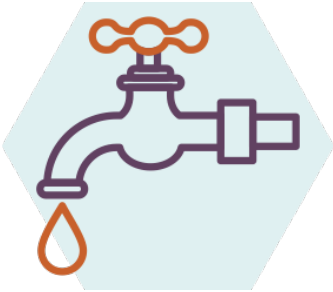


Manufacturing

Waste water treatment

Food and Beverage

Oil and Gas



Utilities

Healthcare Providers

Logistics

Pharma

Who is the Team? Multiple Silos With Differing Objectives

Security

"I care about data protection, security and governance.
This is business critical."

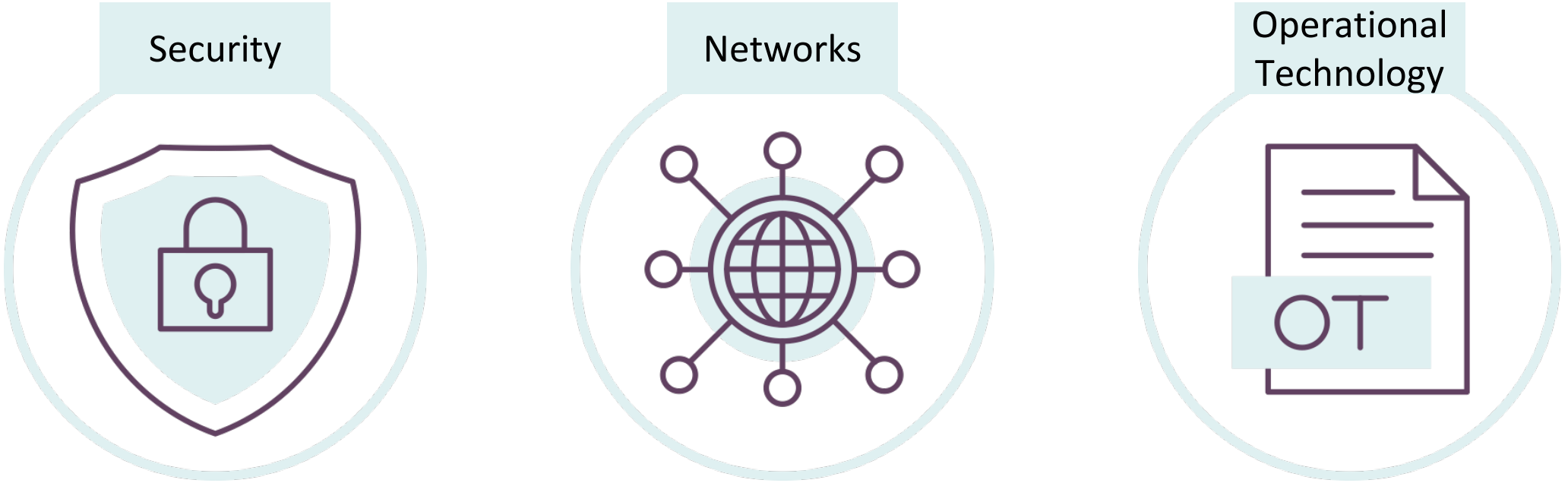
Networks

"I need know what's on my network to ensure capacity and resiliency.
This is business critical."

Operational Technology

"We need to keep operations running efficiently and safely.
This is business critical."

Who is the Team? Multiple Silos With Differing Objectives



Board of Directors:

“I don’t care about silos. You need to secure it all.”

Digital Transformation Highlights the Problem of Silos

Asset Inventory

- Insufficient visibility into IoT and OT devices
- Devices not in CMDB
- Rogue devices
- Varying business criticality

Dynamic Segmentation

- No more Purdue air gaps
- Segmentation for devices across IT, OT and cloud
- Devices flows between groups, Internet, cloud

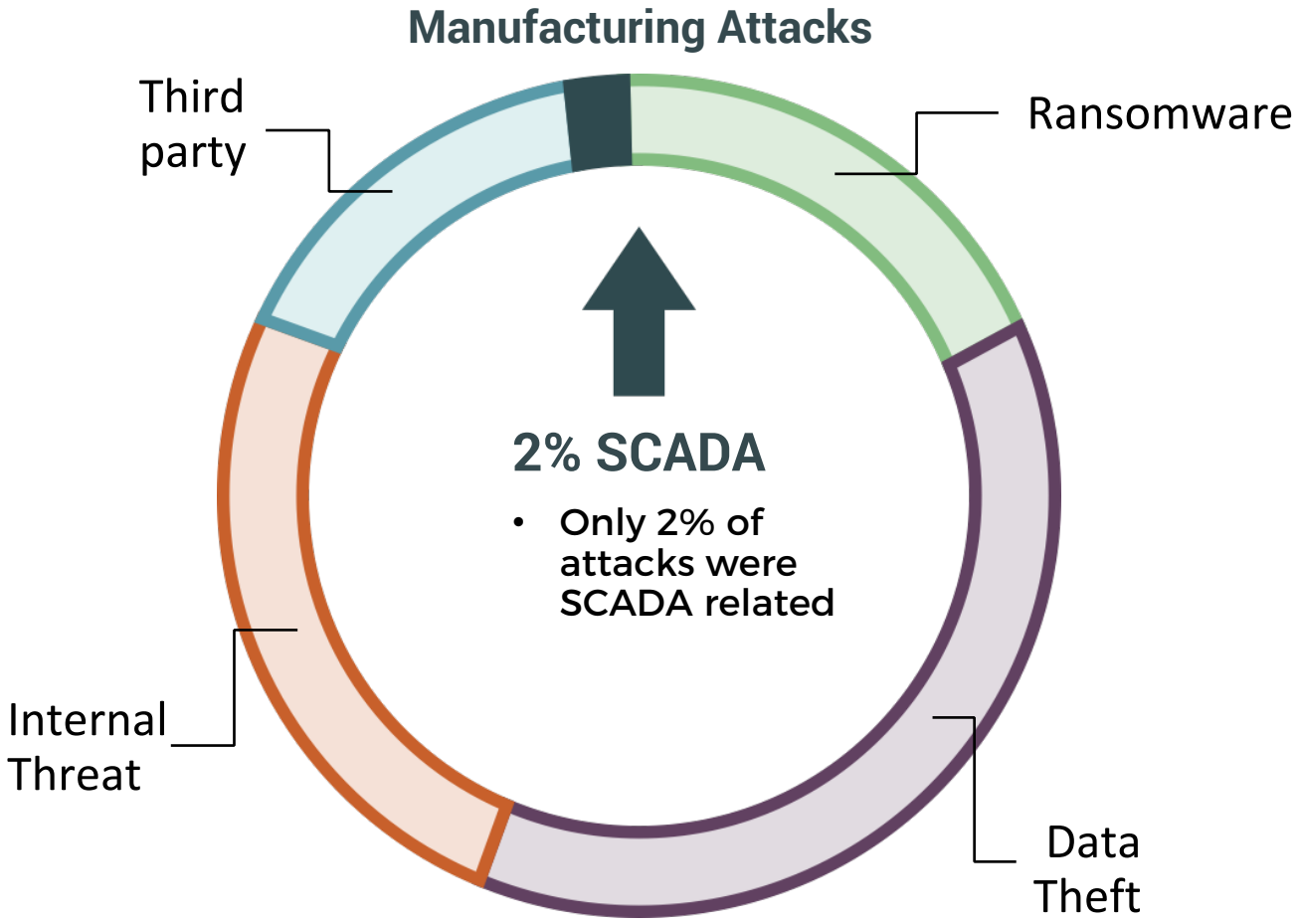
Collaboration Challenges

- Uneven security focus within OT teams
- Minimal OT expertise within security/networking teams
- Separate security strategies

Vulnerabilities & Risks

- Devices with outdated operating systems
- Devices behaving anomalously
- Devices with default credentials

Reality of Manufacturing Risk



"Ransomware, destructive malware, insider threats, and even honest mistakes present an ongoing threat to an organization's infrastructure."

– NCCoE at NIST

* Statistics compiled from IBM X-force 2020 Threat Intelligence Index, and Dragos Manufacturing Sector Threat perspective 2020

Real Threats and Real Headlines

Colonial Pipeline Attack Showed Securing IT/ IoT As Important As OT

- Saturday May 8, 2021 – Reports of Colonial Pipeline ransomware event began appearing
- Colonial and Government reporting – only IT systems and network impacted, Pipeline shutdown was precautionary
- Double extortion – Nearly 100GB of data ex-filtrated prior to ransomware attack, threat of public data release

What's Needed?

Enable teams to work with "Eyes Wide Open"

Unified view of entire attack surface

Integrated toolset to provide common language & frame of reference

Drive collaboration between IT Security, Network, Operational Technology groups

Ensure understanding of conflicting–and complementary–priorities

"…Historical IT and OT functional differences are becoming a liability when security is involved."

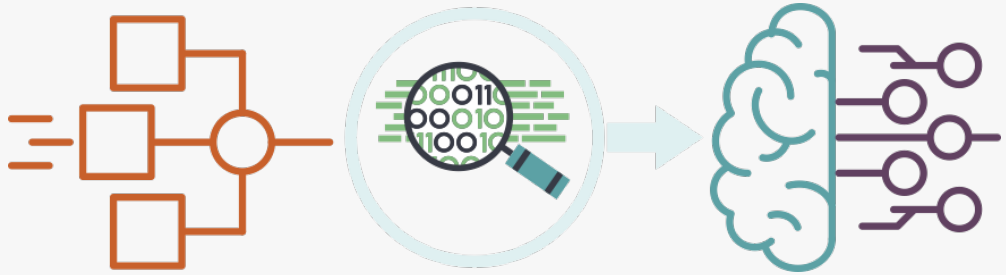
"By 2025, 75% of OT security solutions will be delivered via multifunction platforms interoperable with IT security solutions."

Gartner Market Guide for OT Security
Jan 2021

Two Options for Visibility Across Silos

Send networking, security, OT data into SIEM or equivalent

- Can already do this today
- Siloed data with custom details for some

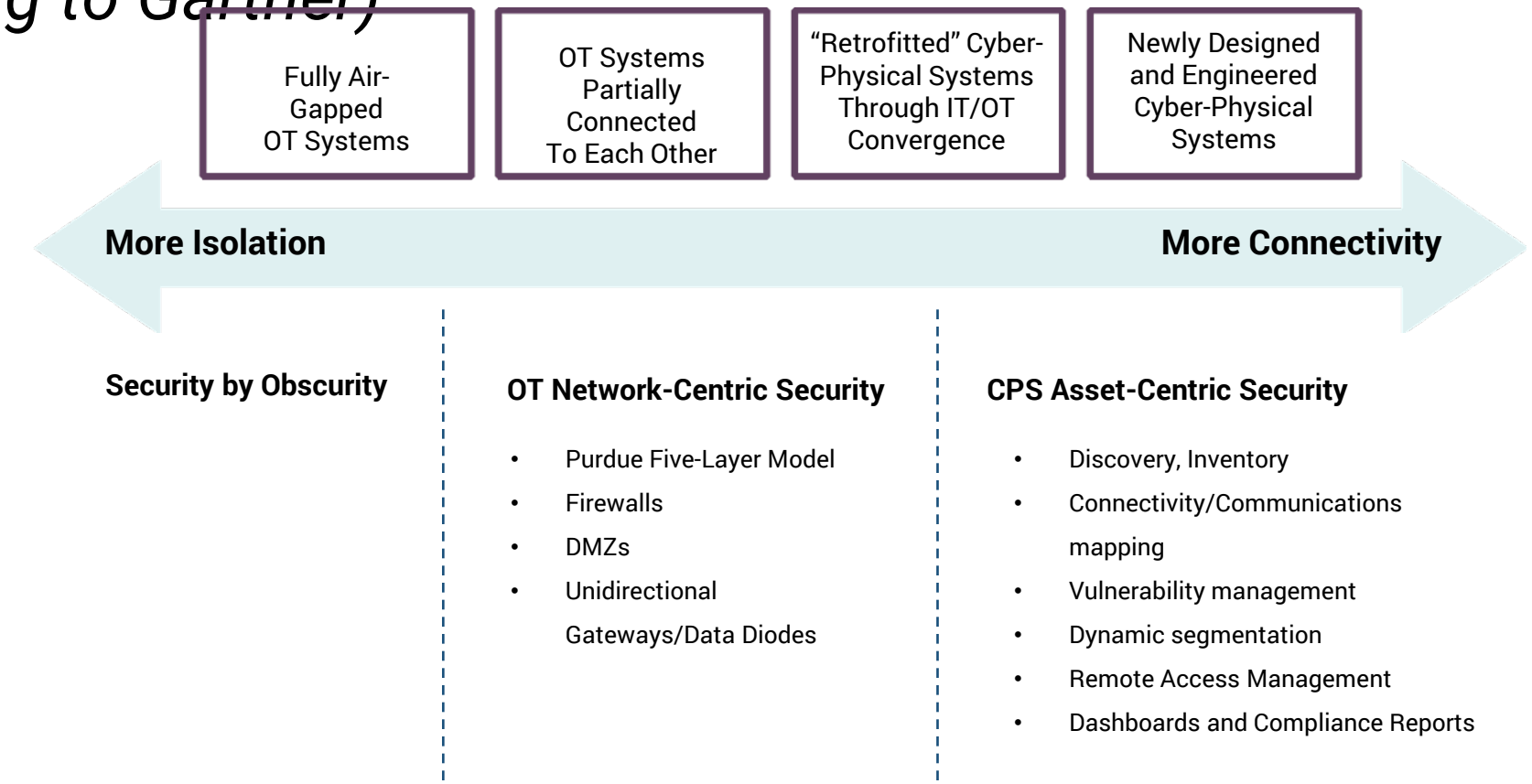


Connected device security platform retrieves and consolidates insights from across the network

- Common multifunction platform for IT Security, Network, & OT
- Device context enriches other networking and security systems: Firewall, NAC, CMDB, SIEM, Vulnerability Management, etc.

Journey Towards Convergence & Asset Centric Security

(According to Gartner)



Gartner

Key Considerations

Discovery, inventory

Needs to be agentless so that there is no impact to business operations

Connectivity & mapping

Physical and network location, as well as communications patterns can identify:

- Location of compromised devices
- Devices communicating to malicious domains
- Internet Telnet/desktop apps
- Validate segmentation

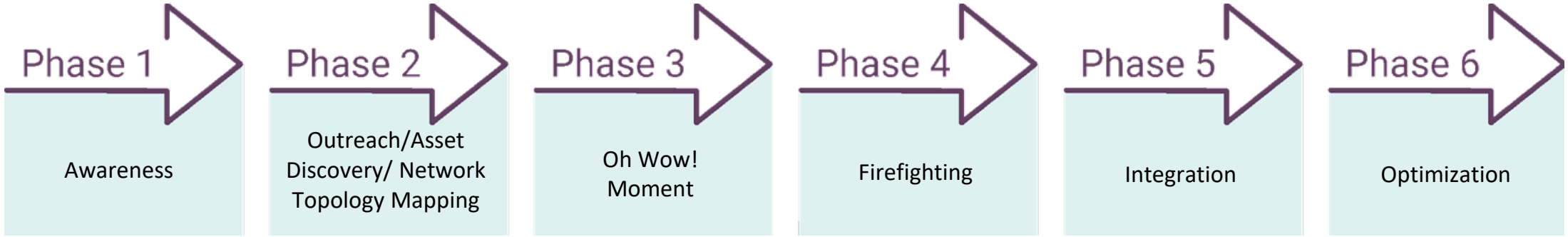
Vulnerability management

Cannot actively scan OT devices
Updates may not be available for devices with outdated operating systems; need segmentation

Dynamic segmentation

Segmentation based on cyber risks and business impact

Organizational Alignment To Secure Converged IT/OT



Phase 1: Get buy-in from the various stakeholders, including the C-suite

- Determine the role teams should play
- Define strategy and key security framework (NIST/Zero Trust/CMMC)

Phase 2: Deploy Connected Device Security Solution with buy in from teams. Start with real-time asset inventory, map device communications

Phase 3 and 4: Mitigate risks

- Manage and patch vulnerabilities.
- Zero Trust segmentation for OT devices with outdated operating systems
- Monitor East-West traffic and anomalous behavior
- Automated policies during incident

Phase 5: Integrate with existing networking and security solutions

Phase 6: Info sharing & collaboration across teams

Ordr Customer Case Study

Global Auto Parts Manufacturer

- **Objective: Discover devices and malware on corporate network and shop floor**
- **Process: On-site competitive evaluation**
  - Vendor A: Primarily reporting, with limited in-depth device information
  - Vendor B: OT centric strength but incomplete features for IoT and IT devices in “carpeted space”
  - Vendor C: Legacy technology with very high TCO and limited device visibility
  - Ordr: Ideal combination of visibility and network context across IT, IoT, and OT devices
- **Current status:**
  - Deployed in 6 locations worldwide, with additional sites in process
  - Uses Ordr Flow Genome to map flows
  - Use integrated IDS and machine learning to identify malware and behavioral anomalies
  - Plans to implement micro-segmentation via firewall and switch integration, using existing infrastructure

Take-Aways For Securing IT + OT as Networks Converge

- Drive executive *and* cross-functional buy-in and understanding
- Rethink siloed approaches in favor of integrated frameworks
- Invest in *unified* tools for visibility across IT, OT, IoT, and networks
- Commit to moving beyond firefighting to proactive Zero Trust / Least Privilege approaches

12TH ANNUAL LEADERSHIP EVENT

CYBER SECURITY SUMMIT

Security solutions through collaboration.™

ōrdr

Thank You

Bryan Gillson, bgillson@ordr.net
Ordr, Inc.
Visit us at Booth 203