

# Comprehensive Cyber Situational Awareness (SA)

In the Face of *Cyber Entropy*



# Today's Panelists

---



**Dr. Adam Hahn**  
Lead Critical Infrastructure  
Security Engineer  
*MITRE Corporation*



**Suzanne Spaulding**  
Fmr DHS Undersecretary  
For Cyber and Infrastructure  
*Advisor at the  
Center for Strategic and Int'l Studies*



**Phil Trainor**  
Federal Product Manager  
*Nozomi Networks*



**Scott Foote**  
Managing Director  
*Phenomenati Consulting*

# Why Are We Here?

## Awareness Eludes Us

- **Roles**

- Chief Information Officer (CIO)
- Chief Information Security Officer (CISO)
- Chief Technology Officer (CTO)

- **Risk**

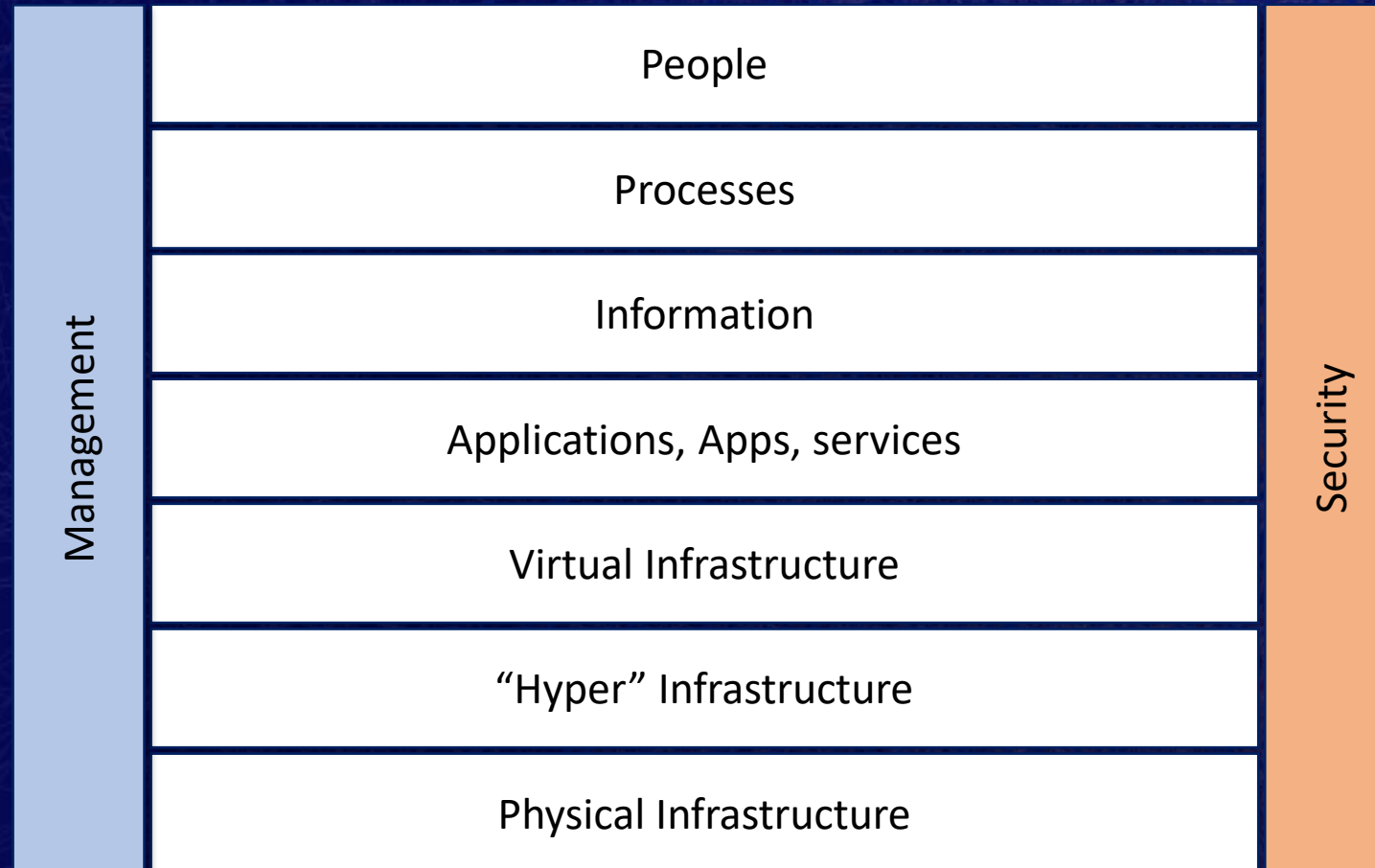
- Cyber **Entropy** → IT → ICS/SCADA (OT) → IoT
- Threats → Vulnerabilities → **Consequences**
- “Digital” Risk, “Cyber” Risk, “Operational” Risk

- **Risk Management Discipline**

- Quest to Bring Order to Chaos
- Information Security / Cyber Security Program
- Security and Safety of Operational Environments and Critical Infrastructure
- Comprehensive, Contextual **Awareness**



# CIO & CISO **Scope** & Expectations





Management	...	People	...	Security
	...	Processes	...	
	...	Information	...	
	...	Applications, Apps, services	...	
	...	Virtual Infrastructure	...	
	...	“Hyper” Infrastructure	...	
	...	Physical Infrastructure	...	

**OT**

**Traditional IT**

**IoT**



# Where to *Begin* Managing **Risk**?

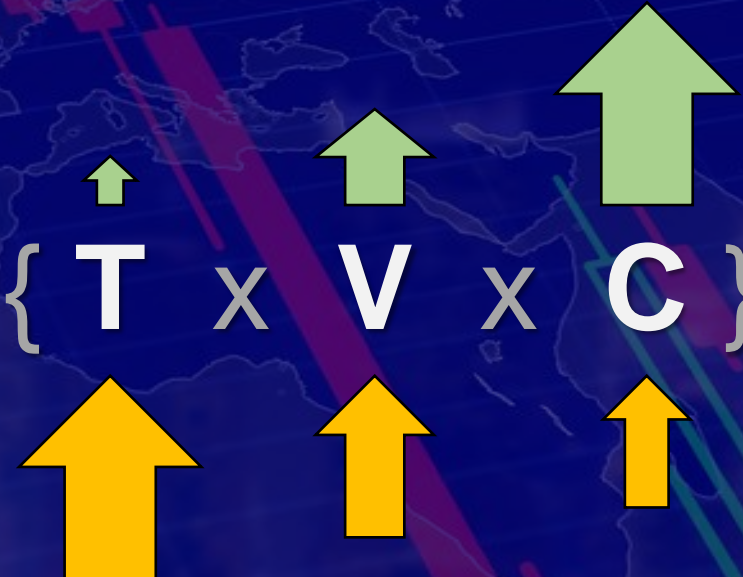
---





# Risk?

The "Risk Formula" (model)

$$\text{Risk} = \sum f \{ \overset{\uparrow}{\mathbf{T}} \times \overset{\uparrow}{\mathbf{V}} \times \overset{\uparrow}{\mathbf{C}} \}$$


Fundamental **Elements** of Risk

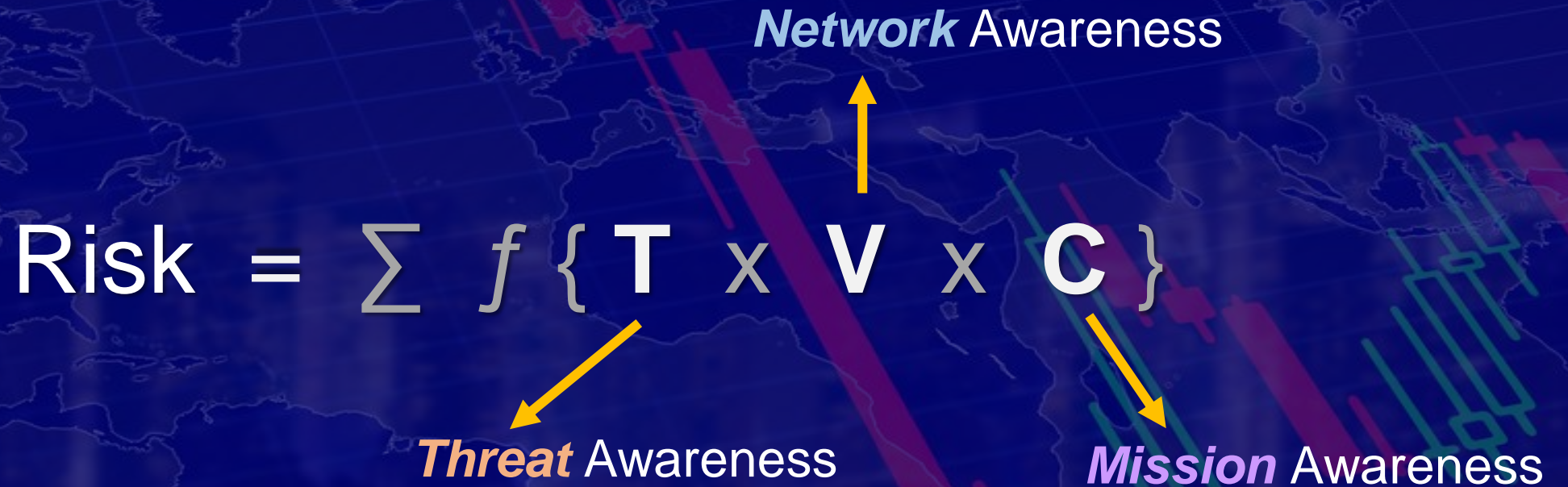
T = Threat  
V = Vulnerability  
C = *Consequence*



# Contextual Situational **Awareness** Informs Decisions

$$\text{Risk} = \sum f \{ \mathbf{T} \times \mathbf{V} \times \mathbf{C} \}$$

*Threat* Awareness      *Network* Awareness      *Mission* Awareness



Fundamental **Elements** of Situational Awareness

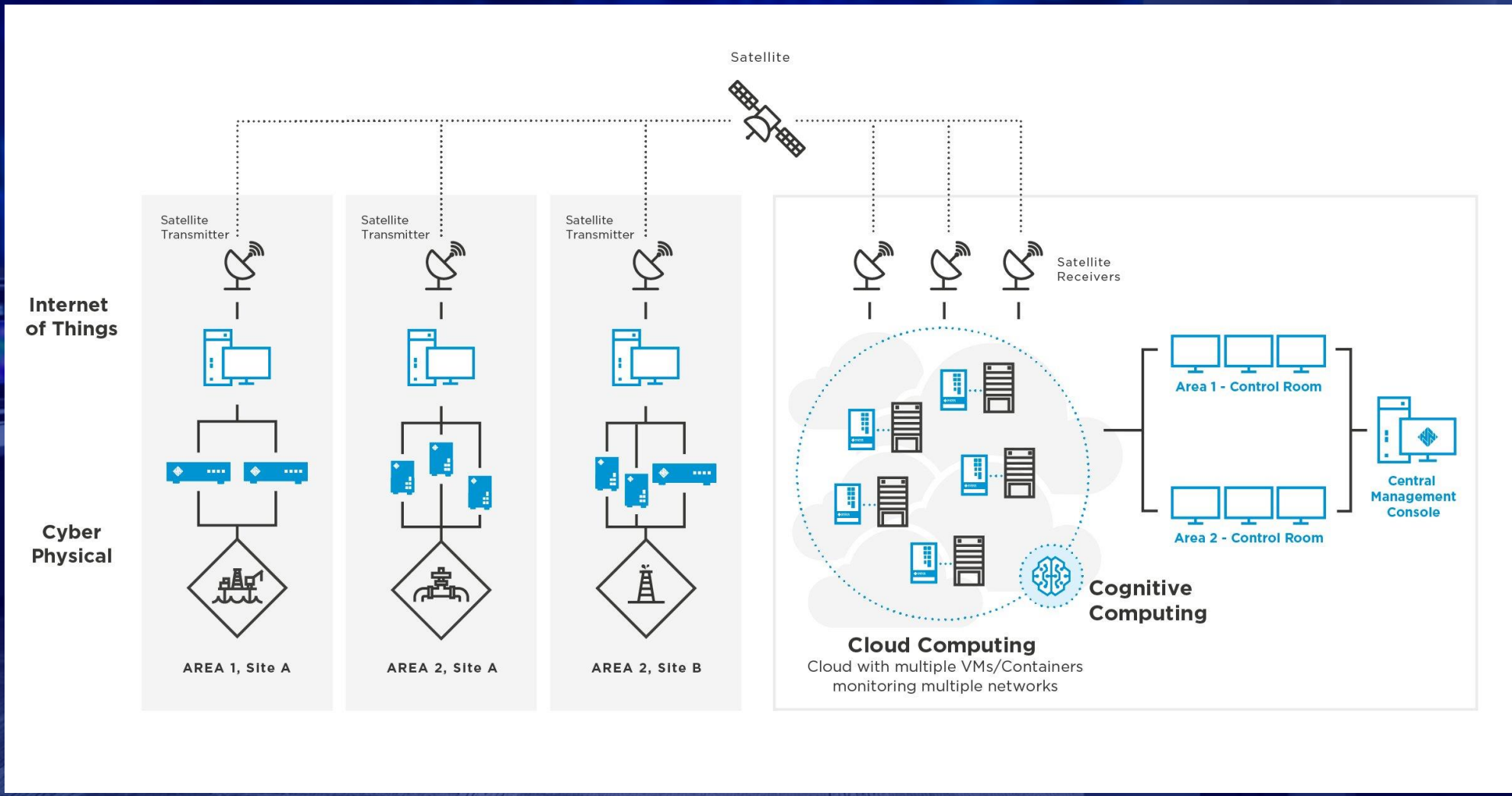


# Threat Awareness – MITRE’s ATT&CK for ICS

Initial Access	Execution	Persistence	Privilege Escalation	Evasion	Discovery	Lateral Movement	Collection	Command and Control	Inhibit Response Function	Impair Process Control	Impact
Drive-by Compromise	Change Operating Mode	Modify Program	Exploitation for Privilege Escalation	Change Operating Mode	Network Connection Enumeration	Default Credentials	Automated Collection	Commonly Used Port	Activate Firmware Update Mode	Brute Force I/O	Damage to Property
Exploit Public-Facing Application	Command-Line Interface	Module Firmware	Hooking	Exploitation for Evasion	Network Sniffing	Exploitation of Remote Services	Data from Information Repositories	Connection Proxy	Alarm Suppression	Modify Parameter	Denial of Control
Exploitation of Remote Services	Execution through API	Project File Infection		Indicator Removal on Host	Remote System Discovery	Lateral Tool Transfer	Detect Operating Mode	Standard Application Layer Protocol	Block Command Message	Module Firmware	Denial of View
External Remote Services	Graphical User Interface	System Firmware		Masquerading	Remote System Information Discovery	Program Download	I/O Image		Block Reporting Message	Spoof Reporting Message	Loss of Availability
Internet Accessible Device	Hooking	Valid Accounts		Rootkit	Wireless Sniffing	Remote Services	Man in the Middle		Block Serial COM	Unauthorized Command Message	Loss of Control
Remote Services	Modify Controller Tasking			Spoof Reporting Message		Valid Accounts	Monitor Process State		Data Destruction		Loss of Productivity and Revenue
Replication Through Removable Media	Native API						Point & Tag Identification		Denial of Service		Loss of Protection
Rogue Master	Scripting						Program Upload		Device Restart/Shutdown		Loss of Safety
Spearphishing Attachment	User Execution						Screen Capture		Manipulate I/O Image		Loss of View
Supply Chain Compromise							Wireless Sniffing		Modify Alarm Settings		Manipulation of Control
Transient Cyber Asset									Rootkit		Manipulation of View
Wireless Compromise									Service Stop		Theft of Operational Information
									System Firmware		

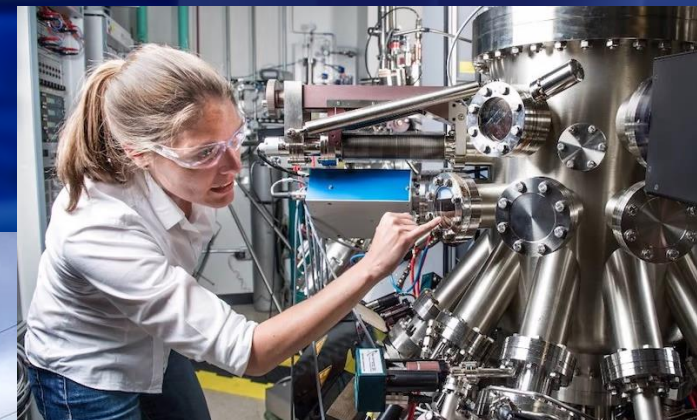


# Network Awareness – Nozomi Networks





# Mission Awareness – Investing in Resiliency





# Questions

---





# Thank You to Our Panelists

---



**Dr. Adam Hahn**

Lead Critical Infrastructure  
Security Engineer  
*MITRE Corporation*



**Suzanne Spaulding**

Fmr DHS Undersecretary  
For Cyber and Infrastructure  
*Advisor at the  
Center for Strategic and Int'l Studies*



**Phil Trainor**

Federal Product Manager  
*Nozomi Networks*



