# Cyber Informed Engineering for Critical Infrastructure

In an era where critical infrastructure faces unprecedented cyber cyber threats, Cyber Informed Engineering (CIE) emerges as a pivotal a pivotal strategy to safeguard essential services. This presentation presentation will explore the significance of CIE and how it can be can be integrated into infrastructure design to enhance cybersecurity. cybersecurity.

AC

**Presenter: Aaron Crow**

www.linkedin.com/in/aaronccrow

# Aaron Crow, CISSP

- **Current Role:**
  - Senior Director for Operational Technology (OT) Security (Morgan Franklin Cyber)
  - Host of PrOTect IT All Podcast
- **Experience:** Over 25 years in IT and cybersecurity, with more than 15 years focused on critical infrastructure and power utilities
- **Previous Positions:**
  - Chief Technology Officer at Industrial Defender
  - Senior Director for Operational Technology (OT) Security at MorganFranklin Consulting
  - Managed OT cybersecurity for over 40 power generation sites at Luminant (Vistra)
- **Community Involvement:**
  - Host of the "PrOTect IT All" podcast, sharing insights on OT cybersecurity
  - Advisory role with Building Cyber Security and involvement with ICS Village, promoting cybersecurity awareness and education

Aaron's extensive background in cybersecurity, particularly in the OT sector, along with his leadership in both asset management and consulting, positions him as a key thought leader in the field

linkedin.com/in/aaronccrow

# Cyber Threats to Critical Infrastructure

1

## Malware Attacks

Sophisticated malware designed to infiltrate and disrupt critical systems, critical systems, causing widespread damage and disruption.

2

## Insider Threats

Malicious actors with insider knowledge exploiting vulnerabilities from within the organization.

3

## Supply Chain Vulnerabilities

Weaknesses in the supply chain that can be leveraged to gain access to critical infrastructure.

4

## Denial-of-Service Attacks

Coordinated efforts to overwhelm and paralyze critical systems, denying access to essential services.

# Cyber Informed Engineering (CIE) Overview

## Definition

CIE is a holistic approach that integrates cybersecurity considerations into the design, construction, and operation of critical infrastructure.

## Objectives

CIE aims to enhance the resilience and security of critical systems, reducing the impact of cyber threats and ensuring the continuity of essential services.

## Interdisciplinary Approach

CIE requires collaboration between engineers, cybersecurity experts, and domain specialists to address the complex challenges of critical infrastructure protection.

# CIE Principles and Strategies

1

## Risk Assessment

Thorough evaluation of potential cyber threats and impact on critical infrastructure components.

2

## Secure Design

Incorporating robust security measures, such as access controls, encryption, and redundancy, into the design of critical systems.

3

## Continuous Monitoring

Implementing real-time monitoring and anomaly detection to promptly identify and respond to cyber incidents.

4

## Understand Consequences

Understand the consequences and impact when conducting Risk assessment in preparation for Secure Design

# Integrating CIE into Infrastructure Design

## System Architecture

Designing critical infrastructure with security-focused system architectures, such as segmentation, redundancy, and failover mechanisms.

## Component Selection

Carefully evaluating and selecting hardware and software components that meet rigorous security standards and can withstand cyber threats.

## Secure Communication

Implementing secure communication protocols and encryption techniques to protect data exchange between critical infrastructure components.

## Operational Processes

Developing robust operational processes and procedures to ensure the continuous monitoring, maintenance, and incident response for critical infrastructure.

# Case Studies: CIE in Action

### Power Grid Resilience

Implementing CIE principles to harden the power grid against cyber threats, ensuring the reliable delivery of electricity.

### Water Infrastructure Security

Integrating CIE strategies into the design and operation of water treatment facilities to protect against contamination and disruption.

### Transportation Network Cybersecurity

Leveraging CIE to enhance the security of transportation systems, including traffic signals, rail networks, and airport operations.

### Safeguarding Healthcare

Applying CIE principles to secure critical healthcare infrastructure, such as medical devices and hospital systems.

# Challenges and Considerations

1

## Legacy Systems

Integrating CIE into existing critical infrastructure that may rely on outdated or legacy systems can pose significant challenges.

2

## Regulatory Compliance

Ensuring CIE-based designs and implementations adhere to evolving regulatory requirements and industry standards.

3

## Workforce Transformation

Upskilling and training the workforce to understand and apply CIE principles effectively is crucial for successful implementation.

# Conclusion and Q&A

## Key Takeaways

- CIE is a holistic approach to enhancing the cybersecurity of critical infrastructure
- CIE principles and strategies can be integrated into the design, construction, and operation of critical systems
- CIE-based solutions can improve the resilience and security of essential services
- Successful CIE implementation requires collaboration, workforce transformation, and addressing regulatory challenges

## Q&A