REMEDYS:
Research Exploring Malware in Energy DeliverY Systems

Julia Cho, Dr. Keri Pearlson

NEED: FUTURE RESPONSE IN THE FACE OF EVOLVING CYBERSECURITY THREAT FOR ENERGY SECTOR

Organizations **often must rely on their own expertise and personal relationships to identify and resolve cyber issues**

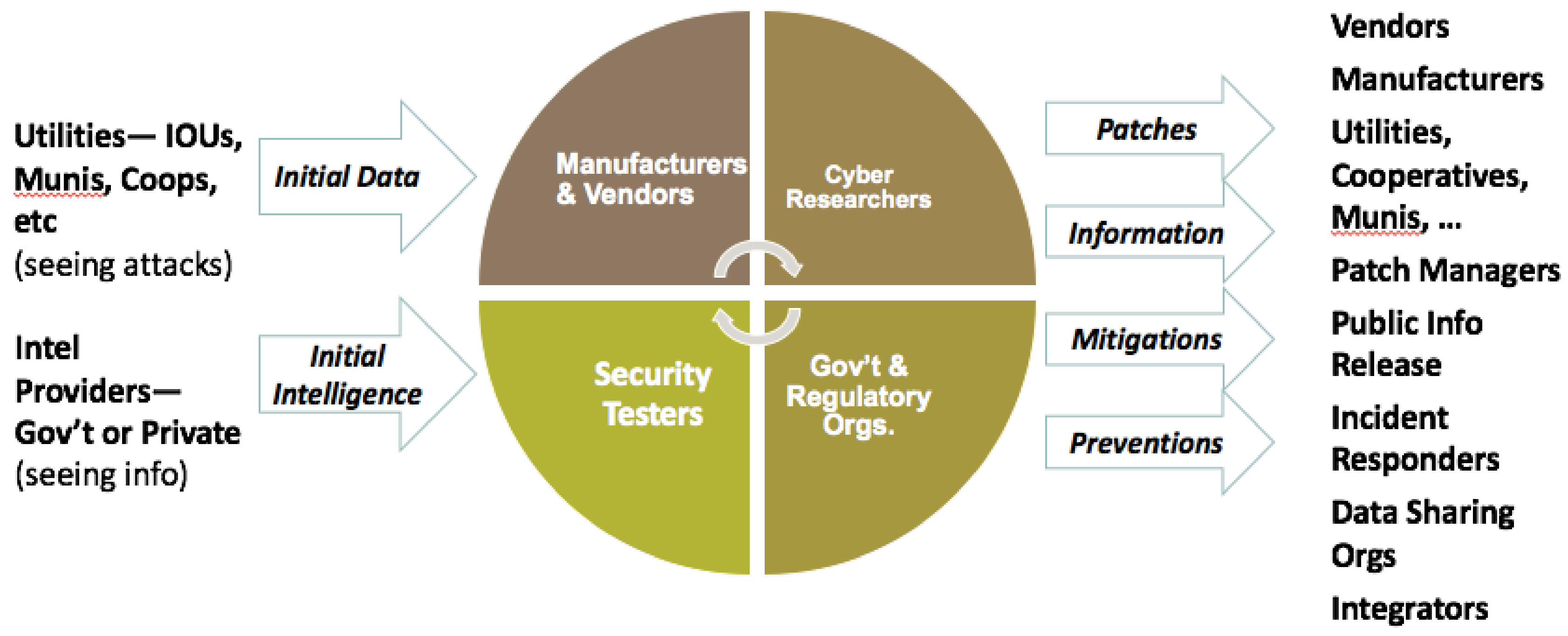
- Valuable time is wasted
- Process can be costly

There is no single coordinating organization that can ensure a timely and comprehensive National mitigation process.

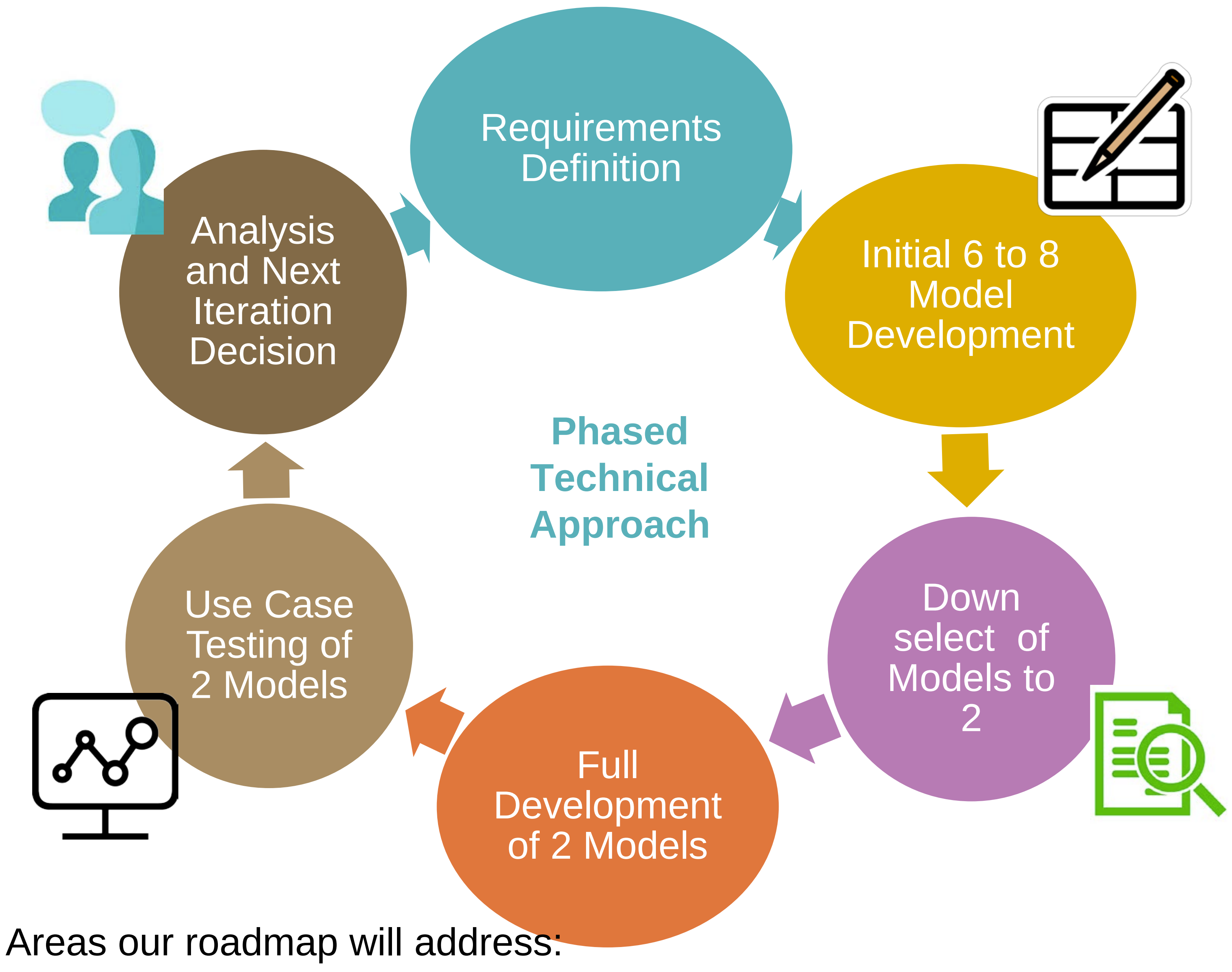
OUR SOLUTION: REMEDYS

Research Exploring Malware in Energy DeliverY Systems (REMEDYS) provides a platform and synchronized actions across the energy sector that assists the members during a cyber event and makes pertinent mitigation processes available.

- **Rapidly recognize malware threats and exploited vulnerabilities**
- **Reduce the risk of damage from malware cyber attack**
- **Quickly propagate the mitigation for malware to stakeholders**



RESEARCH ROADMAP


Requirements Definition
Initial 6 to 8 Model Development
Down select of Models to 2
Full Development of 2 Models
Use Case Testing of 2 Models
Analysis and Next Iteration Decision
Phased Technical Approach

Areas our roadmap will address:

Build a Culture of Cyber Security for the Energy Delivery Ecosystem

- Create a trusted malware-mitigation organization involving each of the stakeholders in the ecosystem which is composed of diverse attitudes, beliefs and values of an organization

Develop and Implement New Protective Measures to Reduce Risk

- Design a successful organizational structure that will enable scalable future relationships in the EDS ecosystem

Sustain Security Improvements

- Build case studies to test and practice how to continuously improve security and to develop organizational models.

SOME RESULTS FROM OUR WORK: TRUST

Requirements of Building Trust Take Time...

- **Expect and provide outstanding performance**
- **Have confidence that organizations will base decisions on more than individual interests.**
- **Share a commitment to cooperate**

For stakeholders to work together to quickly solve a cybersecurity issue, trust must be an integral part of the system's design.

4 REQUIREMENTS OF TRUST

There are **four main requirements** to build trust in relationships. While REMEDYS is about **mitigation sharing, not just information sharing,** the E-ISAC (Electricity Information Sharing and Analysis Center) provides a **useful case study about building trust.**

The E-ISAC enables the electricity industry's sharing of security information and **exhibits the requirements of trust.** This allows stakeholders to:

- Access shared knowledge and experience
- Better manage security resources
- Respond faster to security threats
- Create a stronger, more secure sector ecosystem

***Note:** Though different, REMEDYS will **complement organizations** like the E-ISAC, by providing mitigations, not just information sharing.*

Requirements of Trust	Description	E-ISAC
Clarity and agreement of objectives	• No conflict of interest • Project funding clearly understood and not in conflict with goals of all participants • Power and policies clear and aligned	Leadership and funding provided by NERC, therefore members (industry members, government partners, cross-sector partners) have little power to create conflicts of interest
Clarity about assignments and roles	• Clear commitment and understanding of participant roles (who is expected to do what) • Expectations match abilities of participants	Members and NERC have clear roles and division of work. NERC manages stakeholder engagement, operations. Individual organizations contact E-ISAC for information sharing and receiving information.
Appropriate and clear safeguards	• Formal controls provide a safety net for all participants • Self-interests do not create unsafe environment for other participants	• E-ISAC has built technology safeguards to protect data and flows (backups, monitoring) • Organizational mechanisms and legal documents clarify boundaries for members
Appropriate Confidentiality	• Clarity, alignment and agreement on what can and cannot be shared. • Clear designation of ownership and fair use of contributions (ex. ideas, information, mitigations, etc.)	Confidentiality of partner-shared information through procedures, policy, legal documentation, and other appropriate information management tools

IMPACT ON STATE OF GRID SECURITY

- **Trust is important for the ecosystem to develop and share mitigations needed to solve cybersecurity issues**
- **We believe that organizations who trust each other have an easier way to collaborate, which can reduce the time and expense to solve a cybersecurity issue. (Case studies such as E-ISAC provide useful cases that have lessons to apply to our new opportunity)**
- **Overall, REMEDYS will accelerate the identification, development and availability of solutions for new malware**

NEXT STEPS FOR REMEDYS…

Our broader project is to create a blueprint for REMEDYS. Some of the next steps:

- Define and test organization models for propagating mitigations
  - Define "requirements" of how to build/insure trust of participants
  - Design and test model alternatives
  - Develop use cases to use in discussions with stakeholders

Contact: chojy@mit.edu, kerip@mit.edu
Website: https://cred-c.org/researchactivity/remedys
Collaboration Partners: PNNL, ORNL, DOE, and many stakeholders

CYBER RESILIENT ENERGY DELIVERY CONSORTIUM | CRED-C.ORG

FUNDING SUPPORT PROVIDED BY THE U.S. DEPARTMENT OF ENERGY AND THE U.S. DEPARTMENT OF HOMELAND SECURITY