A DIVISION OF NERC

E-ISAC

ELECTRICITY INFORMATION SHARING AND ANALYSIS CENTER

Electric-Gas Interdependence Security Perspectives

Sam Chanoski, Director, Threat Intelligence, E-ISAC

Electric-Gas Working Group Meeting

July 30, 2019

TLP:WHITE

RELIABILITY | RESILIENCE | SECURITY

Agenda

- About the E-ISAC
- Security risk analysis model
- “Know the threat, know the net”
- What we’re doing about it

E-ISAC Overview

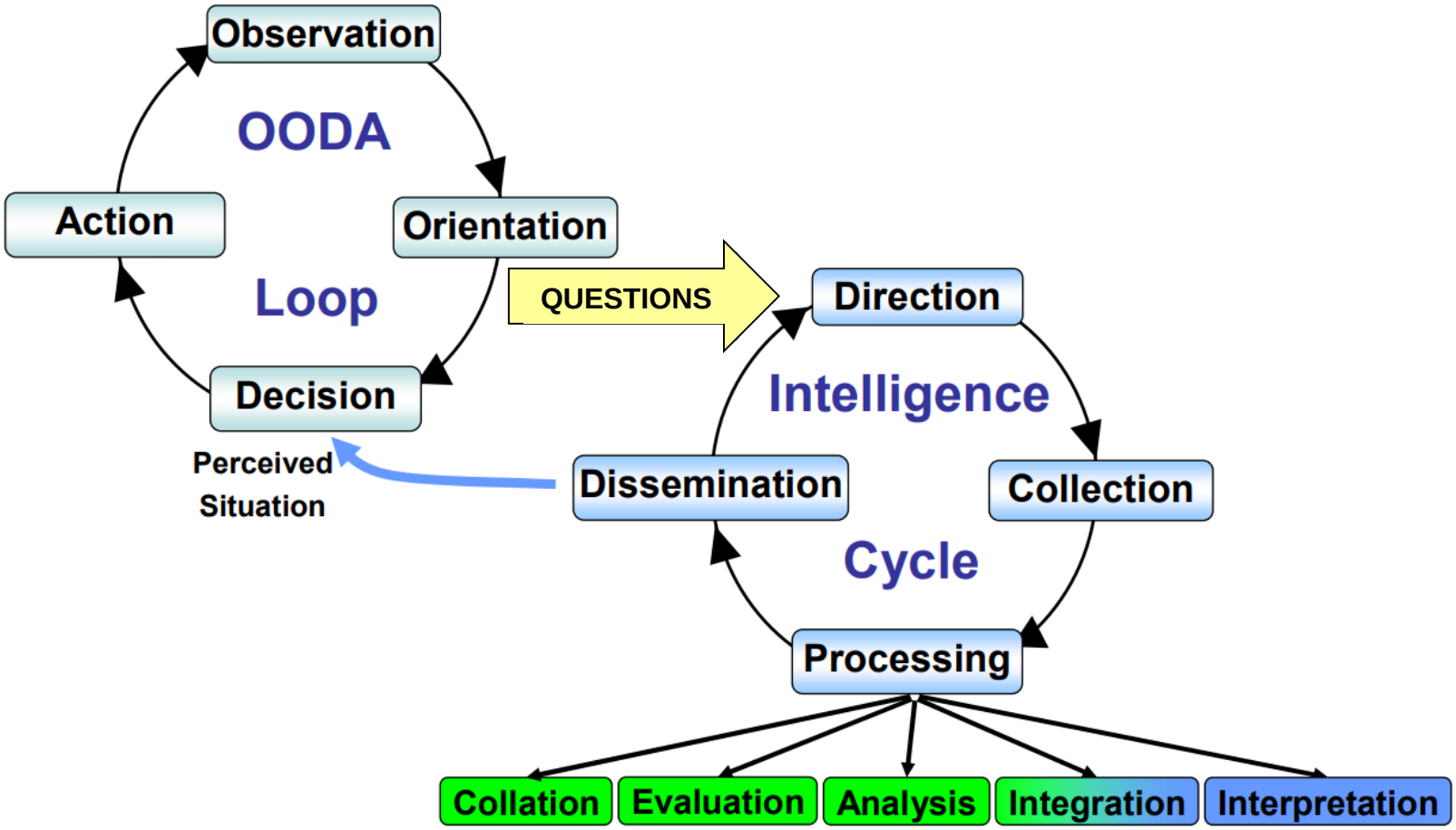
Mission

The E-ISAC reduces cyber and physical security risk to the electricity industry across North America by providing unique insights, leadership, and collaboration

Vision

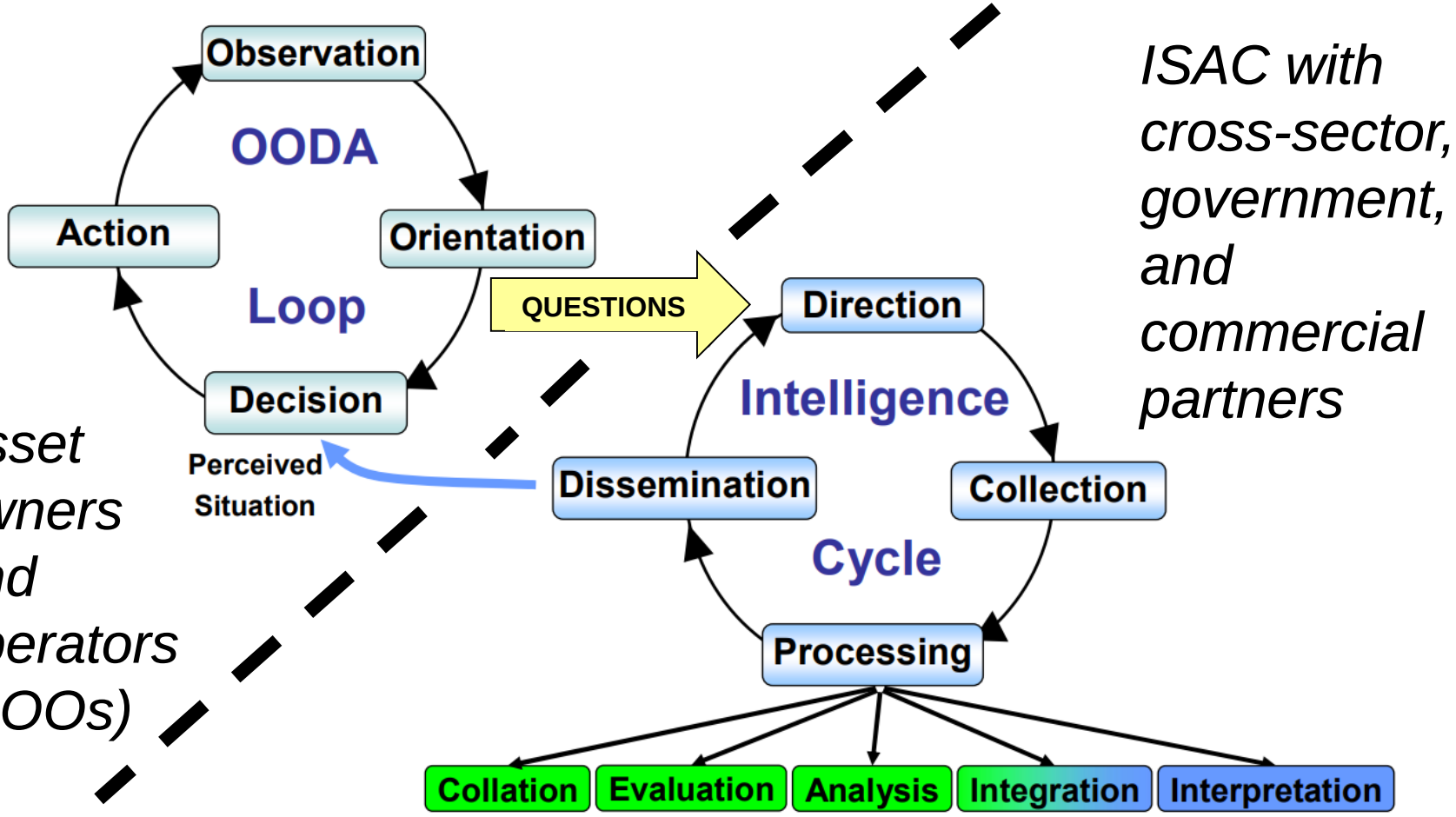
To be a world class, trusted source for quality analysis and rapid sharing of security information for the electricity industry

Analytical Sausage-Making



Adapted from Biermann, Hörling & Snidaro, 2009

Analytical Sausage-Making



Adapted from Biermann, Hörling & Snidaro, 2009

Risks, Threats, Vulnerabilities, oh my!

THREAT

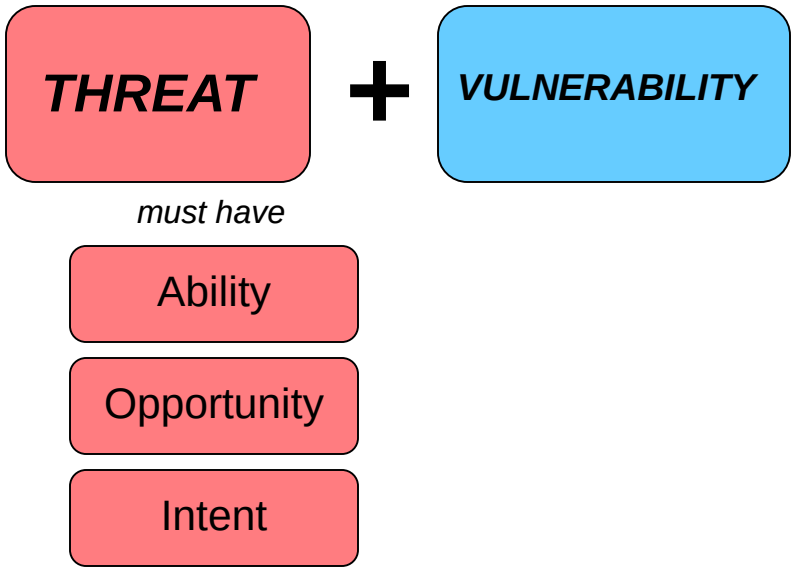
Risks, Threats, Vulnerabilities, oh my!

THREAT

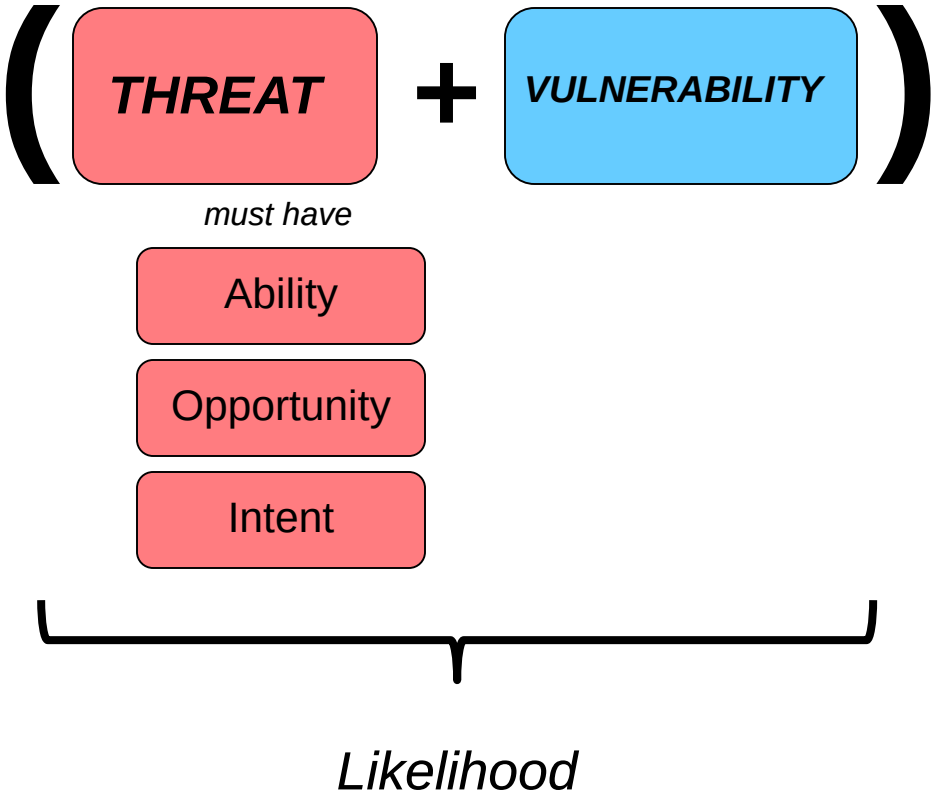
must have

- Ability
- Opportunity
- Intent

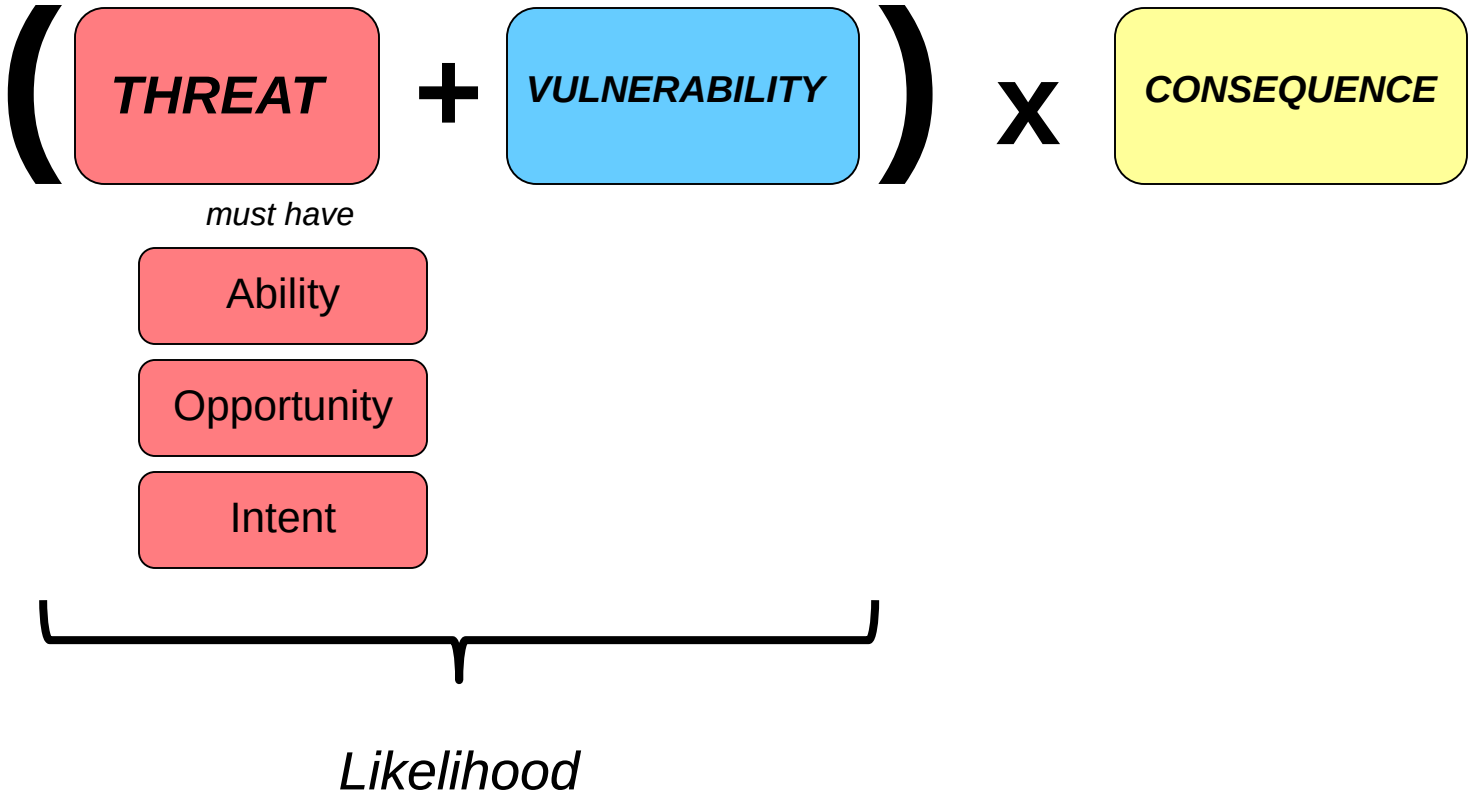
Risks, Threats, Vulnerabilities, oh my!



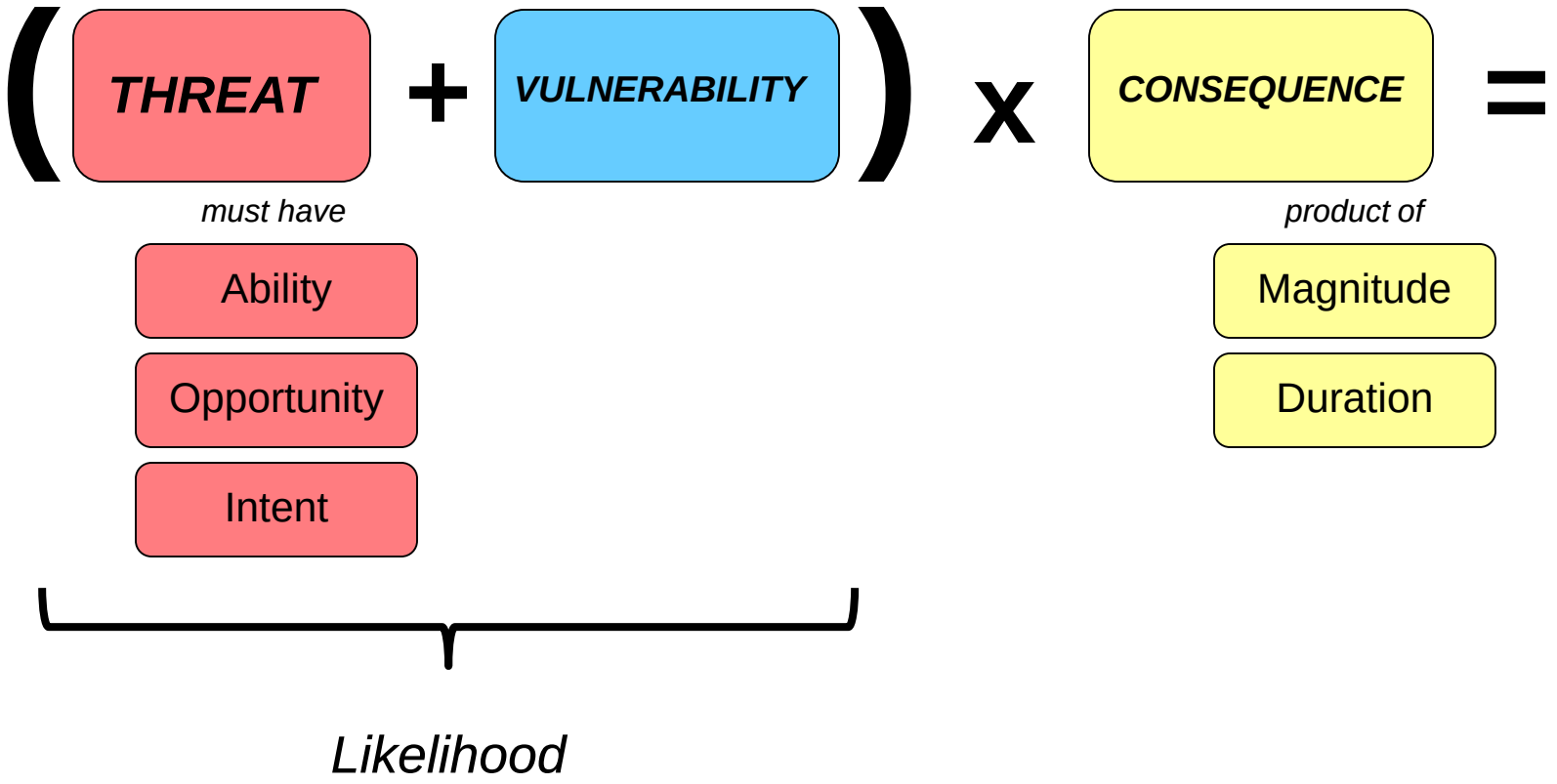
Risks, Threats, Vulnerabilities, oh my!



Risks, Threats, Vulnerabilities, oh my!

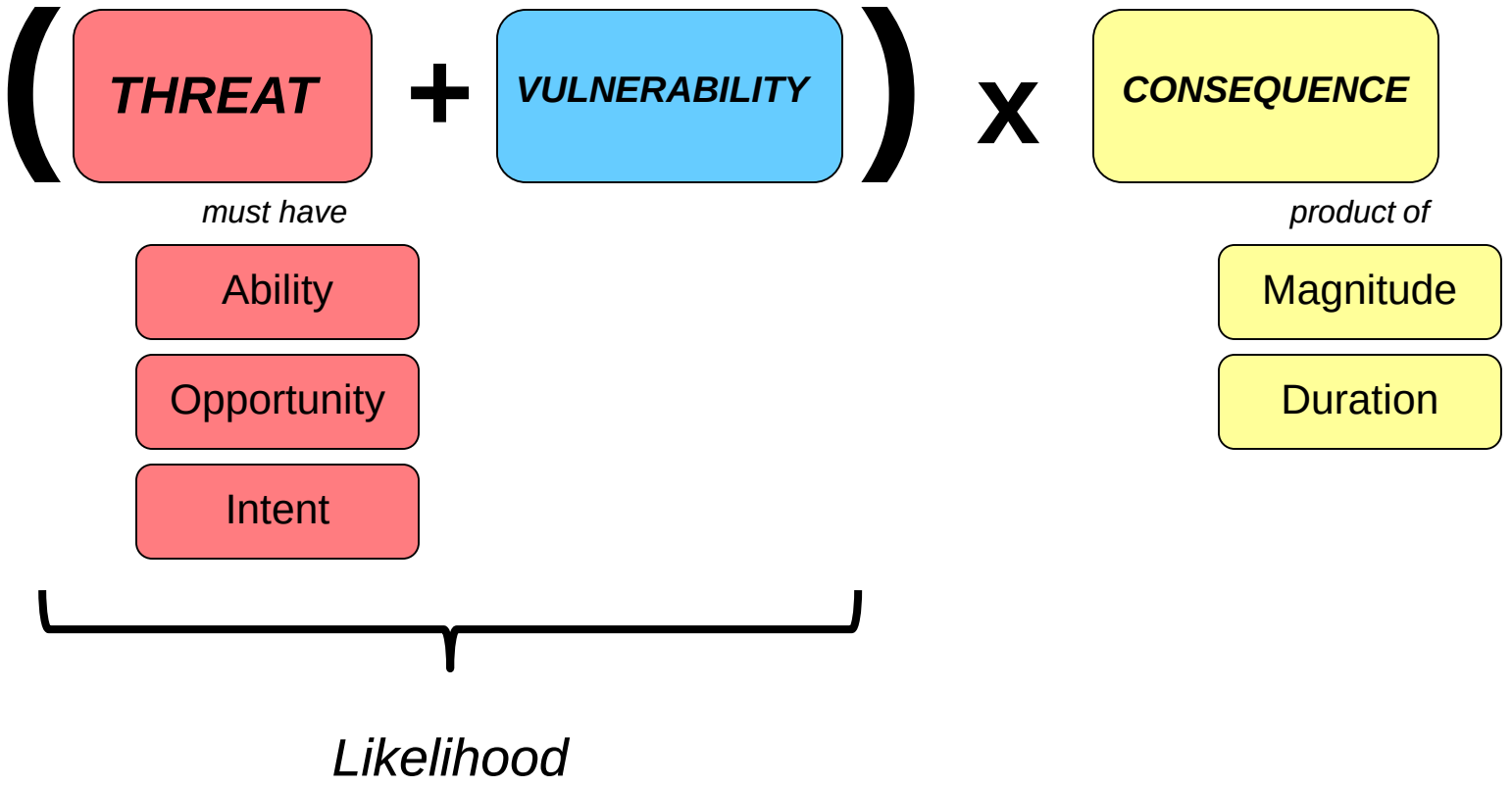


Risks, Threats, Vulnerabilities, oh my!

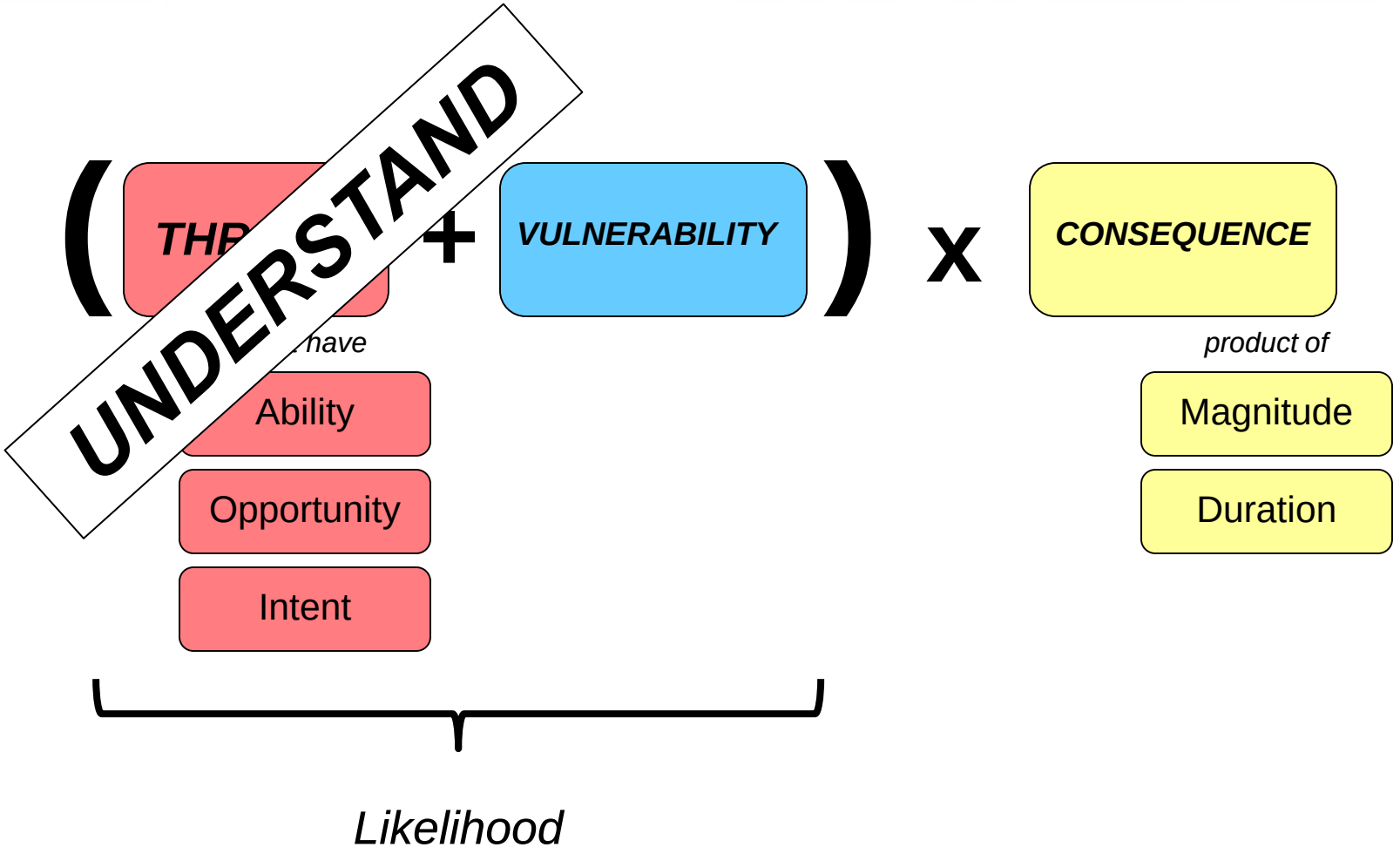


Risks, Threats, Vulnerabilities, oh my!

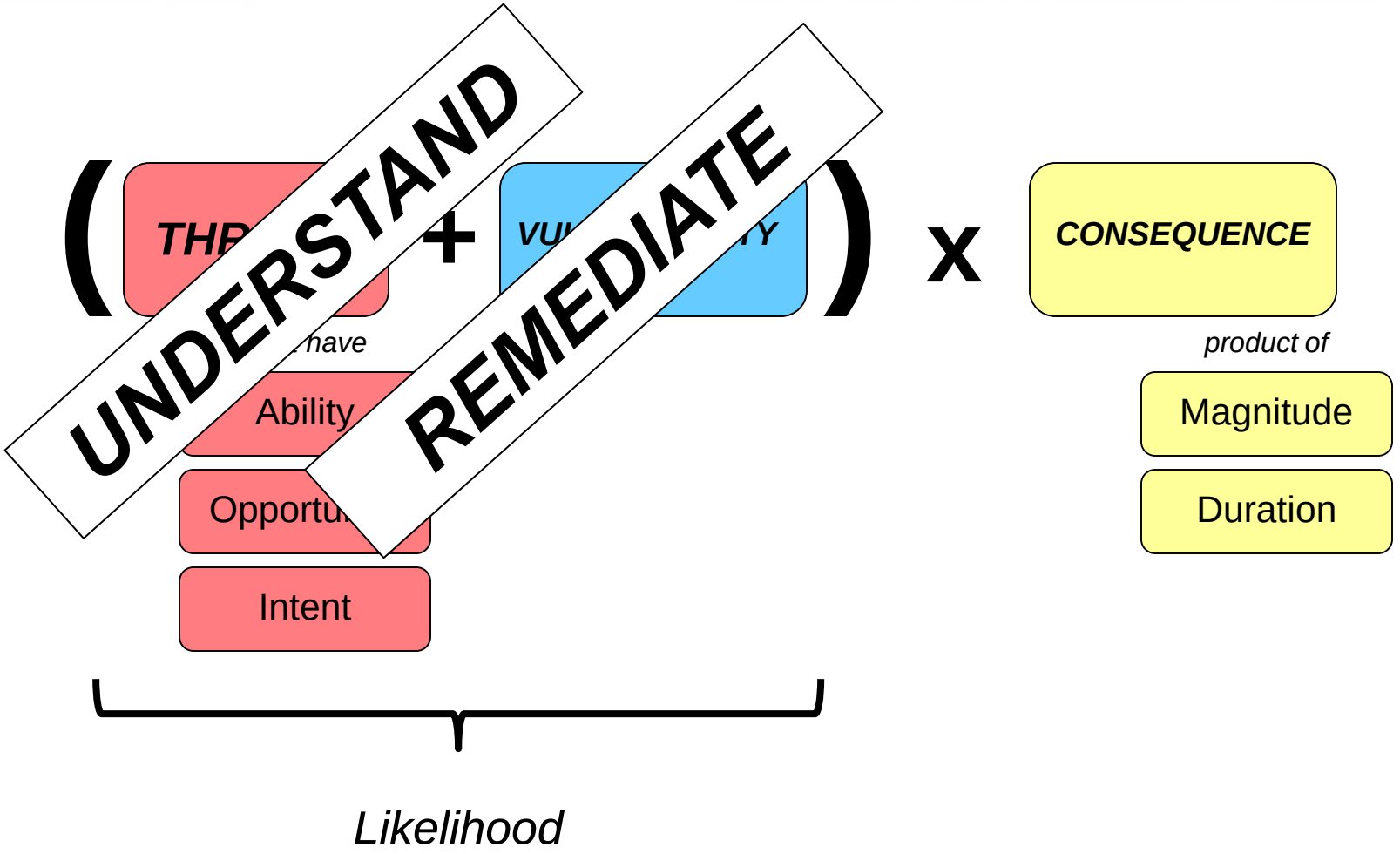
Risks, Threats, Vulnerabilities, oh my!



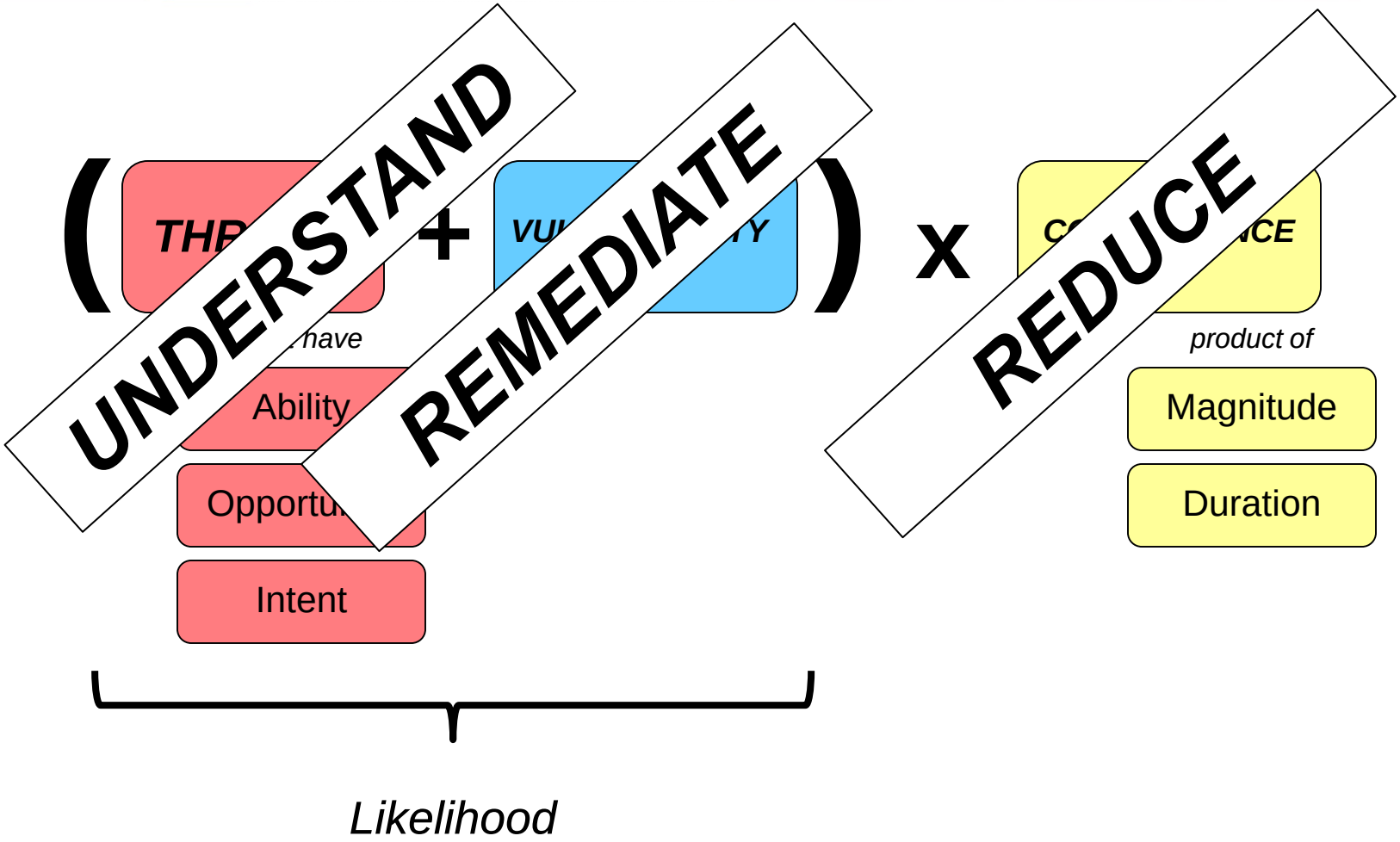
Risks, Threats, Vulnerabilities, oh my!



Risks, Threats, Vulnerabilities, oh my!



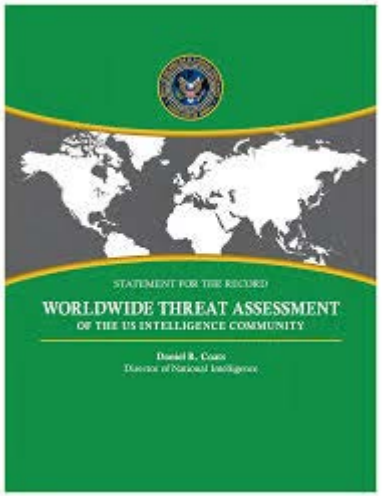
Risks, Threats, Vulnerabilities, oh my!



Risks, Threats, Vulnerabilities, oh my!

The risk is real

- 2019 Worldwide Threat Assessment
- 2018 attack on EDI system causes economic and indirect operational impacts
- 2017, 2019 Triton / TRISIS / Hatman attacks on Safety Instrumented Systems



Latitude Technologies

A team of teams

U.S. DEPARTMENT OF ENERGY

Homeland Security

U.S. Government

NationalCouncilofISACs

WATER ISAC

MS-ISAC
Multi-State Information Sharing & Analysis Center

DNG-ISAC

Other ISACs

ELECTRICITY INFORMATION SHARING AND ANALYSIS CENTER
A Division of NERC

International ISACs (Japan and European)

NRECA
America's Electric Cooperatives

AMERICAN PUBLIC POWER ASSOCIATION

EEI
Edison Electric INSTITUTE

Canadian Electricity Association | Association canadienne de l'électricité

Trade Associations

Public Safety Canada | Sécurité publique Canada

CANADIAN CENTRE FOR CYBER SECURITY | CENTRE CANADIEN POUR LA CYBERSÉCURITÉ

Natural Resources Canada | Ressources naturelles Canada

Canadian Government

What to share

Cyber Security

- Unexplained OT device freezes, reboots, or failures
- Sophisticated phishing (spoofed domains, trusted vendors, high value recipients)
- Scanning or reconnaissance of ICS ports and protocols
- Insights and forensic artifacts from incident response and threat hunting
- Abnormal DNS requests or authentication attempts

Physical Security

- Unusual observation or surveillance of facilities
- Misrepresentation of affiliation
- Theft, loss, or diversion of key safety or security items, systems and technologies
- Expressed or implied threats
- Breach or attempted intrusion
- SCADA/EMS anomalies coincident with a physical security event

Context is (almost) everything!

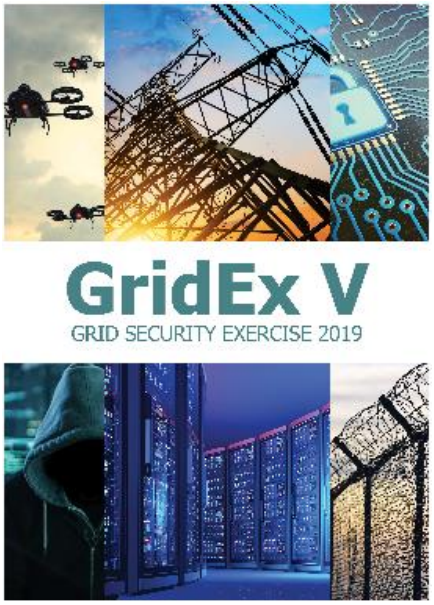
How to exchange information

- Portal, email, phone – whatever works for the member
- No specific forms or formats; use clear language
- *You* control how we further share and attribute the information

E-ISAC	DNG-ISAC	ONG-ISAC
operations@eisac.com	Analyst@DNGISAC.com	info@ongisac.org
www.eisac.com	www.dngisac.com	https://ongisac.org
202-790-6000 (24/7)		

106 days till GridEx V!
November 13-14, 2019

GridEx V objectives



- Exercise incident response plans
- Expand local and regional response
- Engage critical interdependencies
- Increase supply chain participation
- Improve communication
- Gather lessons learned
- Engage senior leadership

The road ahead

- Create more opportunities to collaborate cross sector
- Grow E-ISAC capabilities to serve member needs
- Increase partnership and collaboration with vendors

Questions and Answers

Sam Chanoski
Director, Threat Intelligence
sam.chanoski@eisac.com
w: 404-446-9706