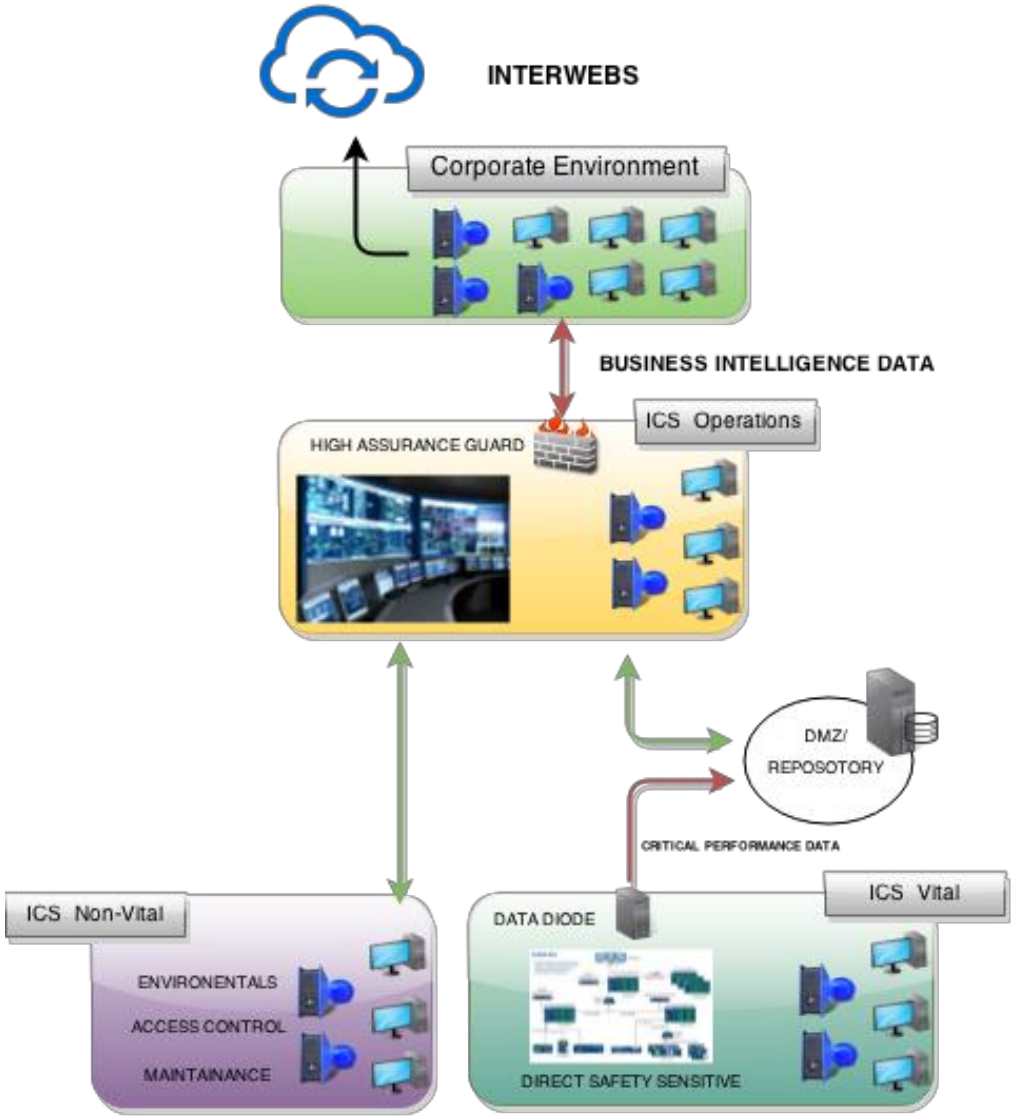

10TH ANNUAL
ICS SECURITY
SUMMIT & TRAINING
Emerging Solutions for Evolving Threats
Moderator:
Derek Harp, ICS Security, SANS Institute
Panelists:
Eric Cornelius, Director of Critical Infrastructure & ICS, Cylance
Adam Meyer, Chief Security Strategist, SurfWatch Labs
Graham Speake, Chief Product Architect, NexDefense
Doug Wylie, Director – Industrial Security Program,
Rockwell Automation

# Adam’s Data Diode Project



# Evolving Landscape

## Themes of a contemporary world

- Interconnected, networked digital devices
- Complex systems needing unfettered access to data
- Security risks and new threat-actors are very real
- Security breaches are becoming the ‘norm’

## Themes of Industrial Control Systems (ICS)

- Systems are growingly complex and interconnected
- ICS ‘Data’ spans both information and control
- Targeted attacks against Control Systems are a reality

## Consistent Concerns and Desires

- Design and maintain a system resilient to attacks
- Comply with emerging standards and legislation
- Protect what is important…

# What are some particularly weak solution areas today?

- Asset discovery
  - Owner/operators do not know what is on their network
  - What communicates with what
  - What protocols are used
- Anomaly detection
  - Is this a new, approved node/communication
- Cross IT/OT solutions

SOPHIA
FINGERPRINTING TOOL

# What will it actually take for end users to adopt these

- Regulation
  - But will never keep up with the bad guys
- Risk insurance
- Documented incidents
- Education
  - Especially decision makers