DRAGOS

Building Defensible Architectures for Critical Infrastructure

Dr. Jacob Benjamin

Director of Professional Services

Oct 30, 2023

Cybersecurity and Artificial Intelligence Research Symposium (CARS)

FIVE CRITICAL CONTROLS

01
ICS Incident Response

02
Defensible Architecture

03
ICS Network Visibility and Monitoring

04
Secure Remote Access

05
Risk Based Vulnerability Management

02 A DEFENSIBLE ARCHITECTURE

The resources and technical skills required to adapt to new vulnerabilities and threats should not be underestimated.

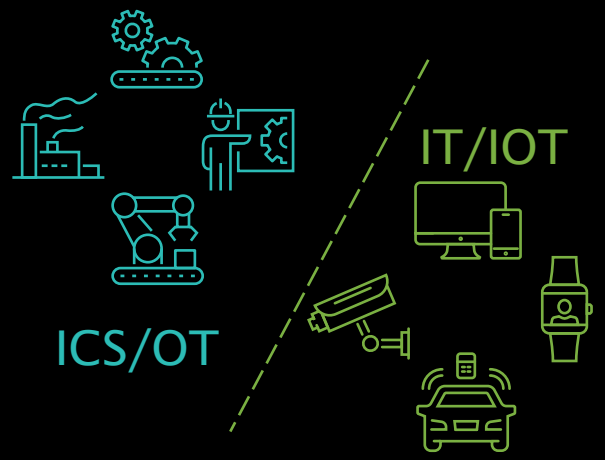
Removing extraneous OT network access points

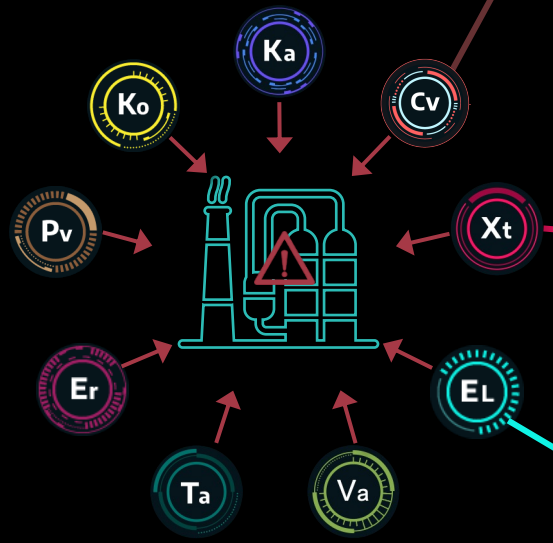
Mitigating high risk vulnerabilities

Maintaining strong policy control at IT/OT interface points

The people and processes to maintain it

ICS/OT CYBER SECURITY ISSUES





CHERNOVITE
SINCE 2021

ADVERSARY:
+ Unique Tool Development

CAPABILITIES:
+ Uses ICS-specific protocols for reconnaissance, manipulation, and disabling of PLCs
+ PLC credential capture, bruteforcing, and denial of service

VICTIM:
+ Oil & Gas, Electric Utilities, and other industries may be targeted
+ Asset owners with Schneider Electric, Omron PLCs, CoDeSyS-based PLCs, as well as any OPC UA operations

INFRASTRUCTURE:
+ Uses victim PLCs, engineering workstations, and PLC control software for lateral movement and manipulation

ICS IMPACT:
+ Loss of safety, availability, and control; manipulation of control
+ ICS Kill Chain Stage 2 - Install/Modify; Execute ICS Attack

ENOTIME
SINCE 2014

VICTIM:
+ Oil & Gas, Electric Utilities
+ Middle East, North America

INFRASTRUCTURE:
+ Virtual Private Server and compromised, legitimate infrastructure
+ European web hosting providers
+ Asian shipping company

execute disruptive ICS
SIS incident

ELECTRUM
SINCE 2016

ADVERSARY:
+ Assessed links with SANDWORM APT, now appears indepedendent

CAPABILITIES:
+ Unique RAT & malicious wiper modules

VICTIM:
+ Electric Sector
+ Ukraine, Europe

INFRASTRUCTURE:
+ Leveraged servers hosting many additional services such as TOR

ICS IMPACT:
+ Executed control system portion of 2016 Ukraine power event, deployed CRASHOVERRIDE designed to manipulate electric transmission equipment

ICS/OT Systems, Networks, & Vulnerabilities are Very Different from IT/IOT

Specialized Threat Groups Target ICS/OT Systems With TT Specific to the Environments

Be Significant Impacts afety, Environment, & Revenue

ICS/OT SECURITY INVESTMENTS SIGNIFICAN RITY

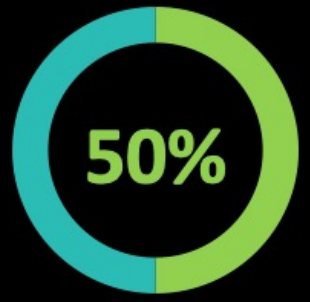
DRAGOS

DEFENSIBLE ARCHITECTURE

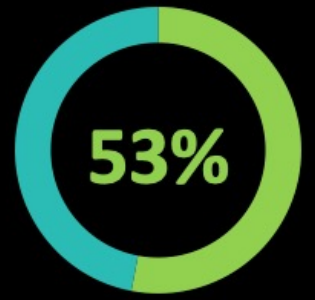
It is the human element that allows a defensible architecture to become a defended architecture.

Defensible Architecture Criteria
Full Visibility
Hardened Assets
Flows Enforced
Rapidly Isolated
Defended

Limited OT Visibility



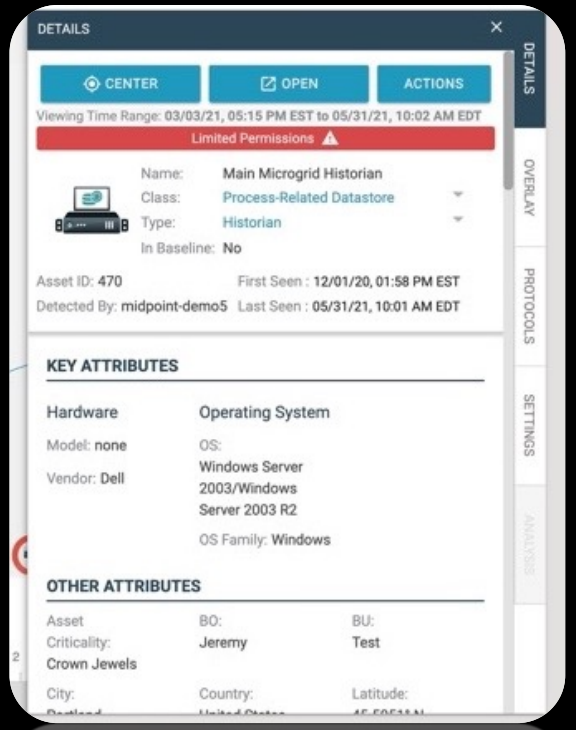
Poor Segmentation



External Connectivity to OT

ASSET VISIBILITY

A comprehensive inventory is essential for any monitoring, threat correlation and effective vulnerability management



Build asset inventory depth through “operations safe” passive collection and device level detail

- Establish asset profile baselines for connected integrations with firewall and CMDB systems
- Group assets in a visual map with customizable zones for easier cyber-ops management
- See historical changes with timeline views to spot unexpected activity

ICS PROTOCOL & TRAFFIC ANALYSIS

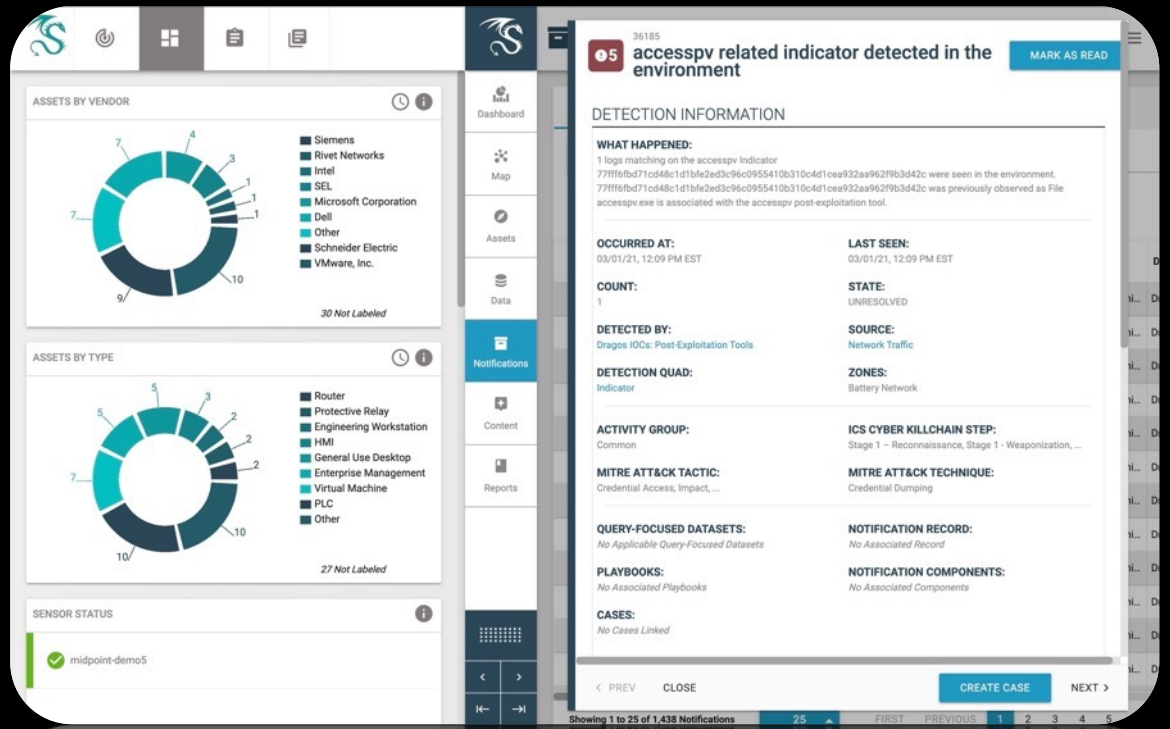
Proper traffic dissection and inspection requires in depth protocol coverage – assets and threats remain hidden until their communications are exposed

Improve the accuracy and understanding of devices in your environment

- Full support across most industrial vendors, equipment, and protocols
- Capture, analyze, and investigate device communications
- Monitor for remote connections, search historical activity

THREAT DETECTION

Adversaries evolve their Tactics, Techniques, and Procedures (TTPs) with subtle behaviors lost in the noise without AI (Actual Intelligence) – creating alert fatigue

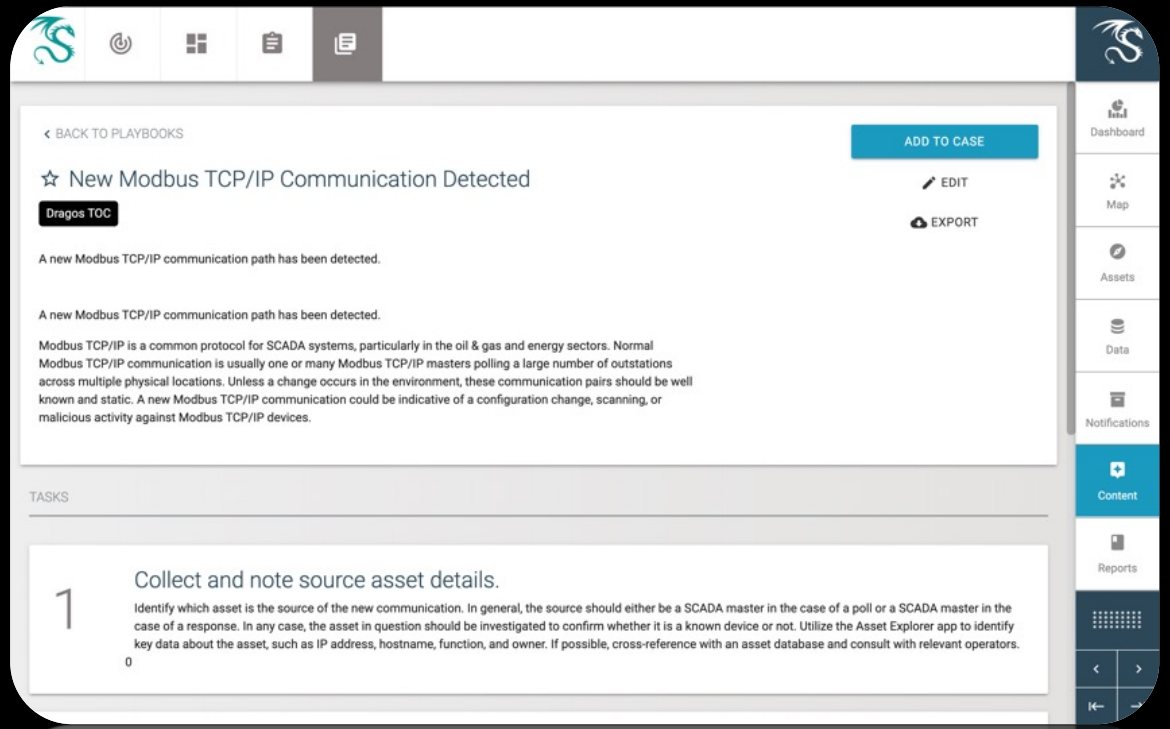


High signal, low noise intelligence-based detections mapped against MITRE ATT&CK for ICS :

- Curated Indicators of Compromise (IOCs), malicious IPs, domains, and hashes from Dragos Intelligence
- Anomalous traffic patterns and baseline deviation alerts
- Composite detections from TTP analysis of threat groups and attacks

ACCELERATED RESPONSE

When faced with a potential incident, clear and carefully vetted guidance can mean the difference between quickly restoring operations or making the situation worse

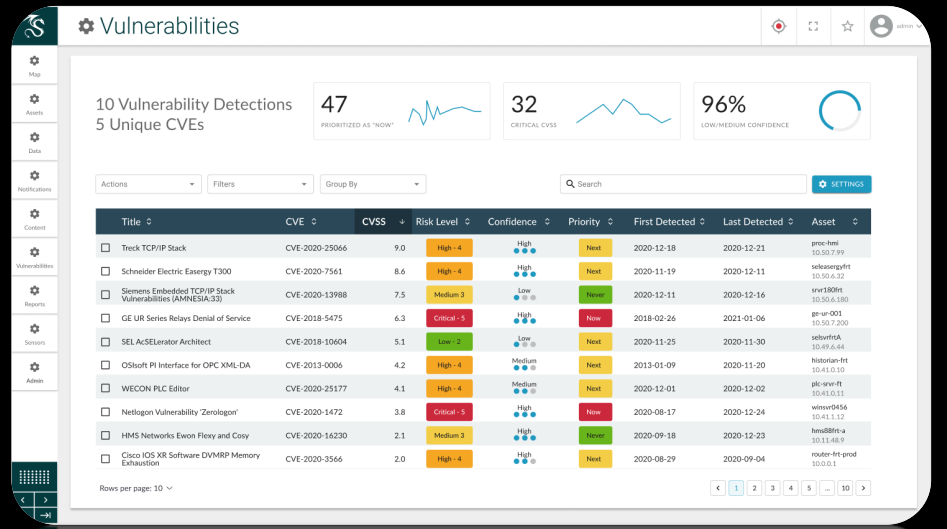


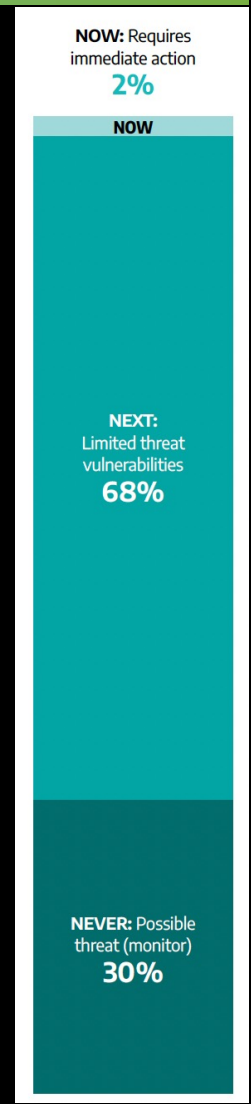
Provide responders with the tools to triage and investigate potential incidents

- Incident response playbooks with OT-centric guidance from industry experts
- Collect evidence and organize by case in the analyst investigation workbench
- Centralized forensics and timeline views to coordinate across OT and IT teams

VULNERABILITY MANAGEMENT

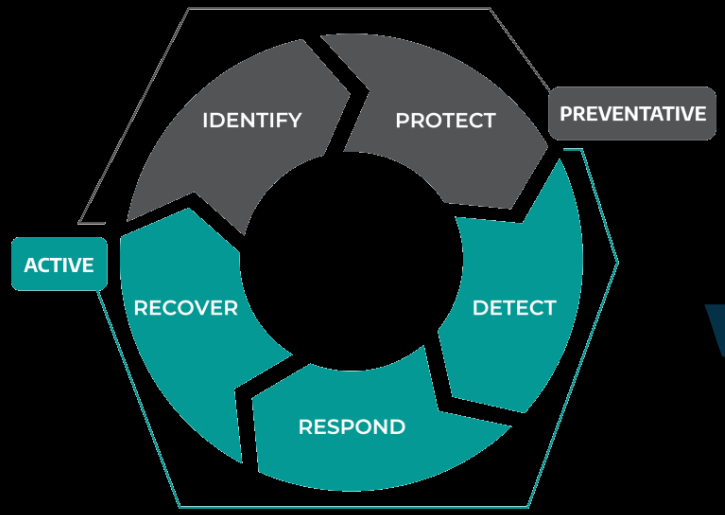
- Visibility enables risk-based approach
- Possible Vulnerability Actions
  - Immediate Action
  - Limited Action
  - Possible Threat
  - No Action
  - Hype

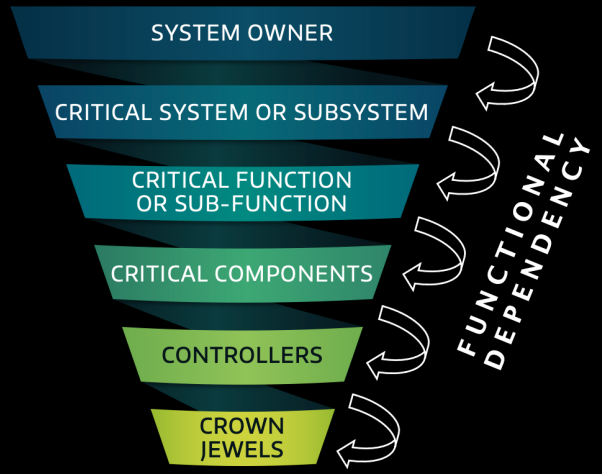


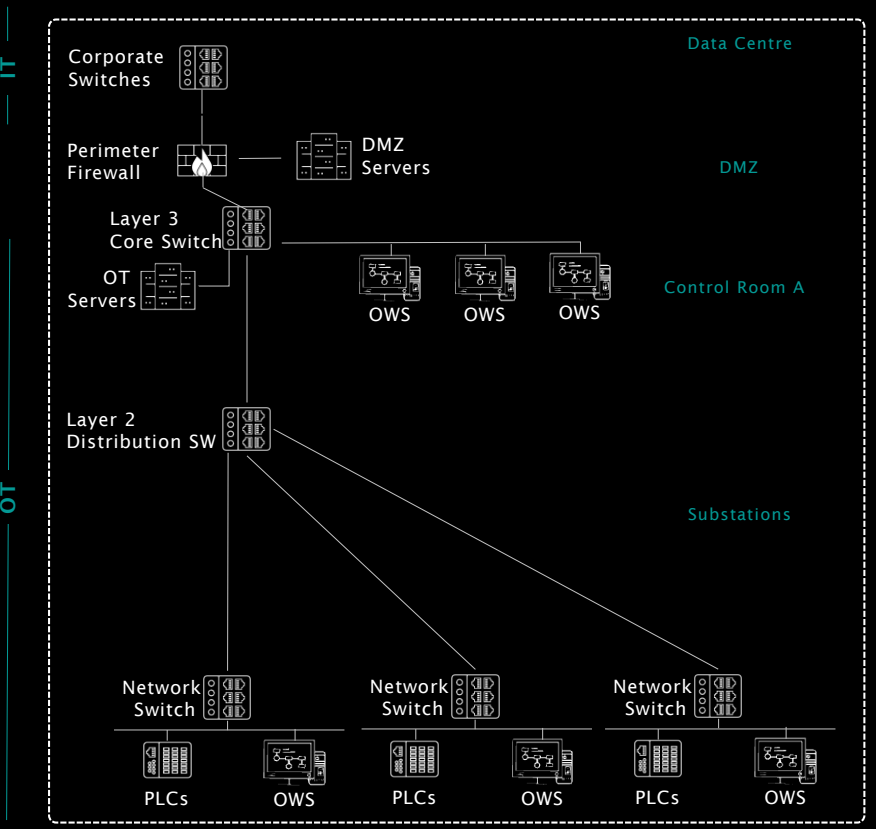


SEGMENTATION AND FLOW ENFORCEMENT

A harsh truth is that prevention is ideal, but not guaranteed. Preventative countermeasures atrophy over time.





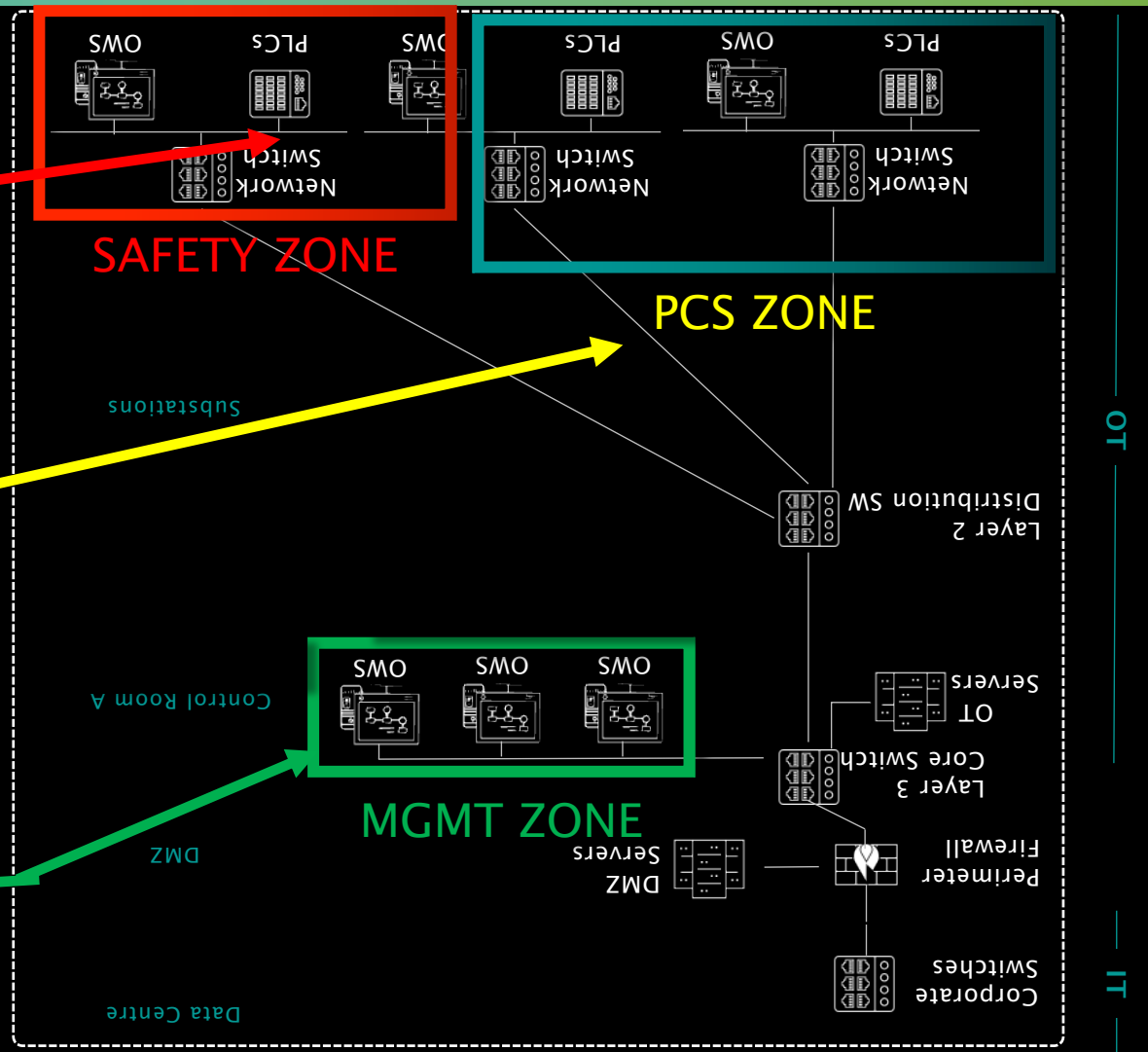


ZONE DEFENSE

Safety Conduit

PCS Conduit

MGMT Conduit



COLLAPSIBLE INFRASTRUCTURE

Allows for rapid isolation and the ability to go into a defensive cyber position during heightened situations such as DBT scenarios and incident response plans.

Cyber Load Shed

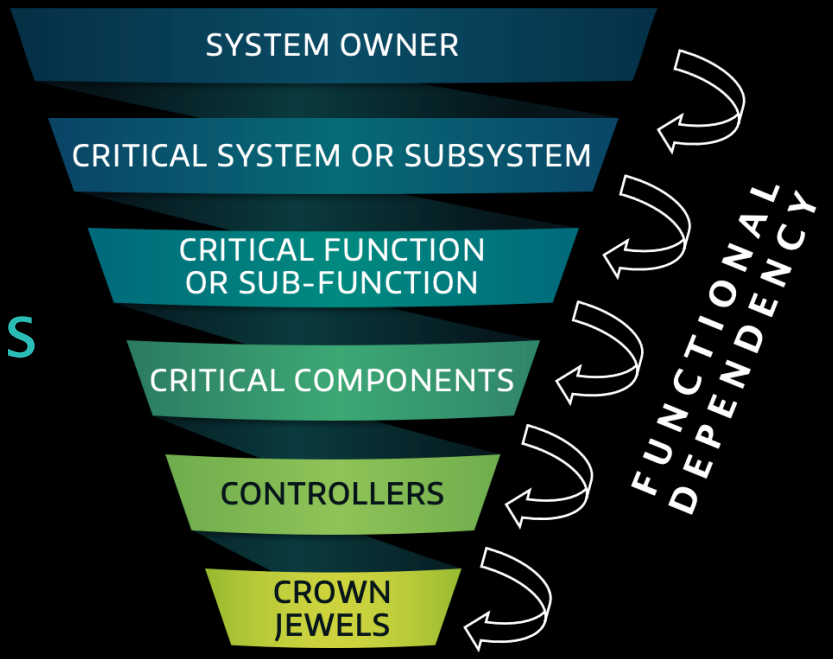
- Cut all non-local connections
- Quickly apply new firewall rules
- Rely on analog means for safety decisions or critical operations

FROM DEFENSIBLE TO DEFENDED

Trained personnel, possessing proficient understanding of the industrial process and its cyber dependencies.

Document & Set Alerts

1. Normal range of set points
2. Communication protocols
3. Sources of approved logic changes



COLLECTION MANAGEMENT FRAMEWORK

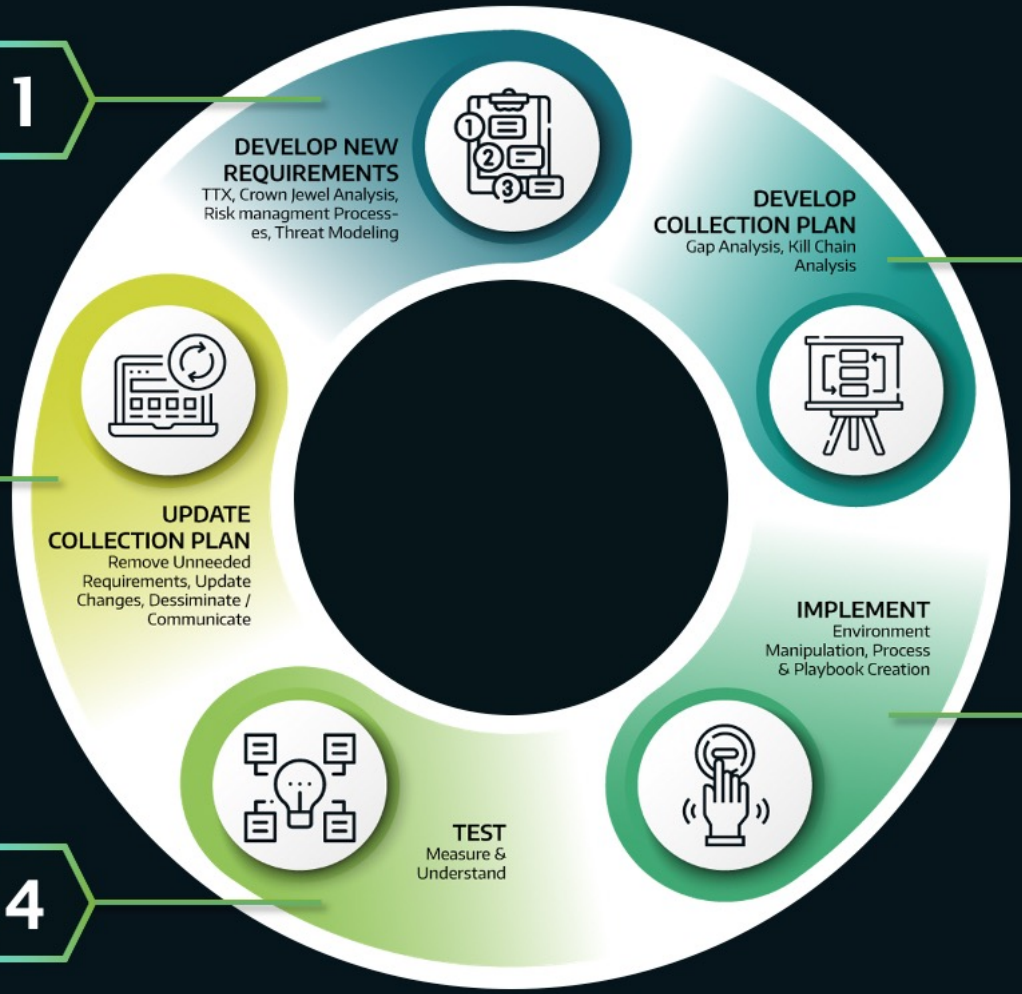
1. Develop requirements that reflect an understanding of business risks.

2. Develop a collection plan using available data sources internal to the enterprise.

3. Implement the collection plan with a focus on the creation of new procedures and identification of new data sources.

4. Test and understand the implications of the collection plan to ensure its effectiveness.

5. Update the collection plan and make adjustments for requirements and collection sources that are no longer relevant.



EXAMPLE CMF DELIVERABLE

Segment / Level	Asset	Data Type	Kill Chain Phases	Data Storage Location	Data Retention	Follow-On Collection
Corporate Network	Edge Firewall/VPN Concentrator	Firewall Logs	Reconnaissance, Command and Control, Delivery	IT SIEM	12 months	Local Firewall Logs, Firewall Config/Rules
Corporate Network	Engineer Laptops	Windows Event Logs, EDR logs	Exploitation, Installation, Actions on Objectives	IT SIEM	12 months	Registry, Memory, Master File Table (MFT)
Corporate Network	Switches	Syslog	Reconnaissance, Command and Control	IT SIEM	12 months	Configuration and Access logs
Network Core	Routers	Syslog	Reconnaissance, Command and Control	IT SIEM	12 months	Configuration and Access logs
Multiple Segments	Firewall	Firewall Logs	Reconnaissance, Command and Control, Delivery	IT SIEM	12 months	Dragos Platform, Firewall Ruleset
DMZ	Jump Host Server	Windows Event Logs	Reconnaissance, Command and Control, Delivery	OT Log Collector (E.g. Dragos Platform) or Local	12 months	Registry, Memory, MFT
Process Network	Cytiva VIA Thaw	Cloud Logs	Installation, Actions, on Objectives	OT Log Collector (E.g. Dragos Platform) or Local	12 months	Chronicle
Process Network	SKAN Isolator (PLC)	Internal Logging	Installation, Actions, on Objectives	OT Log Collector (E.g. Dragos Platform) or Local	12 months	Controller Logic / Config
Process Network	SKAN Isolator (HMI)	Windows Event Logs	Installation, Exploitation, Actions, on Objectives	OT Log Collector (E.g. Dragos Platform) or Local	12 months	Registry, Memory, MFT
Process Network	EEMS PLCs	Syslog, rsyslog, Internal Logging	Installation, Actions, on Objectives	OT Log Collector (E.g. Dragos Platform) or Local	12 months	Controller Logic / Config

FIVE CRITICAL CONTROLS - REVISITED

ICS
CYBERSECURITY
CRITICAL
CONTROLS

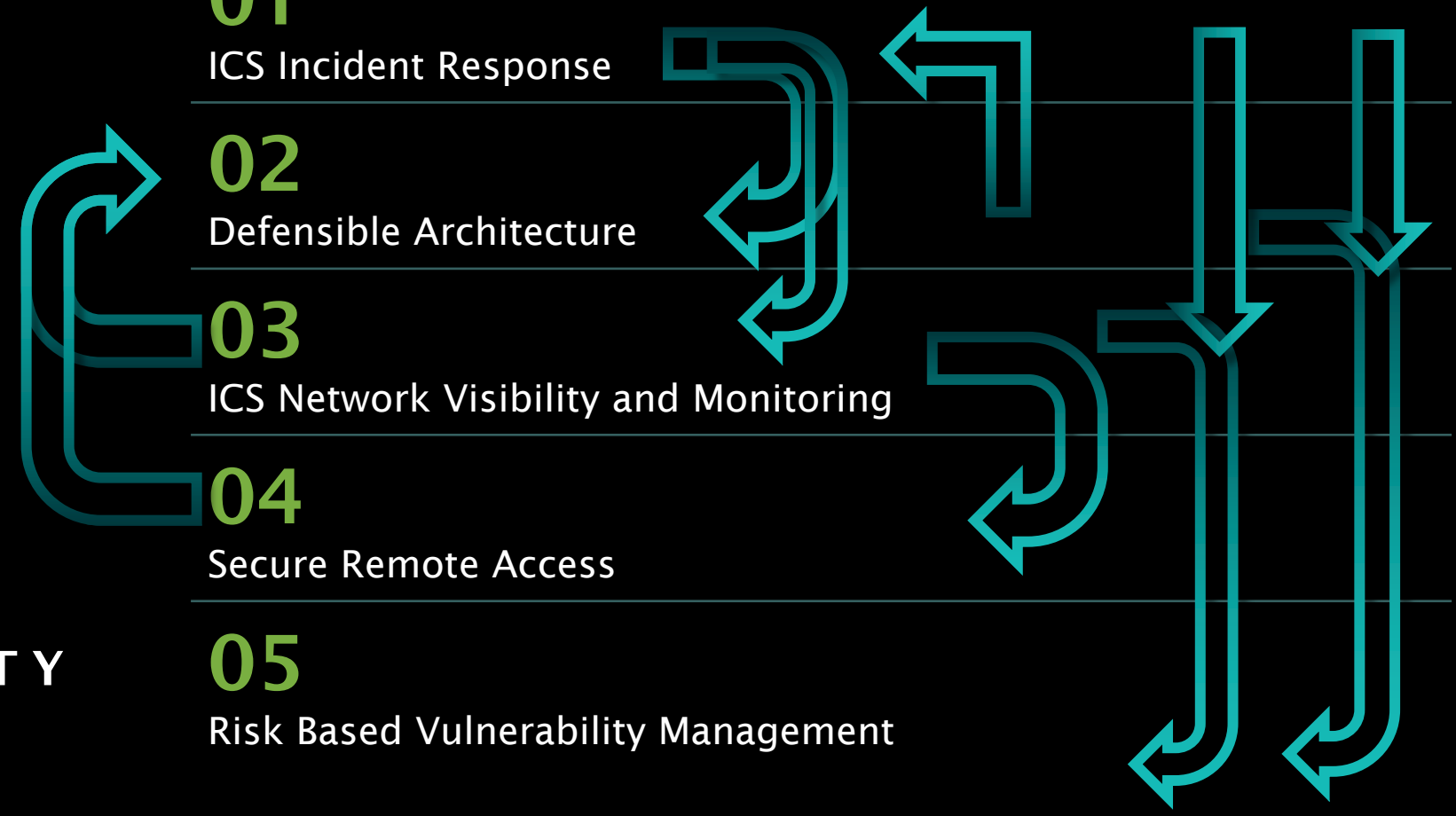
01
ICS Incident Response

02
Defensible Architecture

03
ICS Network Visibility and Monitoring

04
Secure Remote Access

05
Risk Based Vulnerability Management



CONCLUSION

Defenders must assume the architecture will never fully be secure instead focus on building a defensible architecture.

- Prevents as much cyber risk as possible
- Facilitates the human defender
  - Full Visibility
  - Hardened Assets
  - Segmented
  - Flows Enforced
  - Collapsible
  - Understood

FUTURE RESEARCH & OPEN CHALLENGES

The industry has been working to assess adversary capabilities through a keyhole rather than a deeper collection and broader field of vision

- Machine-speed threat intelligence sharing
- Classifying process anomaly vs cyber attack
- OT Incident response collection tools
- Risk Reduction of OT Zero Trust Capabilities

FURTHER READING

- SANS Institute: The Five ICS Critical Controls Whitepaper
- Dragos 2022 Year In Review Report
- Dragos: Implementing a Defensible Architecture Whitepaper
- Dragos: Recommendations to Implement Secure Remote Access (SRA) Today
- Dragos: Bridging the IT / OT Gap for Effective Incident Response Whitepaper

QUESTIONS AND ANSWERS