



## Emerging ICS Cyber Threats

Dr. Jacob Benjamin  
Director of Professional Services  
Dragos, Inc.  
@DrNuclearCyber




# Threat Groups

# Known Threat Groups Targeting Nuclear

## 2 Threat Groups:

- WASSANITE
- DYMALLOY



**WASSONITE**  
SINCE 2018

**ADVERSARY:**

- + Some similarity to COVELLITE
- + Links to Lazarus activity

**CAPABILITIES:**

- + DTrack RAT, Mimikatz, system tools for lateral movement & file transfer

**VICTIM:**



- + Electric, Nuclear, Manufacturing
- + India, South Korea, Japan

**INFRASTRUCTURE:**

- + Adversary-registered and controlled domains & infrastructure for C2
- + Use of compromised, legitimate services in some instances

**ICS IMPACT:**

- + Operations focus on ICS-related organizations, limited to IT network actions for initial access and information collection



**DYMALLOY**  
SINCE 2016

**ADVERSARY:**

- + Some indications of relationship to Dragonfly

**CAPABILITIES:**

- + Commodity malware tools GOODOR, DORSHEL, KARAGANY, Mimikatz
- + Spearphishing & watering hole attacks

**VICTIM:**


- + Energy sector; Oil & Gas, Transportation
- + Turkey, Europe, US

**INFRASTRUCTURE:**

- + Compromised ISP service nodes
- + No domains observed; IP only used for C2, infection

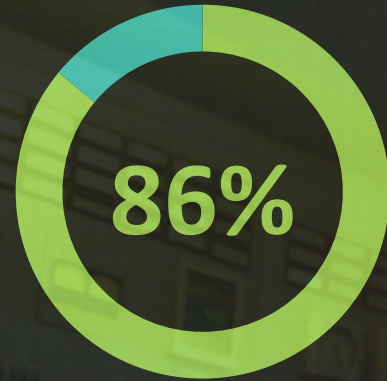
**ICS IMPACT:**

- + Intelligence gathering

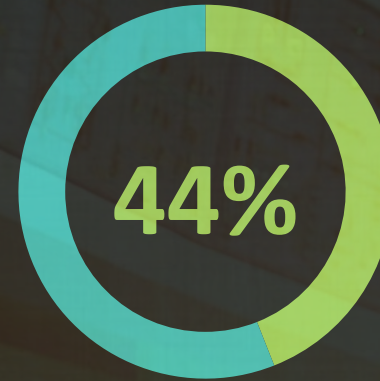




# Key 2021 Findings from the Frontlines



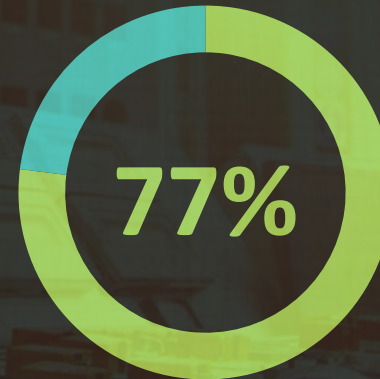
Limited OT Visibility



Shared IT/OT Credentials



External Connectivity to OT



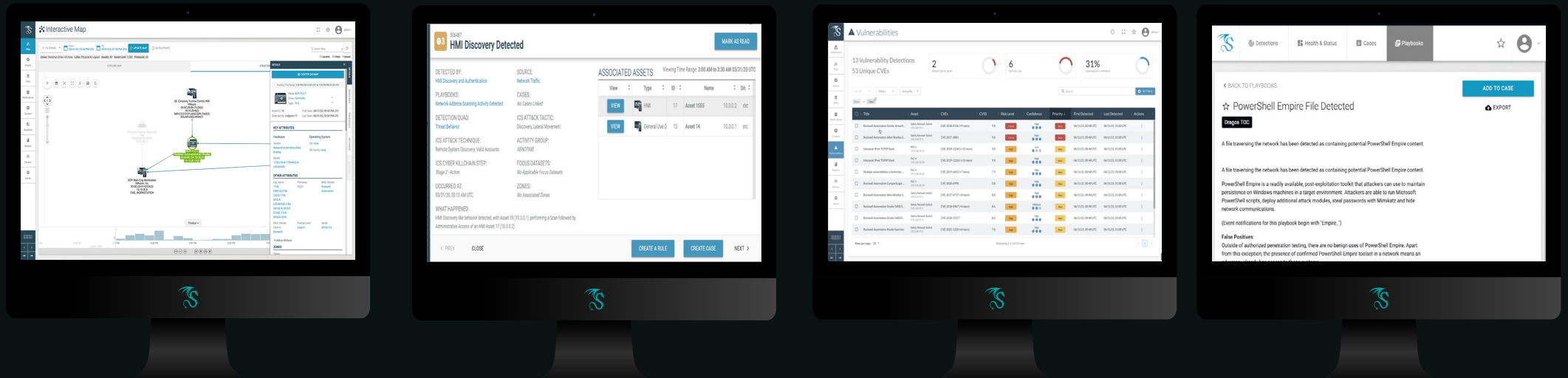
Poor Segmentation

# Visibility & Data Diodes

# The Case for Visibility

## Why is visibility needed when I have a data diode?

- Continuous validation of segmentation
- Threat detection from other attack vectors
- Better understanding of critical assets and operations
- Bolster Incident Response







# THANK YOU

jbenjamin@dragos.com  
info@dragos.com