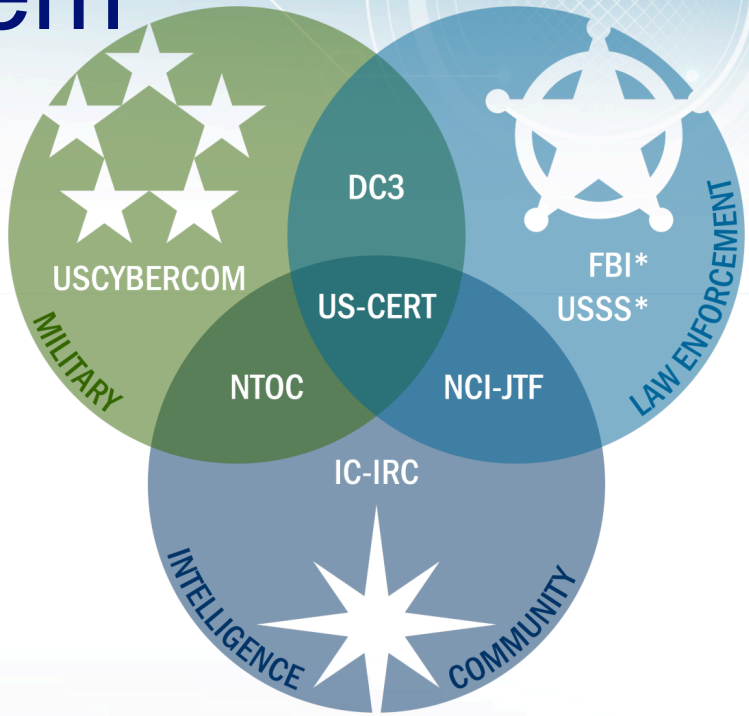
Cross-organizational Incident Handling: Evolving the process model for improved collaboration

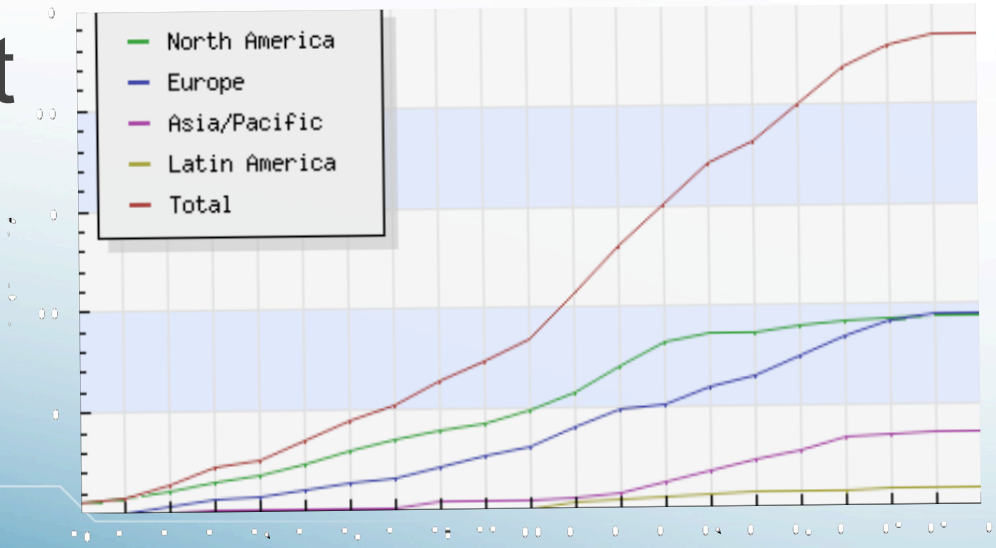
Tom Millar
Chief of Communications

US-CERT
UNITED STATES COMPUTER EMERGENCY READINESS TEAM

Shape of the problem

- >400 partners and constituents
  - public, private, international and domestic
  - diverse capabilities and concerns
- >100,000 incident reports / year

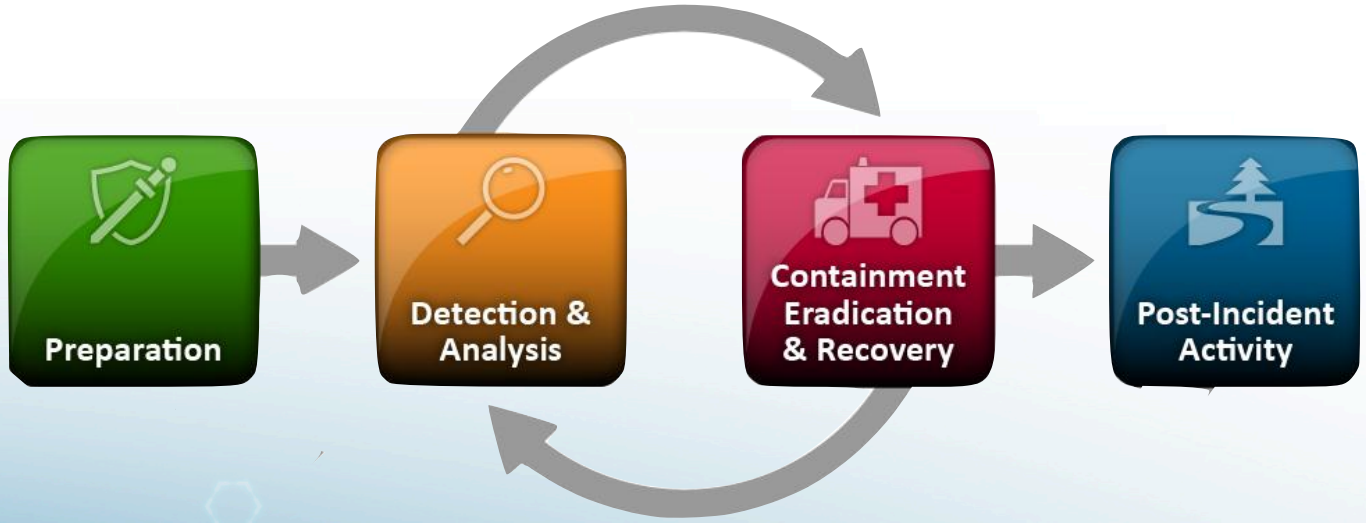




US-CERT
UNITED STATES COMPUTER EMERGENCY READINESS TEAM

Current practices

- Modern cyber incident response in organizations typically follows a variation on a model originally conceived in 1989
- PICERF: Prepare, Identify, Contain, Eradicate, Response, Follow-up



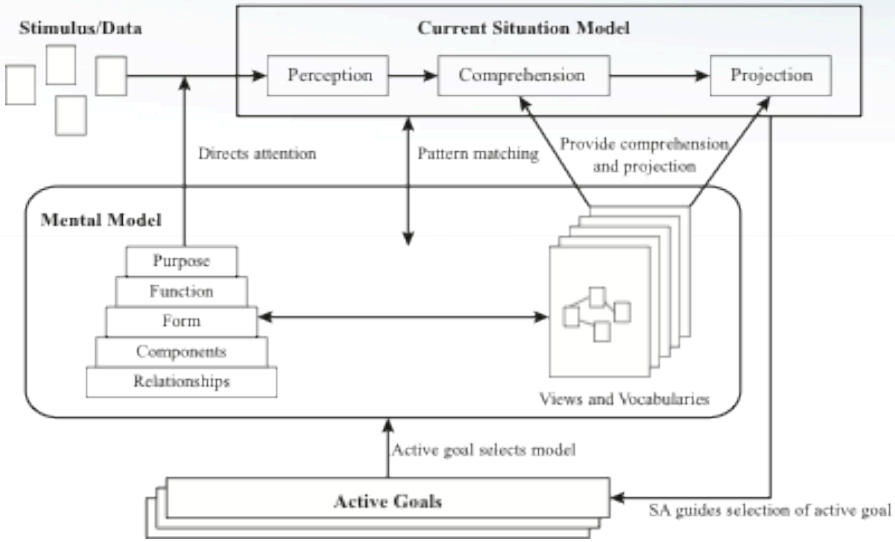
Current practices

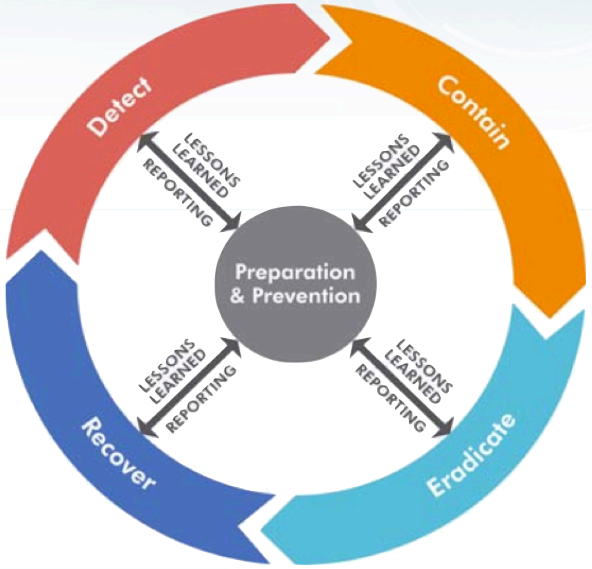
- PICERF doesn't really encourage sharing information and coordinating during the incident handling process
- Most guidance says that teams should share and coordinate with partners, but there's no defined point in the process where coordination occurs
- Unfortunately, in our experience, most sharing seems to happen at the end (during or after the recovery/follow-up phases)

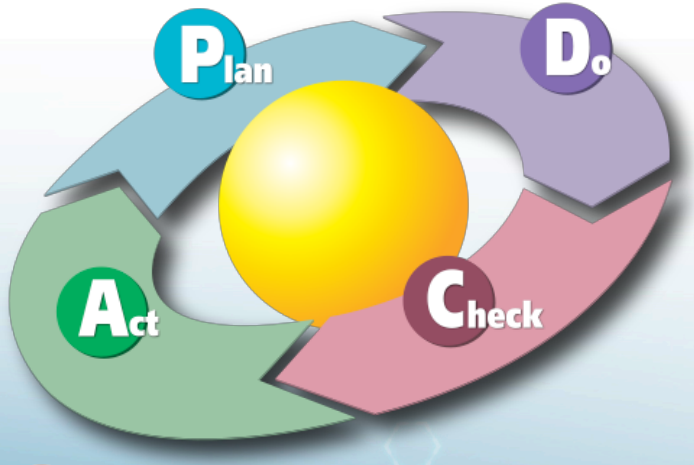
Our needs today

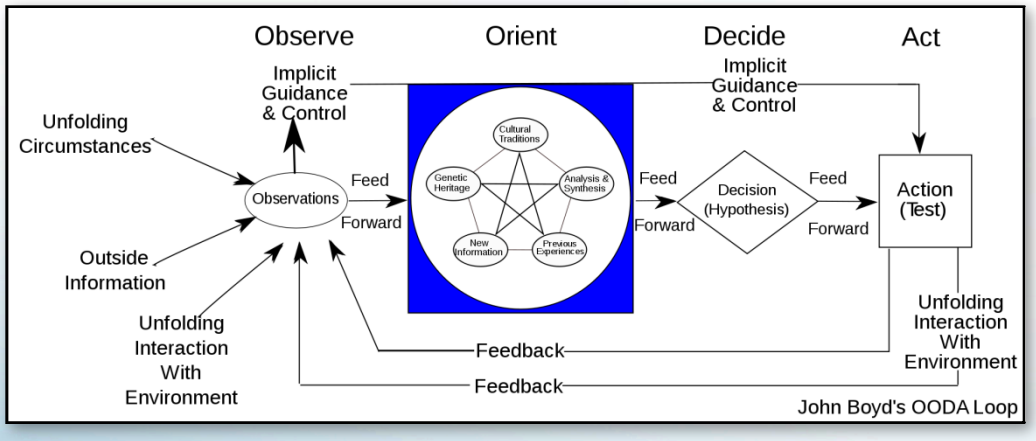
- Sharing the right information with the right partners at the right time
- Understanding partners' information needs, expectations and abilities
- Staying up-to-date and agile

Decision Cycles vs. "Workflow"





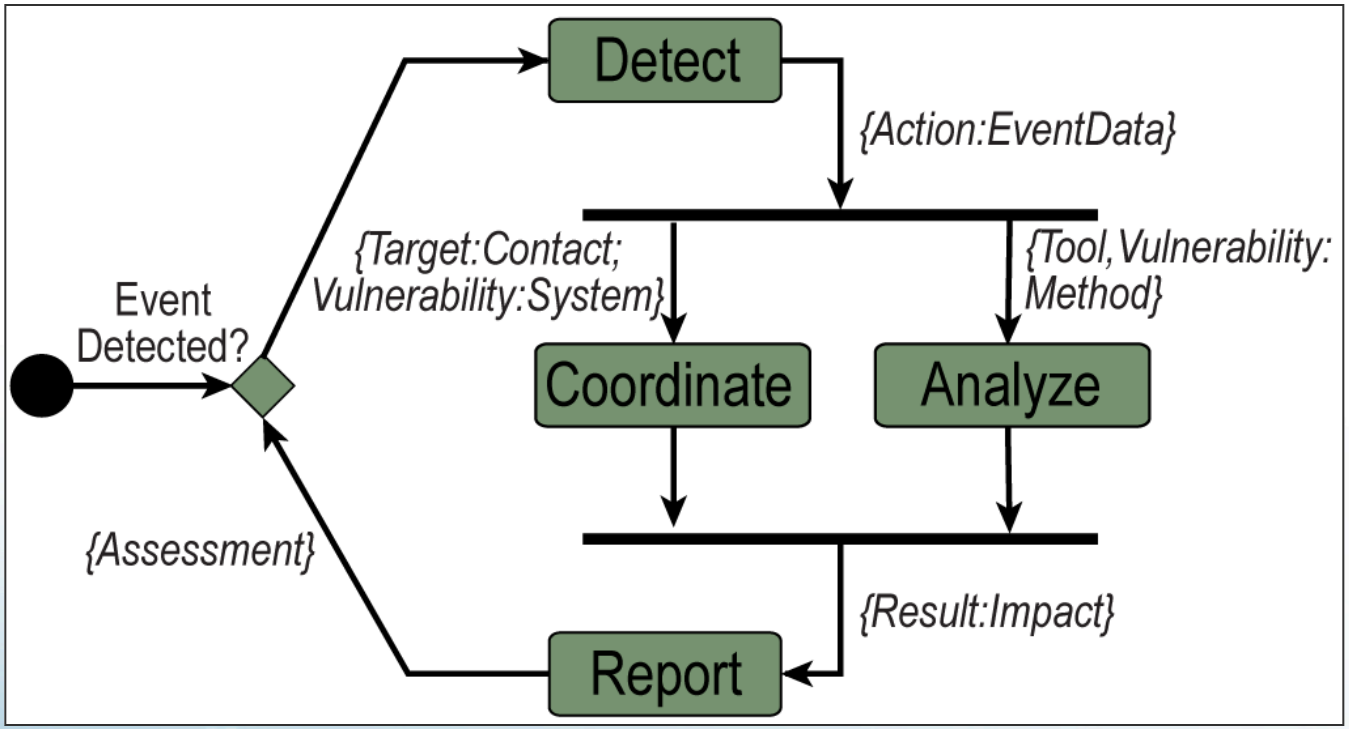




US-CERT
UNITED STATES COMPUTER EMERGENCY READINESS TEAM

Step One: Identify

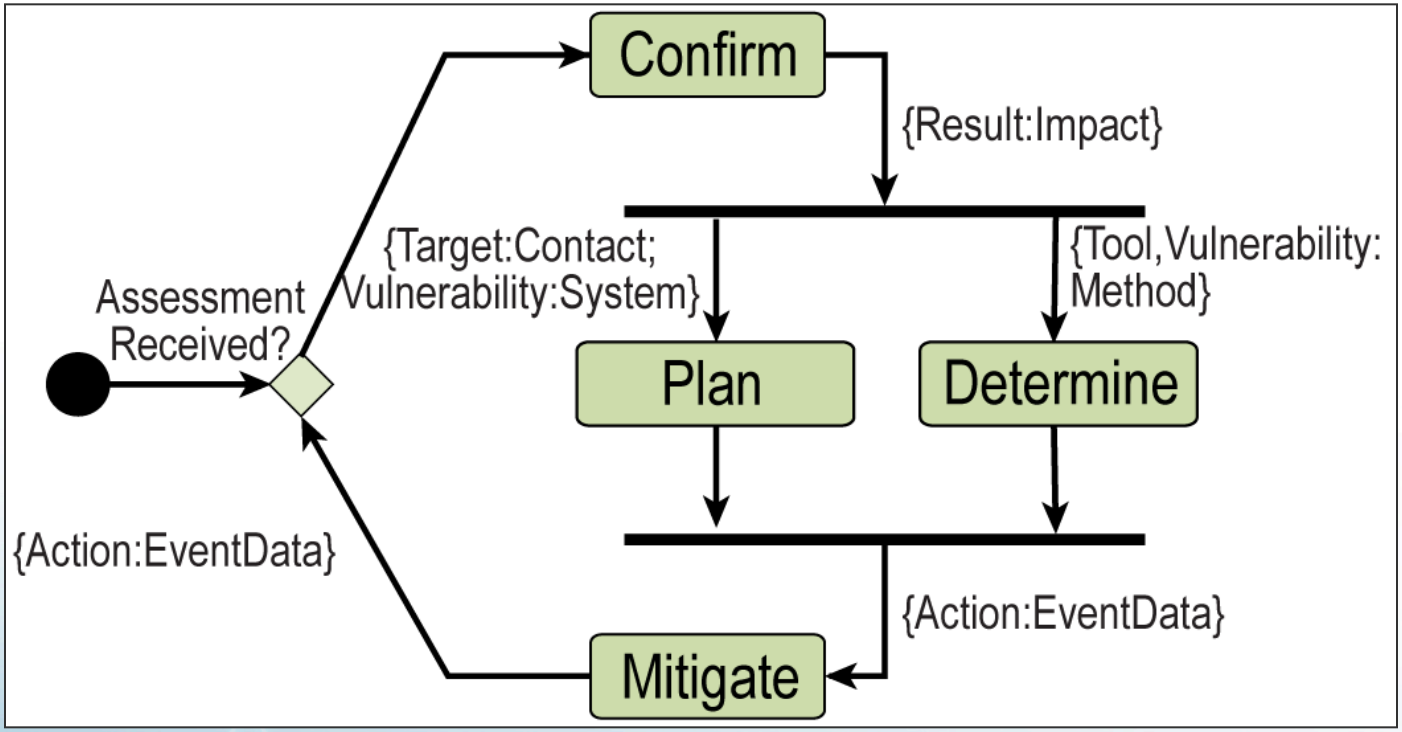
Triage process: detect, analyze and categorize an event, or “observe, orient”



US-CERT
UNITED STATES COMPUTER EMERGENCY READINESS TEAM

Step Two: Respond

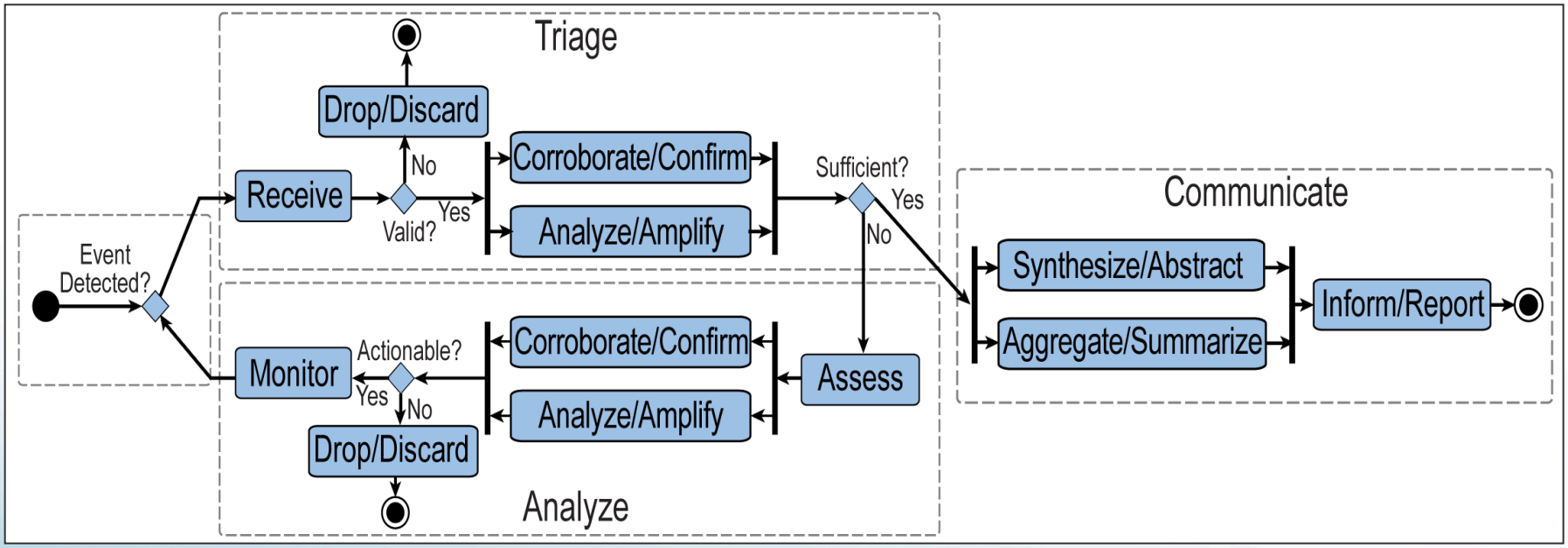
Execution process, or “Plan, Do, Check, Act”



US-CERT
UNITED STATES COMPUTER EMERGENCY READINESS TEAM

Coordination Cycle

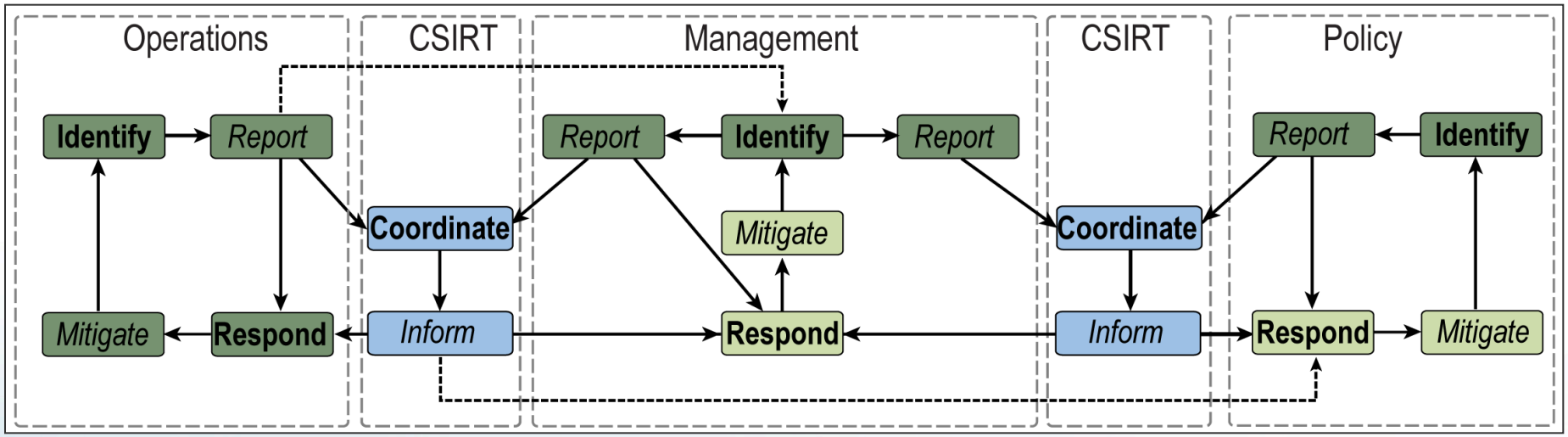
Triage events, communicate consequences, and enable the necessary analysis & response



US-CERT
UNITED STATES COMPUTER EMERGENCY READINESS TEAM

Multi-Level Coordination

Multiple coordinating organizations exist, and for different purposes at different levels



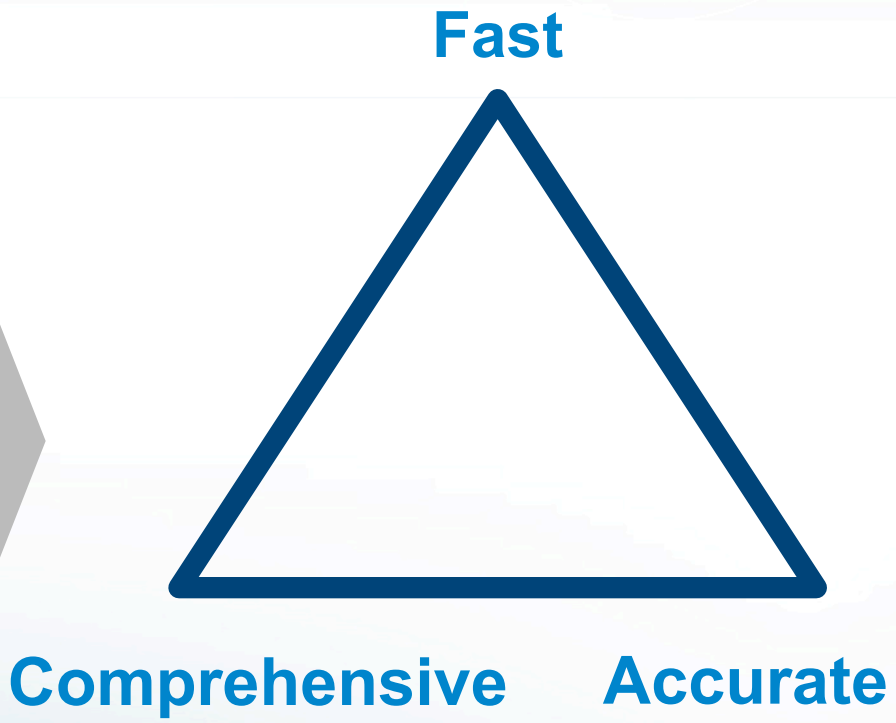
US-CERT
UNITED STATES COMPUTER EMERGENCY READINESS TEAM

Applying the model - Roles

- Identification:
  - Ops = Report on local impact
  - CSIRT = Analyze with historical context
  - Management = Understand consequences

- Respond cycle:
  - Management = Allocate resources
  - CSIRT = Develop recommendations
  - Ops = Remediate based on recommendations

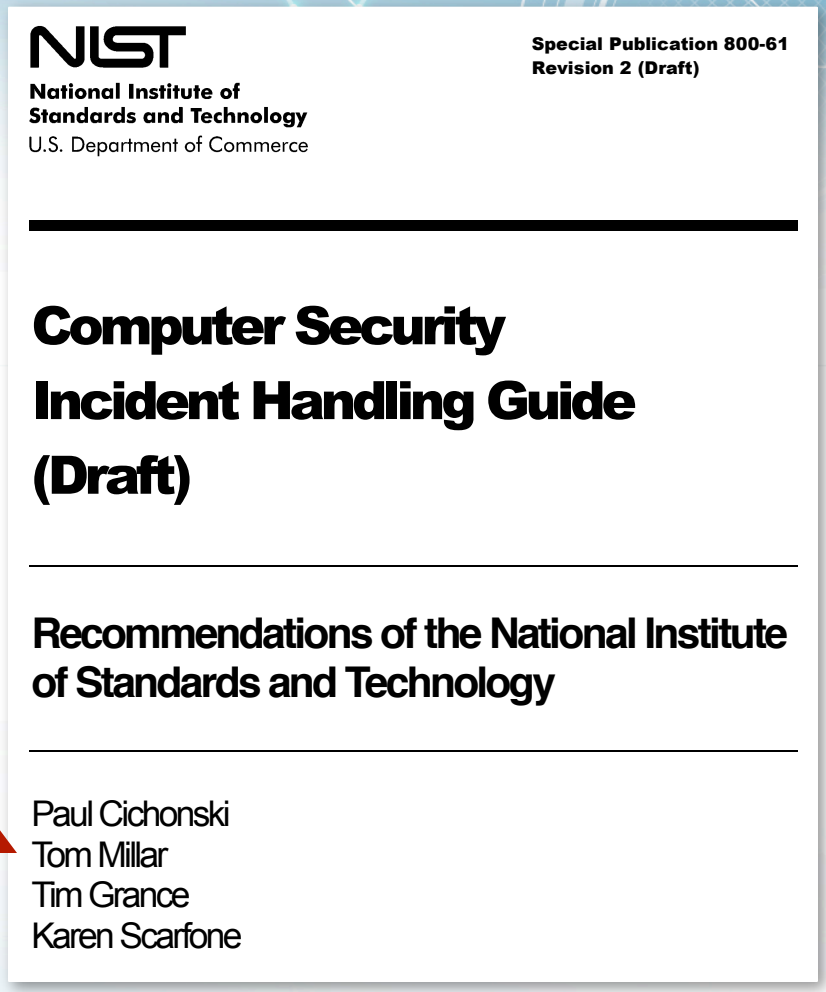
Applying the model - Needs



US-CERT
UNITED STATES COMPUTER EMERGENCY READINESS TEAM

Future work

US-CERT has used this model to re-write its internal Concept of Operations (CONOPS). We are also incorporating aspects of the work into guidance documents for our partners!


NIST
National Institute of Standards and Technology
U.S. Department of Commerce

Special Publication 800-61
Revision 2 (Draft)

Computer Security Incident Handling Guide (Draft)

Recommendations of the National Institute of Standards and Technology

Paul Cichonski
Tom Millar
Tim Grance
Karen Scarfone

The model should inform training, business procedures, and tool development - and each of these takes time!

US-CERT
UNITED STATES COMPUTER EMERGENCY READINESS TEAM

Homeland Security