

→ Webinar



# Assuring Software Products in Critical Systems



**Carrie Wibben**  
President, Exiger



**Cassie Crossley**  
VP, Supply Chain Security,  
Cybersecurity & Product Security  
Office, Schneider Electric



**JC Herz**  
Senior Vice President,  
Software Supply Chain  
Solutions, Exiger

04.3.24 | 1 PM ET

# Playbook Pillars



**Commit to Transparency and Trusted Partnerships**

**Prioritize Critical Products**

**Illuminate and Assess Risk**

**Identify and Implement Mitigations  
to Remediate Risk**

**Continuously Monitor Product for Risk Indicators**

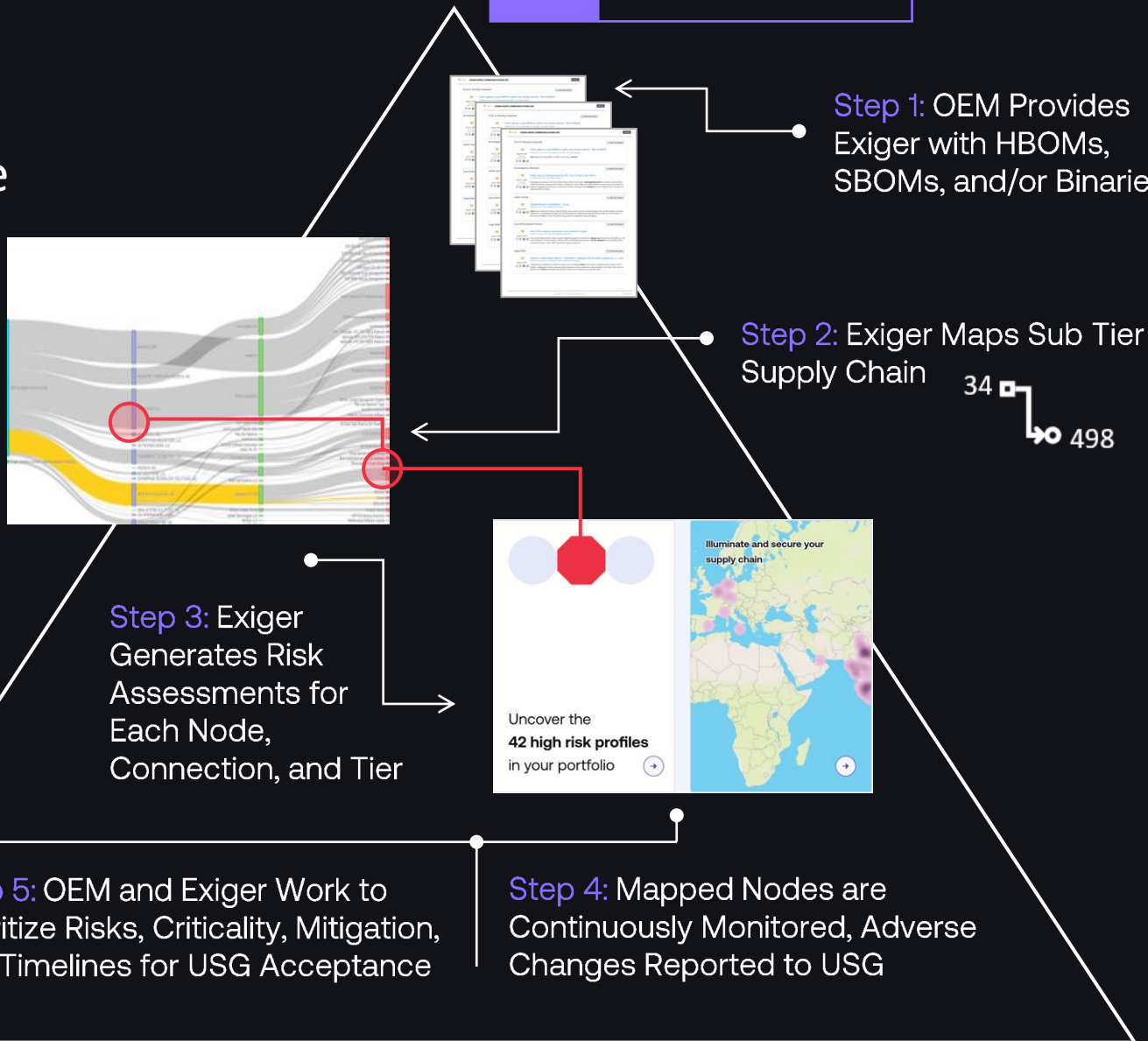
Exiger worked with Schneider Electric and the USG to build the Supply Chain Product Assurance Playbook, a scalable solution for rapidly mapping and mitigating product risks at scale.

### Comparison Analysis

Current USG assurance program, **DOE CyTRICS**, is rigorous but cost and time prohibitive.

In FY22, DOE reported the program invested **\$32 million to investigate 11 systems**, ultimately identifying 28 vulnerabilities.

4-6 Week Process



# The Chemistry of Composite Risk

## Foreign Ownership, Control or Influence ("FOCI")

- State Ownership
- Foreign Locations
- Dominating Markets, Customers, Suppliers
- Corporate Records
- Transaction News
- Hiring Foreign Nationals through H1B Visa Program

## Environmental, Social & Governance Risk ("ESG")

- Environmental Controversies
- Non-Harmful Products & Quality Products
- Diversity, Equity & Inclusion
- Safe Workplace
- Data Privacy
- Fair Customer Treatment
- Safe Labor Practices
- Human Rights & Modern Slavery
- Compliance with Laws & Regulation
- Business with High-Risk Countries
- Fair Taxes
- Sound Governance

## Reputational, Criminal & Regulatory Risk ("RCR")

- Watchlists
- Trade Restriction Lists
- Criminal Records
- Debarment Lists
- Sanctions Lists
- Personnel Risk/Insider Threat
- Intellectual Property Theft
- Lack of Corporate Presence
- Identification of Adverse Media

## Operational Risk ("OR")

- Locations & Geopolitical Risk
- Hardware Counterfeit & Compromise Reporting
- Labor Issue Reporting
- Software Integrity
- Alternative Suppliers
- Predictive Obsolescence
- Certification & Awards
- Catastrophic Weather Events
- Climate Events

## Financial Health ("FH")

- Financial Fines
- Financial Crimes
- Bribery & Corruption
- Central Bank Reprimands
- Debarment & Sanctions Lists
- S&P & Moody's Indicators
- Analysts & Broker Data

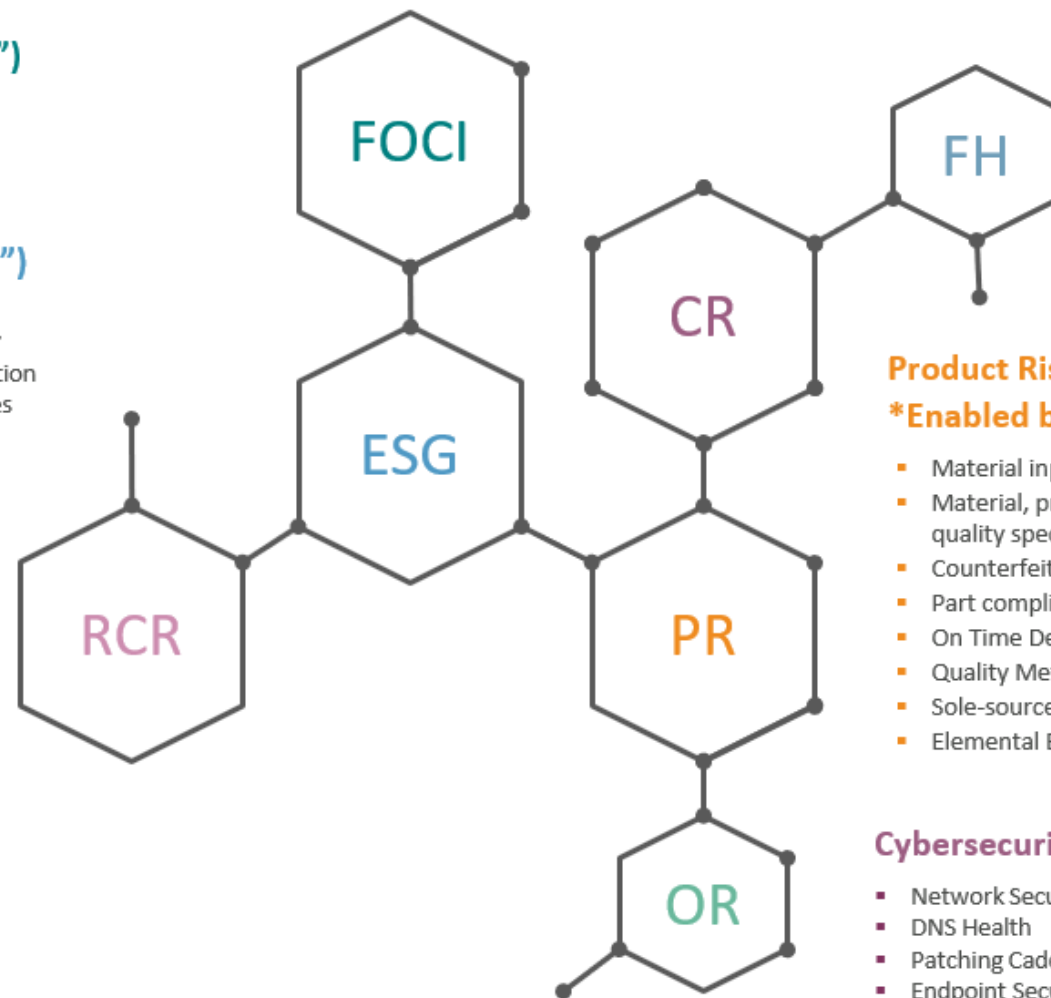
## Product Risk ("PR")

**\*Enabled by SDX and Ion Channel\***

- Material input to end-product
- Material, processing, and quality specifications
- Counterfeit Risk
- Part compliance
- On Time Delivery
- Quality Metrics
- Sole-source vs multi-source
- Elemental Exposure
- ICS File Provenance
- End of Life
- Change of Control
- Integration Risk
- Prohibited Components
- Technical Debt
- Geopolitical Risk
- Vendor Negligence

## Cybersecurity Risk ("CR")

- Network Security
- DNS Health
- Patching Cadence
- Endpoint Security
- IP Reputation
- Application Security
- Cubit Score
- Social Engineering
- CVE
- Data Breach (Open Source)
- Software Security (Open Source)
- Hacker Chatter
- Information Leak






# Moderated Session



O'REILLY™

# Software Supply Chain Security

Securing the End-to-End Supply Chain for Software, Firmware, and Hardware



Cassie Crossley  
Foreword by Emily Heath

*"During a time of ever-increasing threats to our systems, this book serves as a practical guide for any organization looking to include Software Supply Chain Security as part of their risk management program."*

**-- Grant Schneider**

**Former US Federal Chief Information Security Officer**

Check out Cassie's book [here](#)! One lucky attendee will be gifted a **free copy** of the e-book, so be sure to check your email after the event!





# Audience Q&A

Post your questions in  
the Livestream chat!