



San Francisco | March 4–8 | Moscone Center

A large, abstract graphic in the top right corner consisting of numerous thin, curved lines of varying colors (blue, yellow, green) radiating from a central point, resembling a network or a starburst.

BETTER.

SESSION ID: PDAC-W12

What Lurks within Your IT: Spotlight on the Dark Side of the Supply Chain

Dawn Cappelli

VP Global Security and CISO
Rockwell Automation
@DawnCappelli

Edna Conway

Chief Security Officer, Global Value Chain
Cisco Systems, Inc.
@Edna_Conway

Why Are We Here? Digital Transformation



IT/OT Convergence



Connected Devices



Function & Data



Multiple Clouds

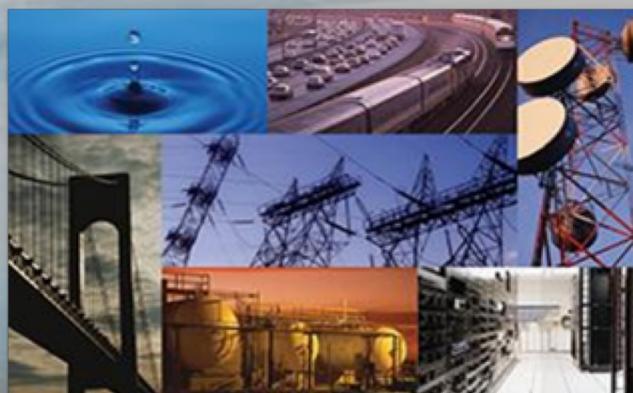
Convergence of IT & OT



Connected Home



Connected Factory



Critical Infrastructure

Who & What is the 3rd Party Ecosystem



Threats Continue To Rise

In Quantity, Intensity, Sophistication and Impact



EVERY DAY



Securely Harness the 3rd Party Ecosystem

Threats



Manipulation



Espionage



Disruption

Threat Impacts



Taint



Counterfeit



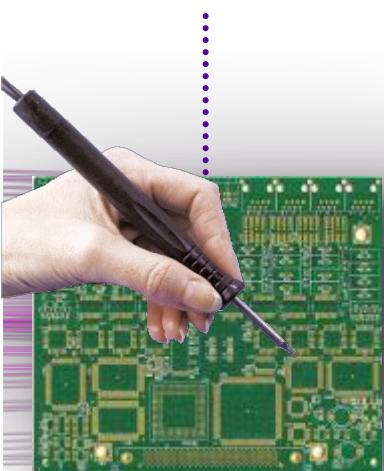
IP Misuse



Information Security
Breach

Where & How “Bad Actors” Can Succeed

Altered electrical flow on a printed circuit board



3rd party software containing vulnerabilities

Alteration during import/export or transportation



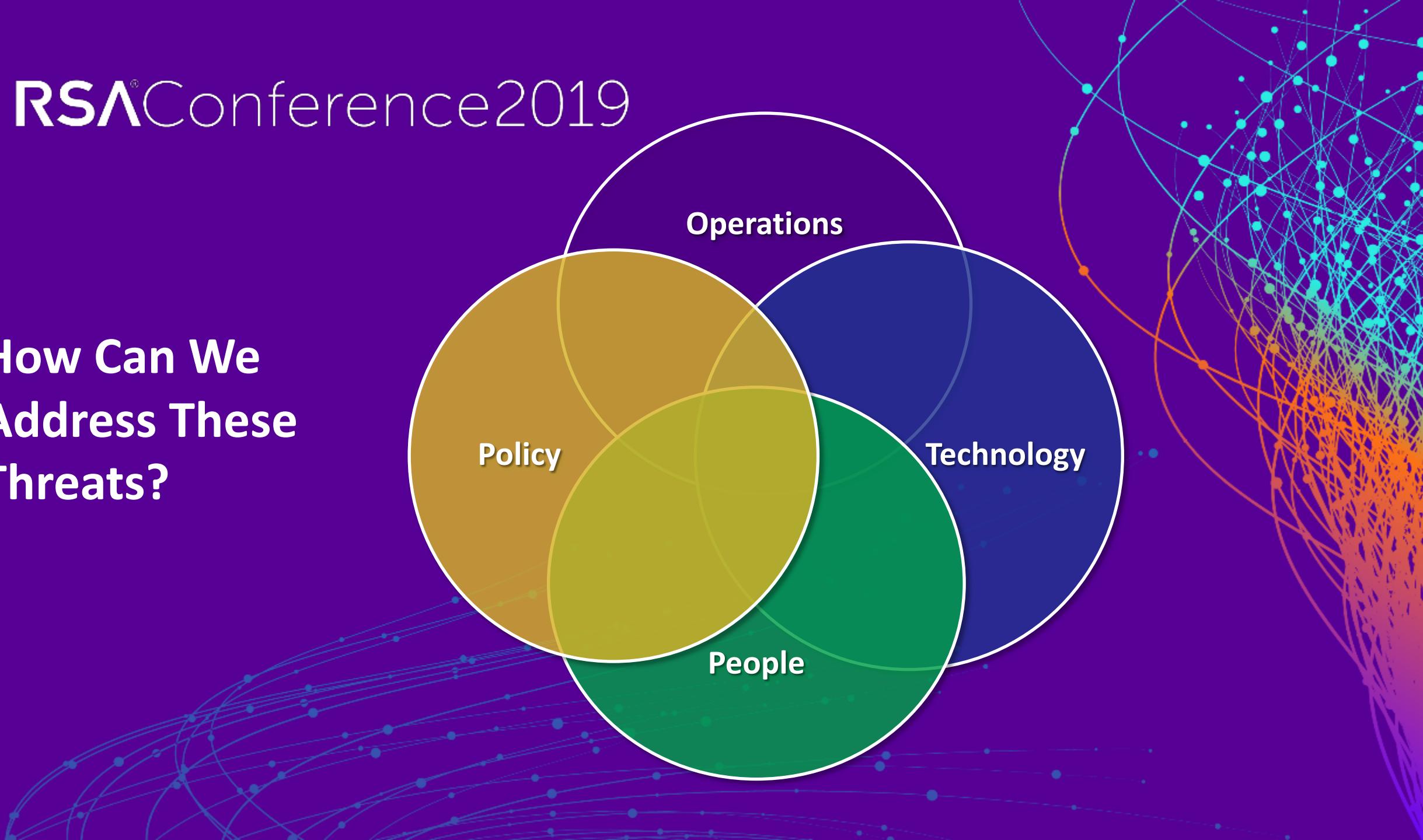
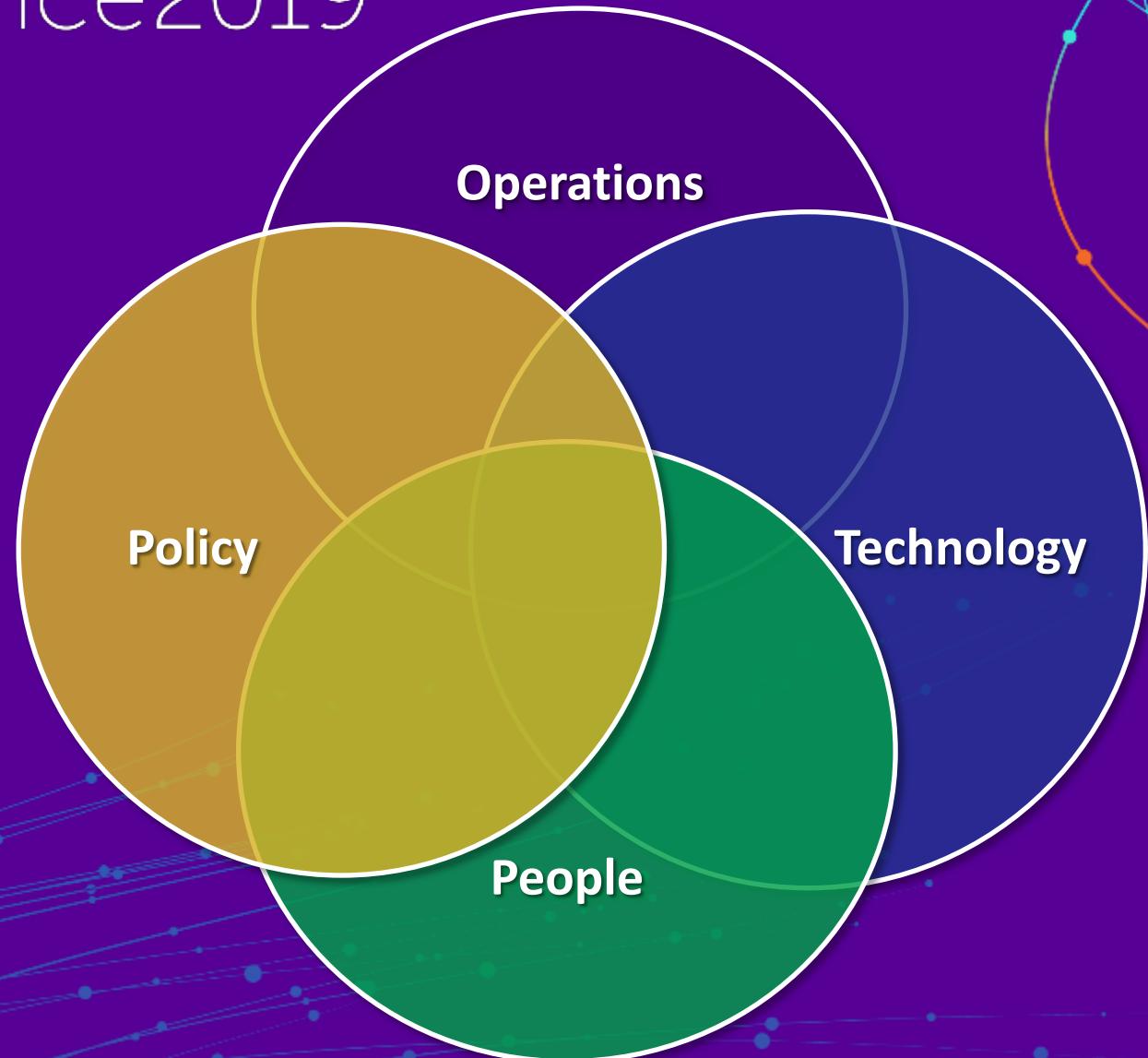
“Added” integrated circuits on a printed circuit board assembly

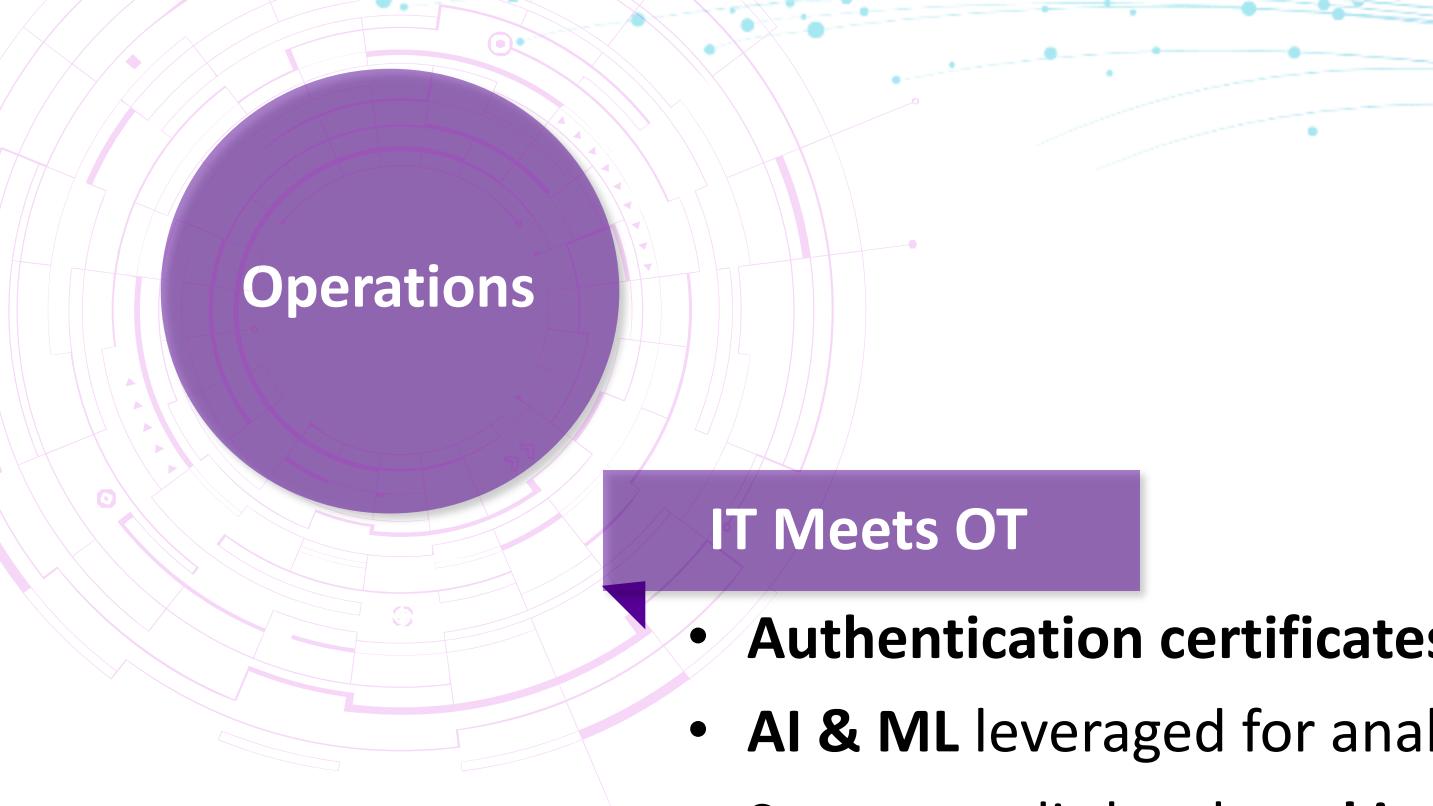


Functional impact to critical infrastructure



**How Can We
Address These
Threats?**





Operations

IT Meets OT

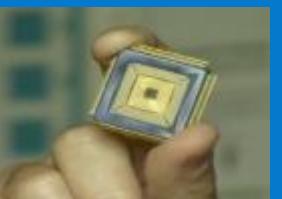
- **Authentication certificates** for identity management
- **AI & ML** leveraged for analysis of IoT data streams
- Secure, audit-level **tracking of IoT data transactions**
- **Blockchain** of custody for immutable device ID
- **Encryption** for data deployed in transit and at rest
- Joint IT and OT **resiliency** built in
- **Enterprise security** as part of your Industrial IoT deployment

Technology

Trust Anchor

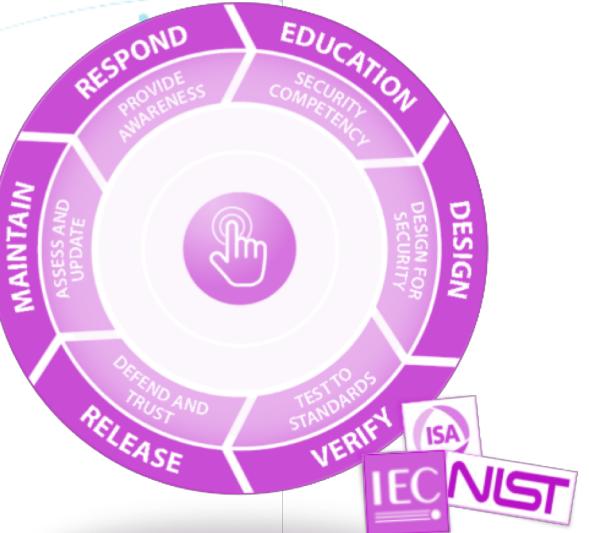
Secure Identity Verification

- Authenticity and License Check
 - Verify Secure Identity



Product Security

- Immutable Identity
 - Secure Storage (Keys and Objects)
 - Certifiable Entropy Source
 - Secure Crypto Assist
 - Secure Application Certificates



Vendors must build security into products with a focus on security throughout the product's lifecycle:

- Product Security Office
- Secure Development Lifecycle



Policy

Architecture Domain Structure



Security Policy





People

Insider Risk

- Formal program to protect customers' Intellectual Property**
- Controls for cyber sabotage of their products and customer sites**
- Controls and training for customer data handling (e.g. USB usage)**
- Background checks**
- Third party personnel as insider risks**
- Security awareness and communications**
- Role-specific and ongoing**

Leverage NIST Cybersecurity Framework for Supply Chain Risk

#RSAC



Ensure Suppliers Deploy a Layered Approach to Security



Navigating the Dark Side of Supply Chain

A Roadmap You Can Apply

1

Build Your Foundation

- Map the who, what and where of your 3rd party ecosystem
- Implement a secure development lifecycle
- Identify areas for potential unauthorized modification
- Research modification detection techniques/technology

Navigating the Dark Side of Supply Chain

A Roadmap You Can Apply

#RSAC

2

Develop Your Roadmap

- Develop a comprehensive architecture employing a layered approach
- Address 3rd party security with a risk based approach
- Leverage government and industry partnership



Navigating the Dark Side of Supply Chain

A Roadmap You Can Apply

#RSAC

3

Execute
Flexibly

- Limit access and connection with a least privilege, role-based approach
- Balance benefit of connectivity vs. risks of information access and control
- Deploy IT security practices in operations: (e.g. segmentation)



We are all in this together.



Questions?

