

# ENERGY SECTOR CYBER ATTACKS: FRONT LINES



Presented by Chris Sistrunk, Senior Consultant  
EnergySec Webinar – May 3, 2016



# Agenda

- M-Trends 2016 – What has Mandiant responded to?
- Threat landscape overview
- Attack readiness
- Case study
- Key takeaways/outlook

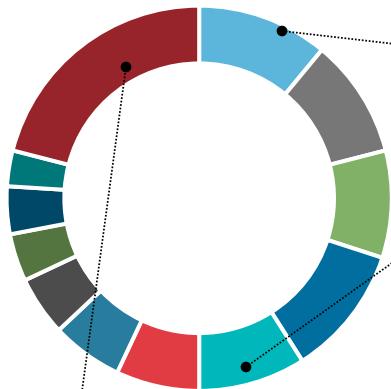
# BY THE NUMBERS M-TRENDS 2016

# Who's a Target?

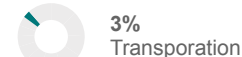
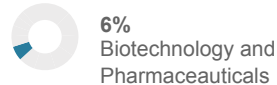
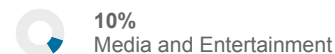
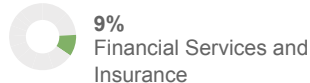
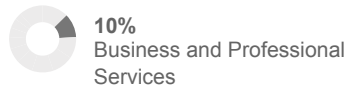
In 2015 we noted changes in the number of engagements at companies in several key industries:

↑ **High Tech** –up from 7% to 11%

↓ **Retail** –down from 14% to 9%



**Other:** Legal Services, Telecommunication, Government, Agriculture & Forestry, **Energy** 1%



# How Compromises Are Being Detected

47% Internal



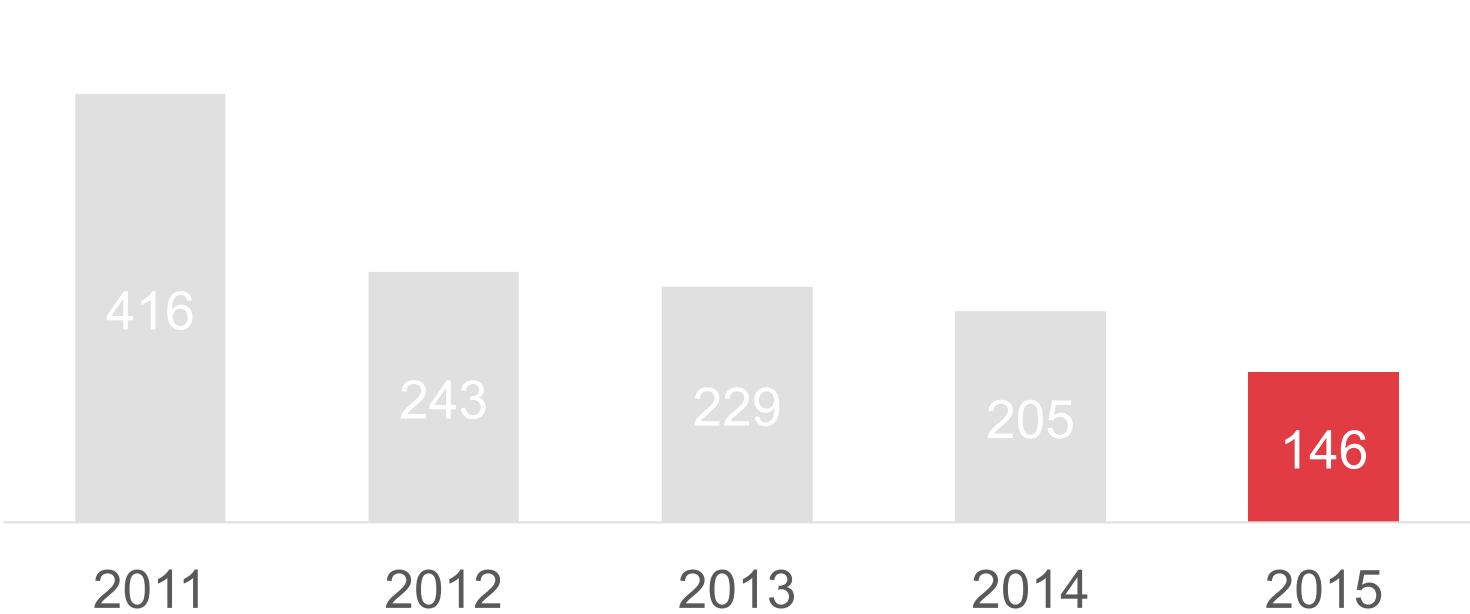
53% External

# Dwell Time

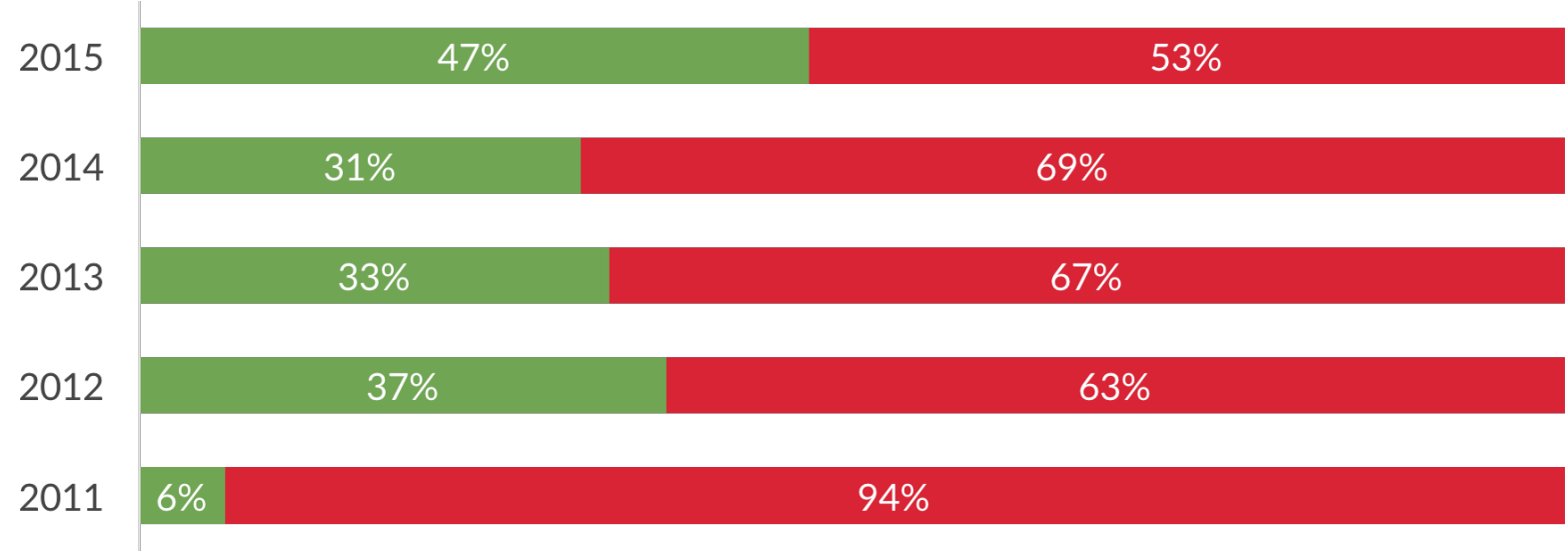
**146**  
**DAYS**

**59**  
**DAYS LESS THAN  
2014**

# Median Days Before Discovery



# Internal Detection Vs. External Notification



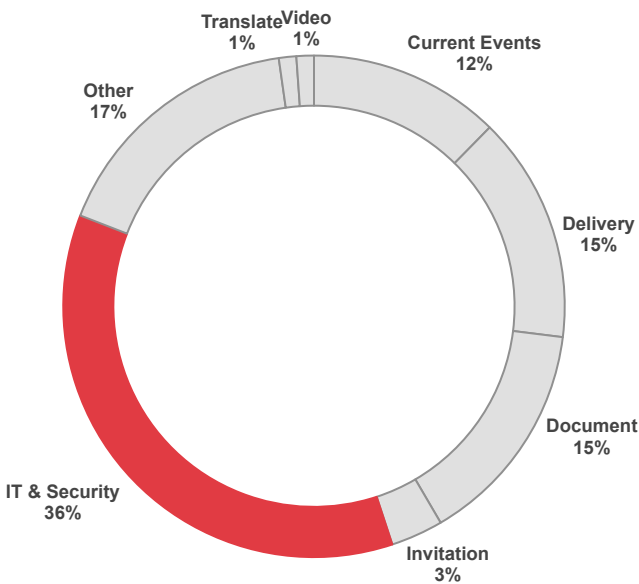


# APT Phishing

89% of Phishing Email sent on Weekdays













Majority of phishing emails were IT or security related, often attempting to impersonate the targeted company's IT Department or an anti-virus vendor



# THREAT LANDSCAPE

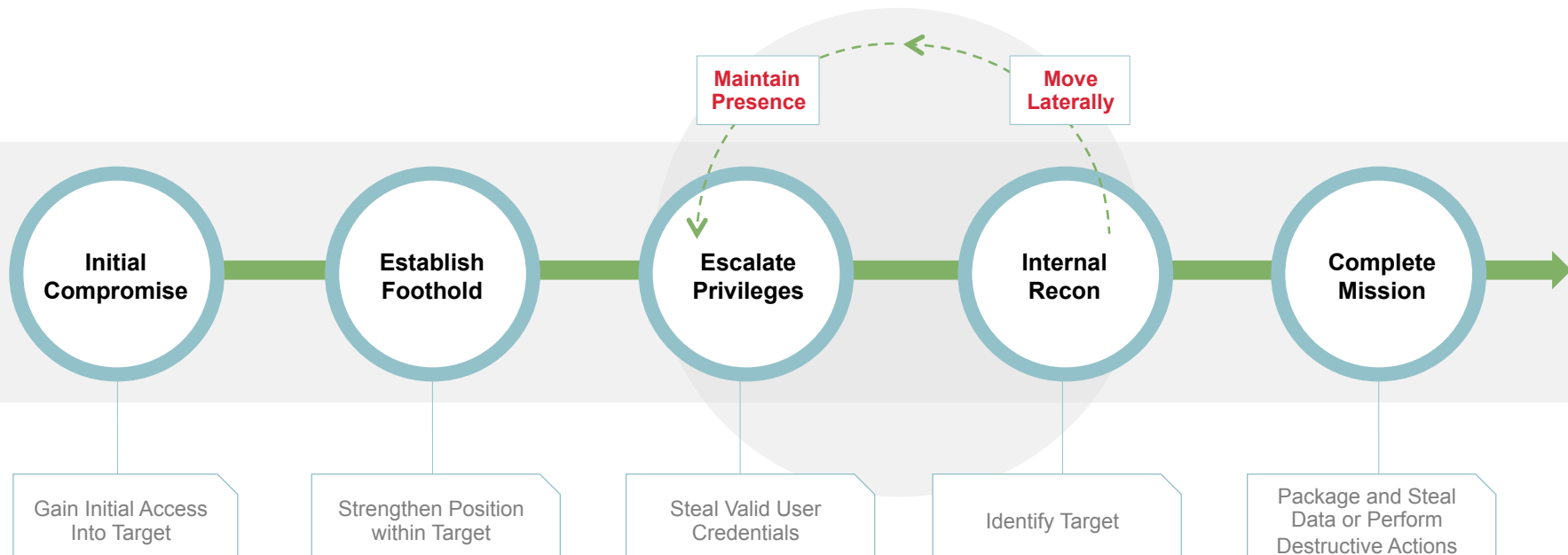
# Breaking Down the Threat

	Nuisance	Data Theft	Cyber Crime	Hacktivism	Network Attack
Objective	 Access & Propagation	 Economic, Political Advantage	 Financial Gain	 Defamation, Press & Policy	 Escalation, Destruction
Example	Botnets & Spam	Advanced Persistent Threat	Credit Card, PHI, and PII Theft	Website Defacements	Destroy Critical Infrastructure
Targeted					
Character	Automated	Persistent	Financially Motivated	Conspicuous	Conflict Driven
	Conficker	Telvent	BWL Ransomware	?	Ukraine Attack

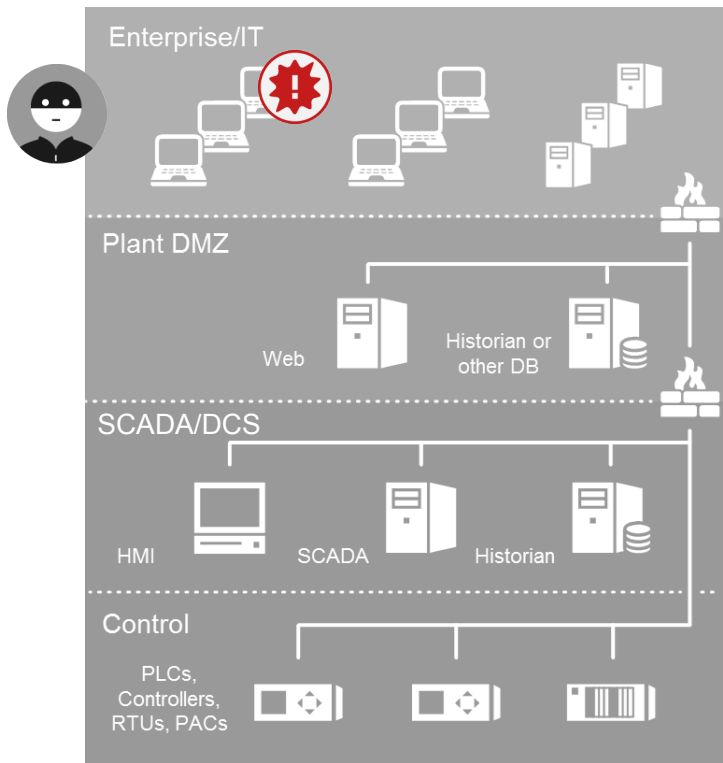
# UKRAINE ATTACK: ANALYSIS & RECOMMENDATIONS

*Mapping controls to attacker techniques, tactics,  
& procedures (TTPs)*

# Anatomy of a Targeted Attack



# Initial compromise



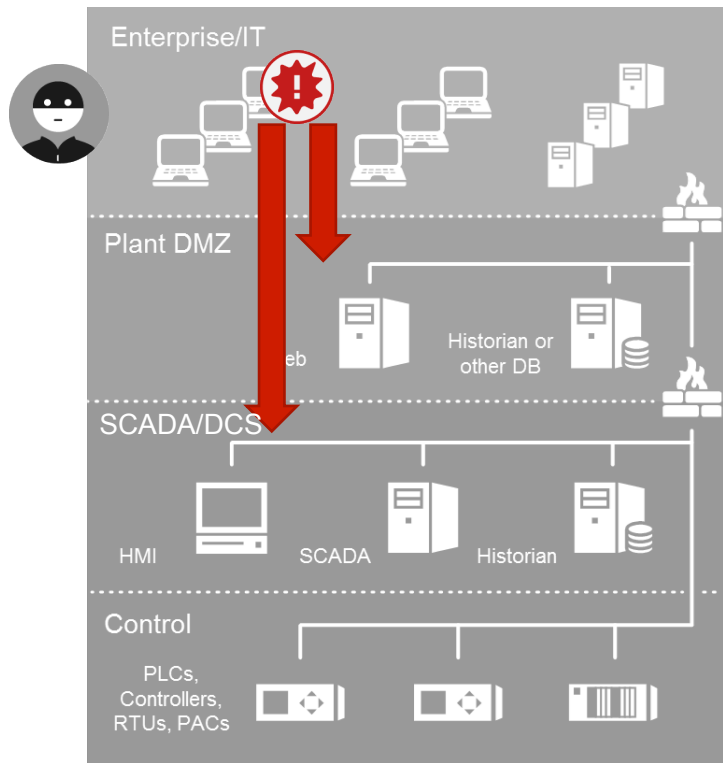
## TTP: Spearphishing

- Email attachment sandbox detonation
- Security awareness training for employees
- Reminders (ex. External origin warning)

## TTP: BlackEnergy3 installation

- Malware protection strategy
- IOC matching

# Gain access to the ICS



## TTP: Credential Capture/Use; ICS reconnaissance

- Network security monitoring for abnormal behavior

## TTP: Active Directory compromise

- Network segmentation
- Separate AD server for ICS environment

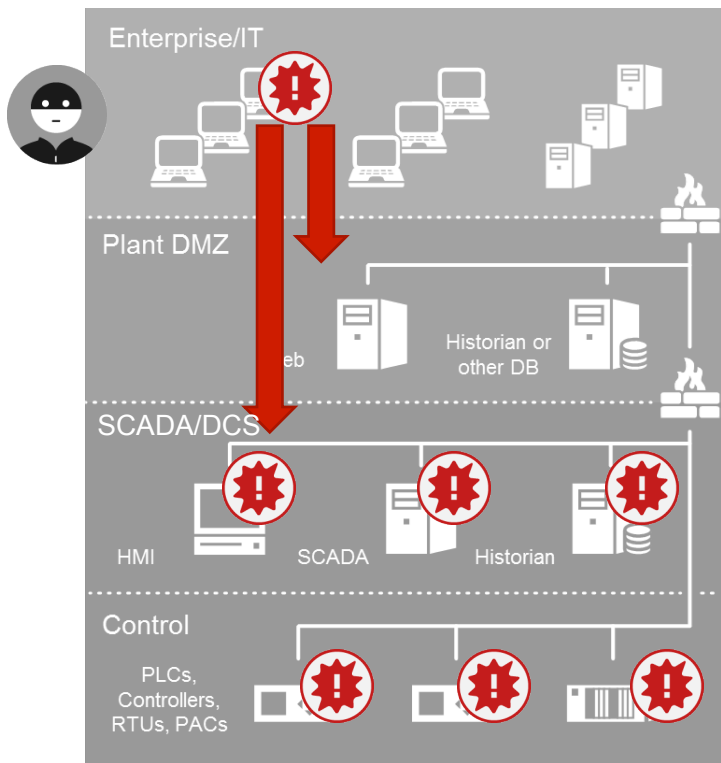
## TTP: Multiple command and control machines

- IP whitelisting for access to ICS network
- Virtualize ICS applications to simplify connectivity from IT to ICS; “Jumpbox” concept with detailed logging

## TTP: Remote Desktop HMI sessions through VPN

- Two-factor authentication
- Ability to shut down VPN access
- Ability to disable Remote Desktop/Remote Assistance

# Disrupt operations



## TTP: Issue interactive commands on ICS

- Incident response planning and practice
- Ability to sever all remote connections
- Ability to move to manual operations

## TTP: Destructive malware on ICS hosts

- Malware protection strategy / Application whitelisting
- Robust backup & recovery procedures – including things like spares, firmware images, RTU configurations

## TTP: Telephone Denial of Service (TDoS)

- Alternate outage communication channel



# Ukraine Attack Lessons Learned

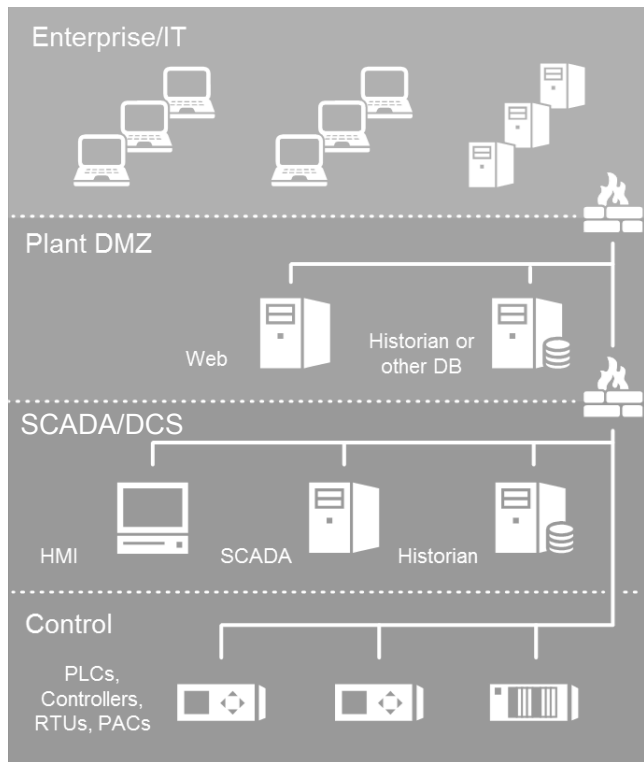
- Targeted attackers have:
  - Motivation
  - Determination
  - Resources
  - Cooperation and Coordination
- Electric utilities must have:
  - Defensible architecture
  - Monitoring and detection capability
  - Integrated IT/OT incident response plan
  - Most importantly...people

## Recommendation



Build an ICS architecture  
that you can actually defend

# Summary of key ICS security architecture technical controls



- ✓ **Network Segmentation**  
Isolate the ICS network from the IT network as much as possible
- ✓ **Rationalize remote access**  
If you can't eliminate remote access, reduce complexity of connectivity from IT to ICS via application virtualization or other methods
- ✓ **Two-factor authentication**  
Make the attacker work harder than just stealing administrator credentials
- ✓ **Application whitelisting, malware protection, and IOC matching**  
Make it difficult for the attacker to install malware, execute files, and persist

## Recommendation



Enhance your ICS-specific  
monitoring & detection

# ICS network security monitoring strategy

## ✓ **Network sensor covering ICS ingress/egress point**

Gain a full understanding of how compromised machines are communicating with your ICS

## ✓ **IDS/IPS**

Increase your ability to recognize attacks on ICS from the IT environment

## ✓ **Log collection**

Windows Events, Syslog increasingly generated by controllers

## ✓ **Agents on Windows hosts (after validation)**

Work with your vendor, validate it yourself, or take a calculated risk

## Recommendation



Have an integrated IT/OT  
incident response plan

## What is an IRP and why do we need one?

- ✓ Establish high-level governance
- ✓ Aligns policies, responsibilities, and efforts under a Mission Statement
- ✓ Defines roles & responsibilities
- ✓ Provides common definitions so everyone understands terminology and meaning

**Acme, Inc.**

*Cyber Security Incident  
Response Plan  
Version 1*

# Create one plan mapped to IT and ICS environments



+

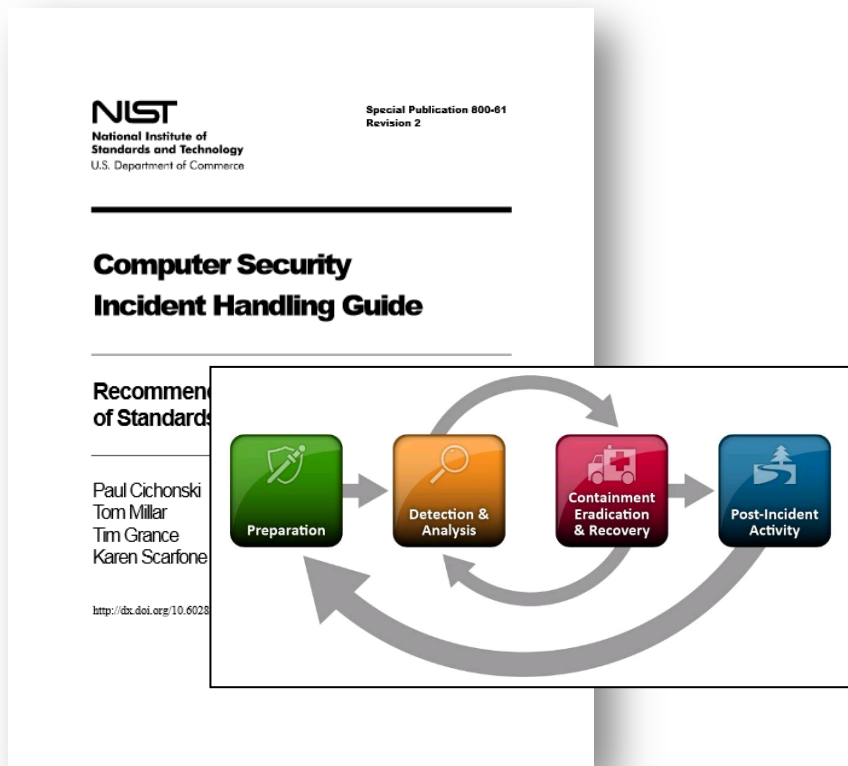


## Why?

- Coordinated and comprehensive
- Business risks and drivers are shared
- Cyber security and operational expertise are found in different places



# There's a standard for that!



## NIST SP 800-81 Revision 2:

### *Computer Security Incident Handling Guide*

- Definitions for key terms like “incident” and “event”
- Elements of a good policy, plan, and procedure for incident response
- List of the most common type of computer security incidents
- Incident Response Scenarios

# THINGS TO THINK ABOUT

*Major themes and takeaways for defenders*

## Takeaway #1



Air gapped industrial control systems are the exception and not the rule

## Takeaway #2



Successful attacks on ICS do not necessarily need to exploit ICS-specific vulnerabilities

## Takeaway #3



Compliance and best practices aren't good enough... you need to know if you are compromised

## Takeaway #4



No organization can prevent 100% of attacks – you win by minimizing an attack's impact

# QUESTIONS?