Coordinated Cybersecurity Incident Handling

Marcos Osorno, Thomas Millar, Danielle Rager

Presented by: Marcos Osorno marcos.osorno@jhuapl.edu
Johns Hopkins University Applied Physics Laboratory
ICCRTS 2011

US-CERT
UNITED STATES COMPUTER EMERGENCY READINESS TEAM

APL

What are we trying to do?

Inform the design of a domestic federal network defense cybersecurity incident handling system by creating a coordinated, distributed incident handling process.

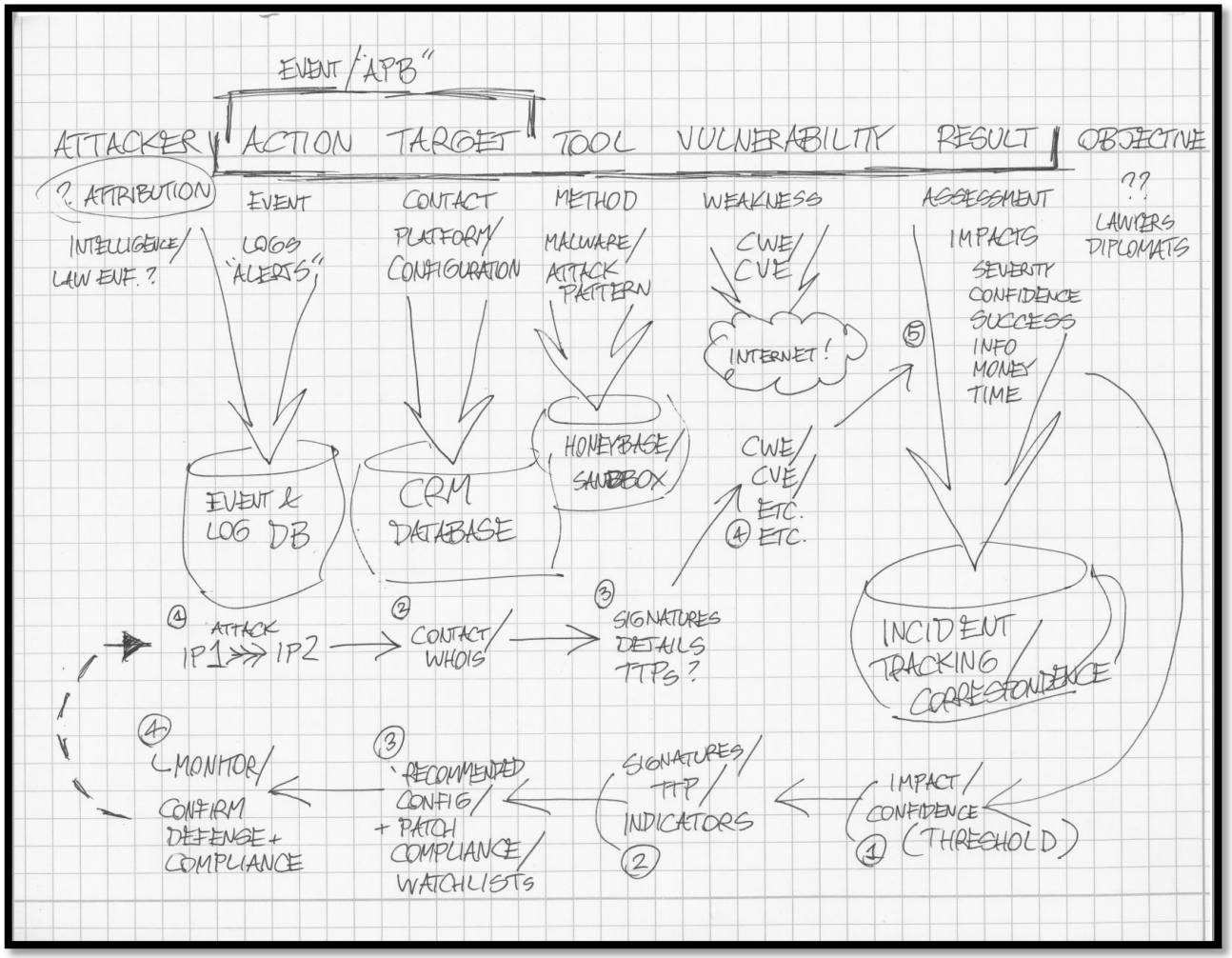
US-CERT + NIST + JHU/APL

What are we trying to do?

Inform the design of a domestic federal network defense cybersecurity incident handling system by creating a **coordinated, distributed incident handling process.**

US-CERT + NIST + JHU/APL

Where did we start?



What did we do?

Inform the design of a domestic federal network defense cybersecurity incident handling system*by creating a coordinated, distributed incident handling process.

elements, interconnections, and purpose

Concepts, Data, Systems

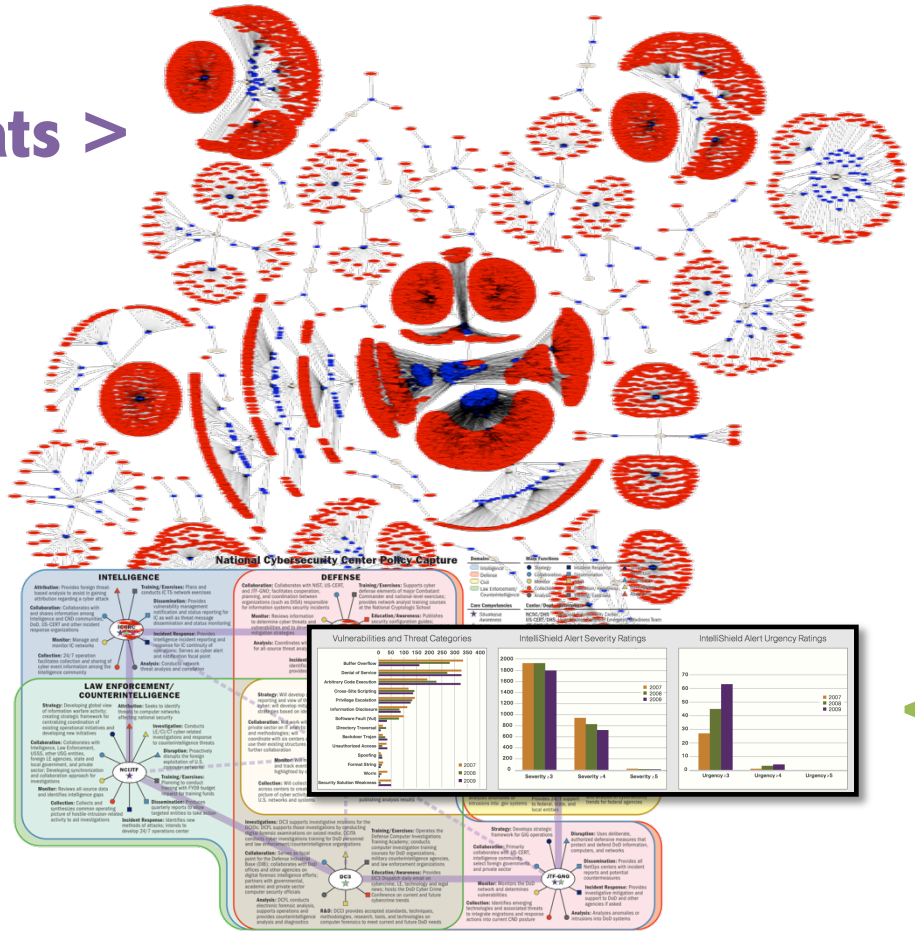
Activities & Processes

Federal-civil network defense

[*] Meadows, *Thinking in Systems*

Complexity & Heterogeneity

complex threats >



cyber centers >

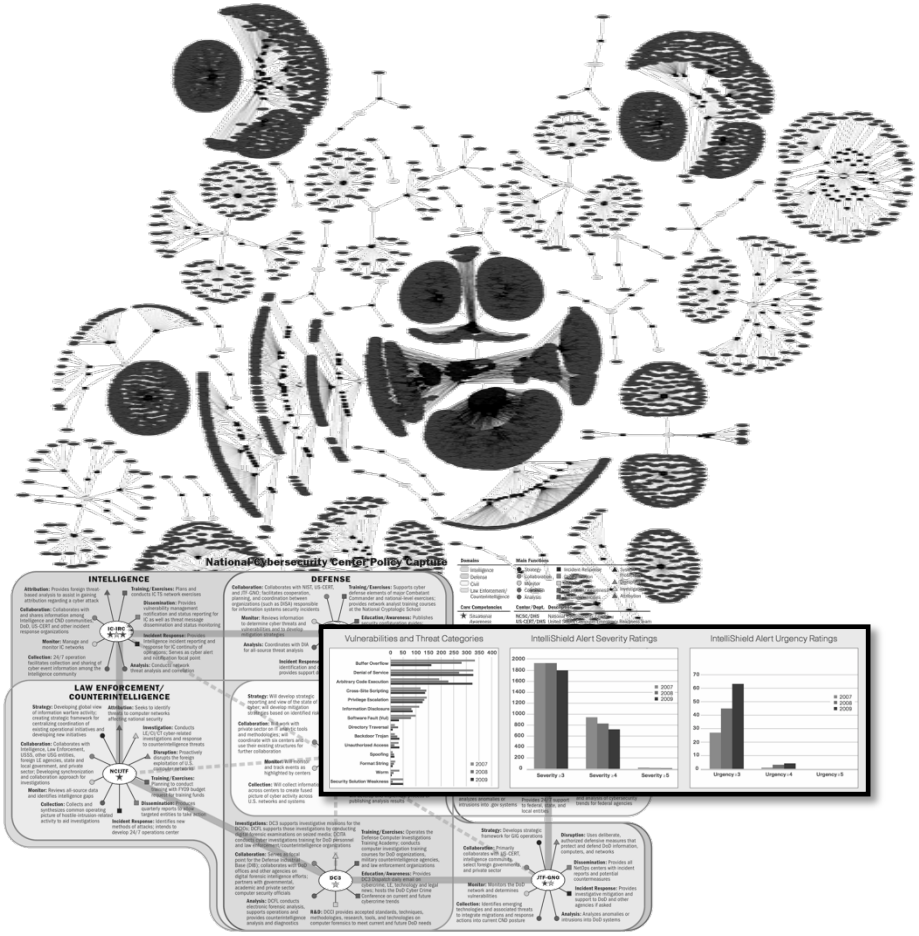
< threat types

Visualizing Waledac http://www.sudosecure.net/archives/429

US-CERT
UNITED STATES COMPUTER EMERGENCY READINESS TEAM

APL

Scale & Diversity



United States Government

1.9 million federal employees

1.25 million in federal civil sector

100+ department and agencies

208 thousand in largest dept

4 thousand in smallest dept

80.4% in IS/IT dependent work

354 million ft² in 8,600 buildings

2,758 access points (2008)

16,843 incident reports in 2008

206% increase from 2006

US-CERT

UNITED STATES COMPUTER EMERGENCY READINESS TEAM

APL

Current Incident Handling Processes

2004: US National Institute of Standards and Tech.

Background

1990: Lawrence Livermore National Labs

2004: US National Institute of Standards and Tech.

Current Trends

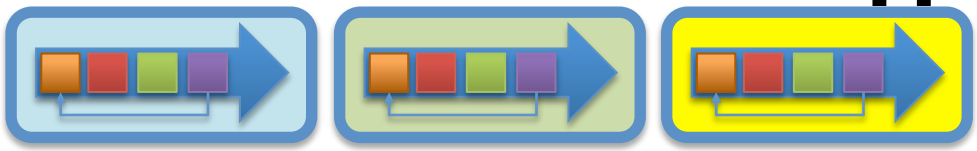
1990: Lawrence Livermore National Labs

2004: US National Institute of Standards and Tech.

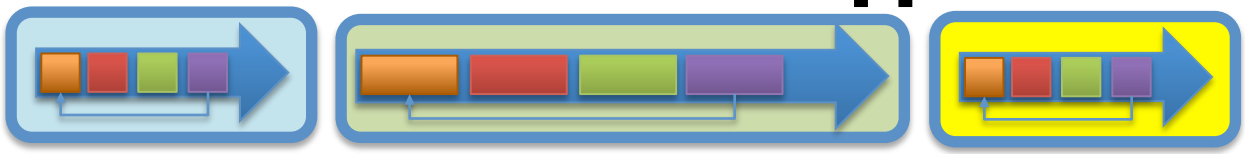
2009: Chairman of the Joint Chiefs of Staff

What about multiple incidents?

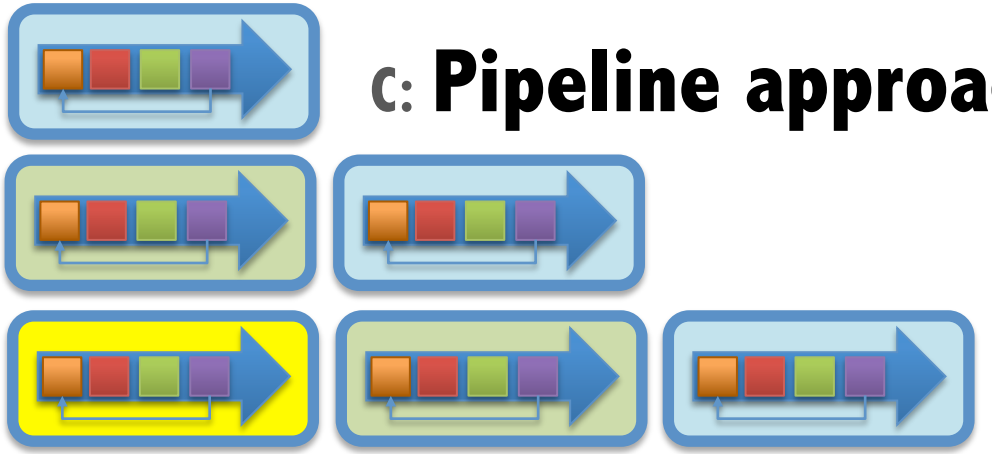
A: Serial constant time approach



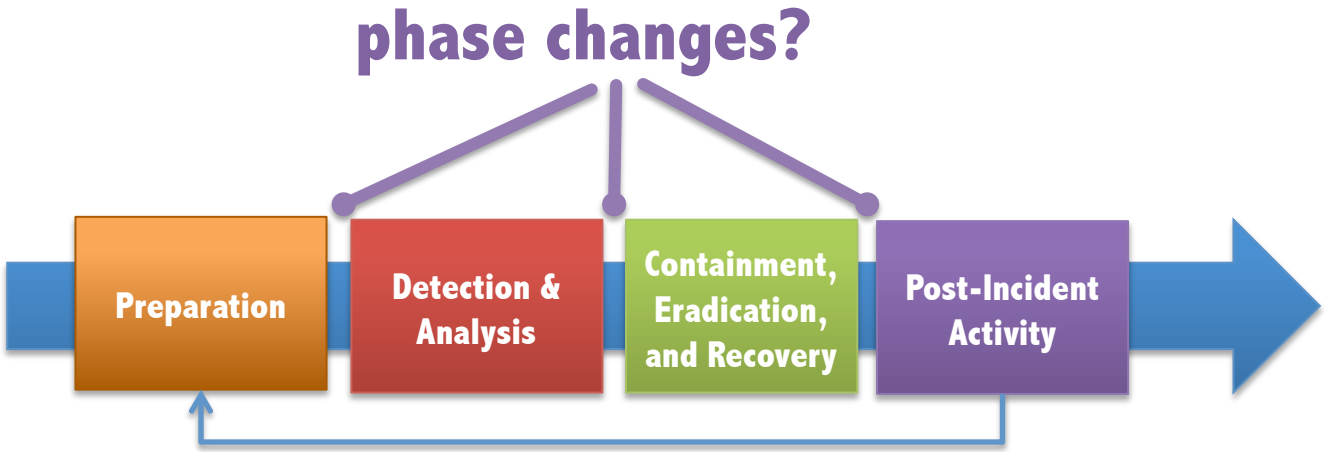
B: Serial variable time approach

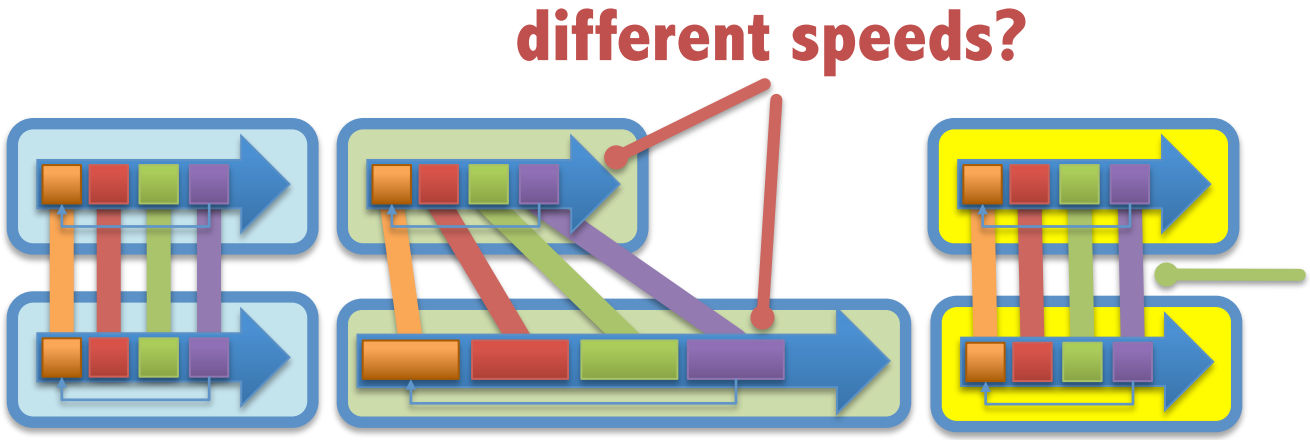


C: Pipeline approach



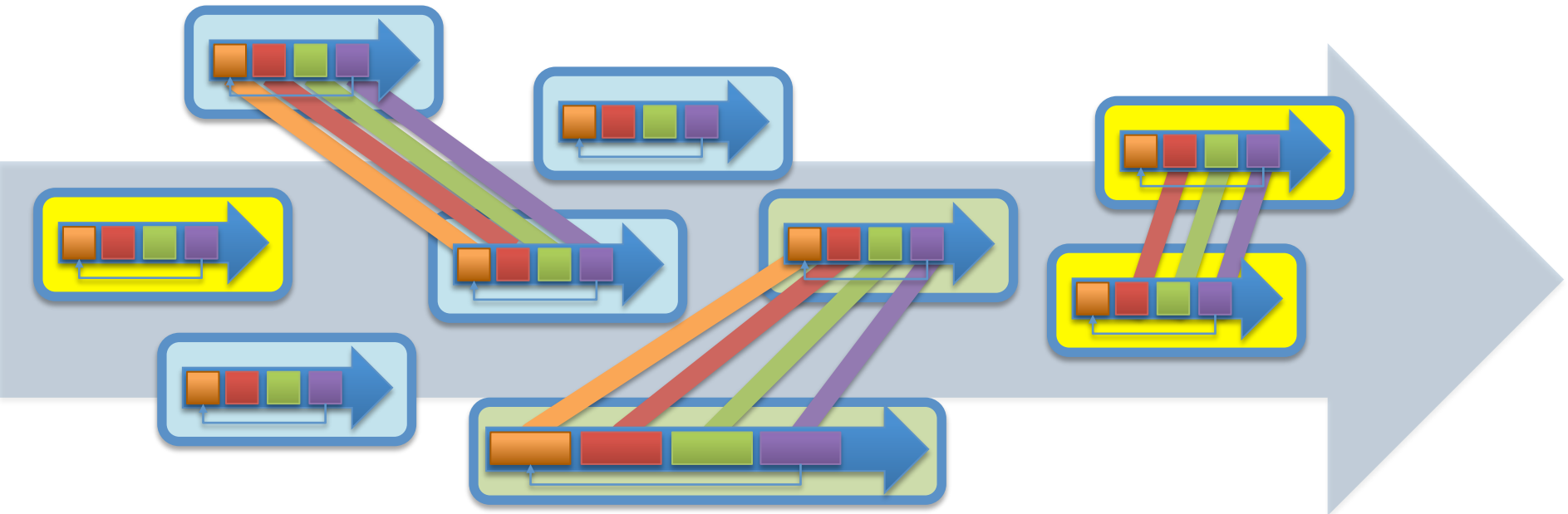
What about cross-cutting incidents?





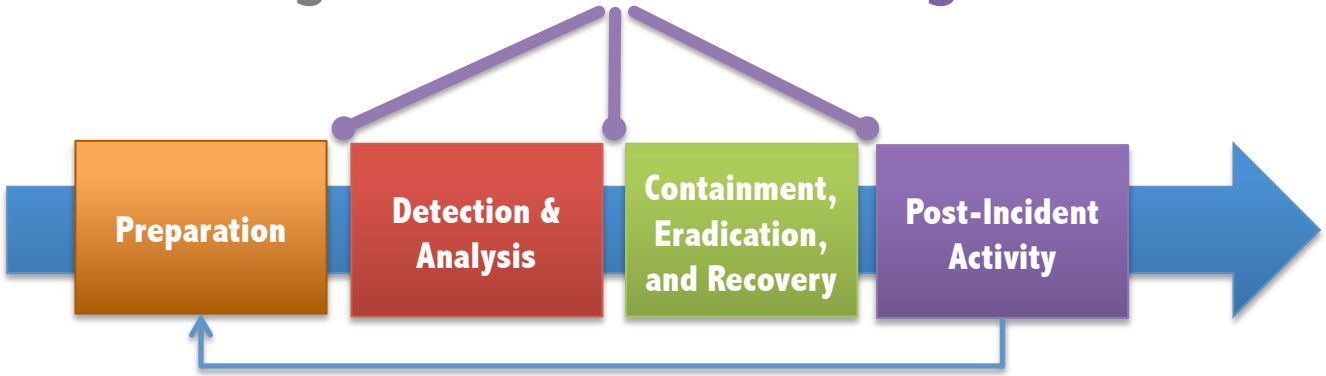
information and sharing?

So how could we deal with it?

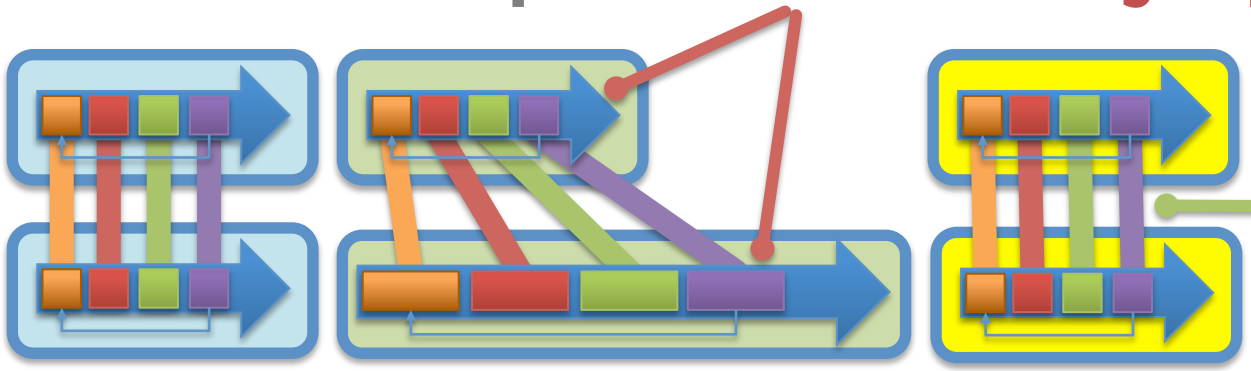


Three broad answers

phase changes? focus on handling activities not an incident



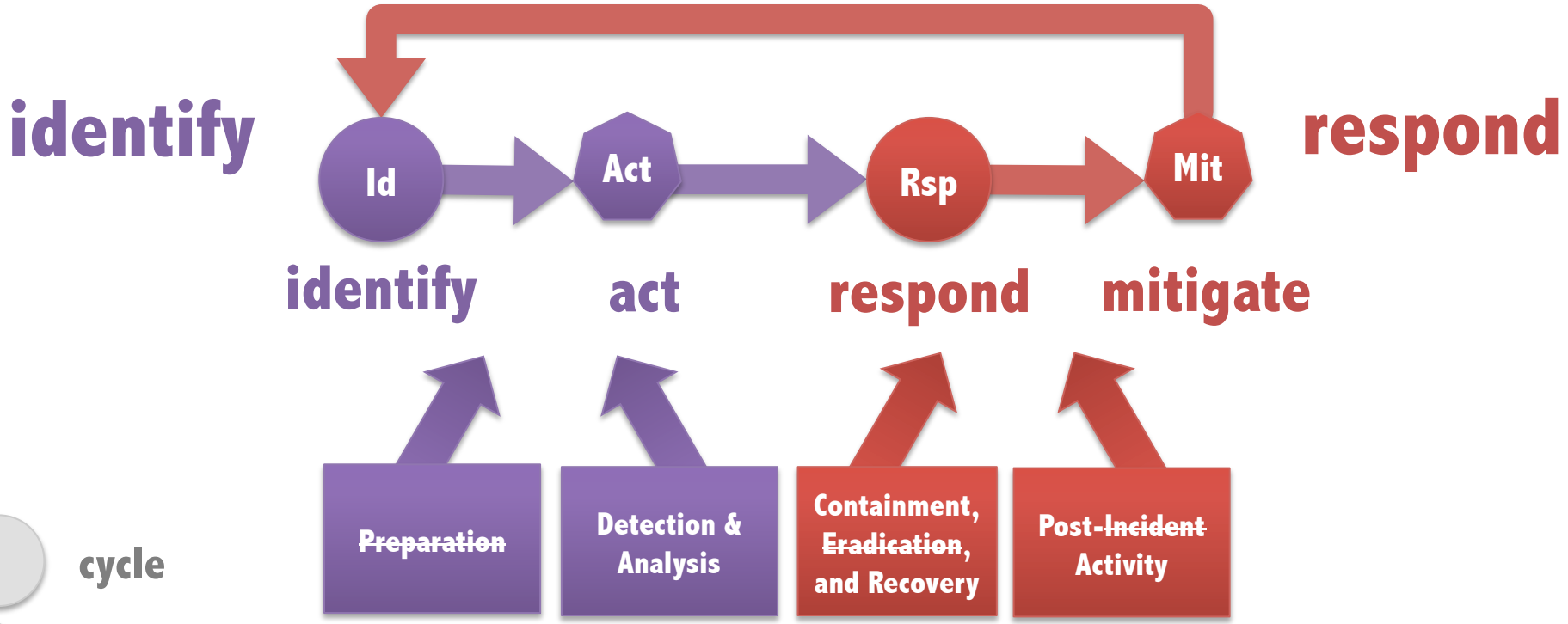
different speeds? reduce locking dependencies



information and sharing? standard data, common activities

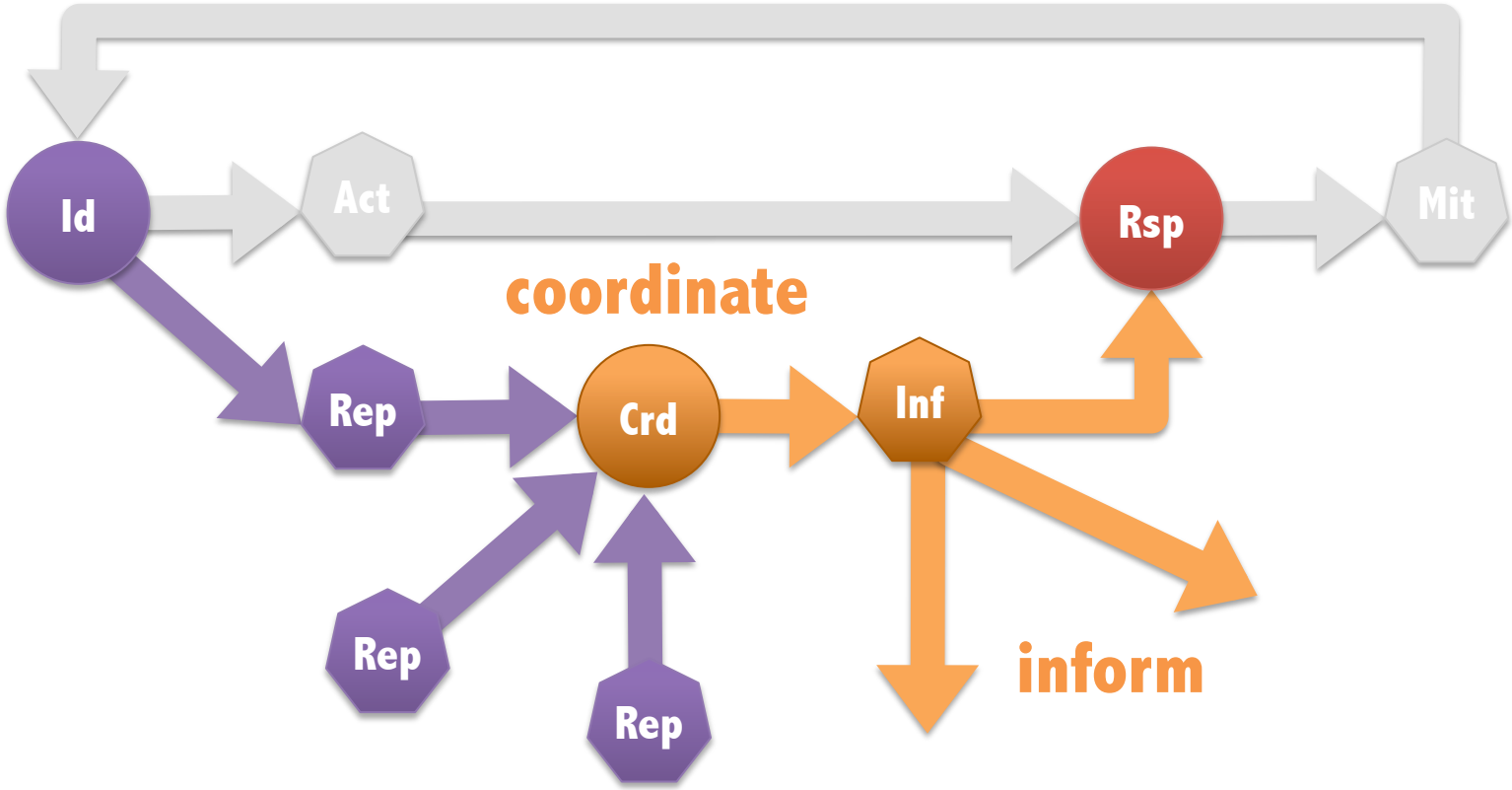
1. Focus on activities

phase changes? focus on handling activities not an incident

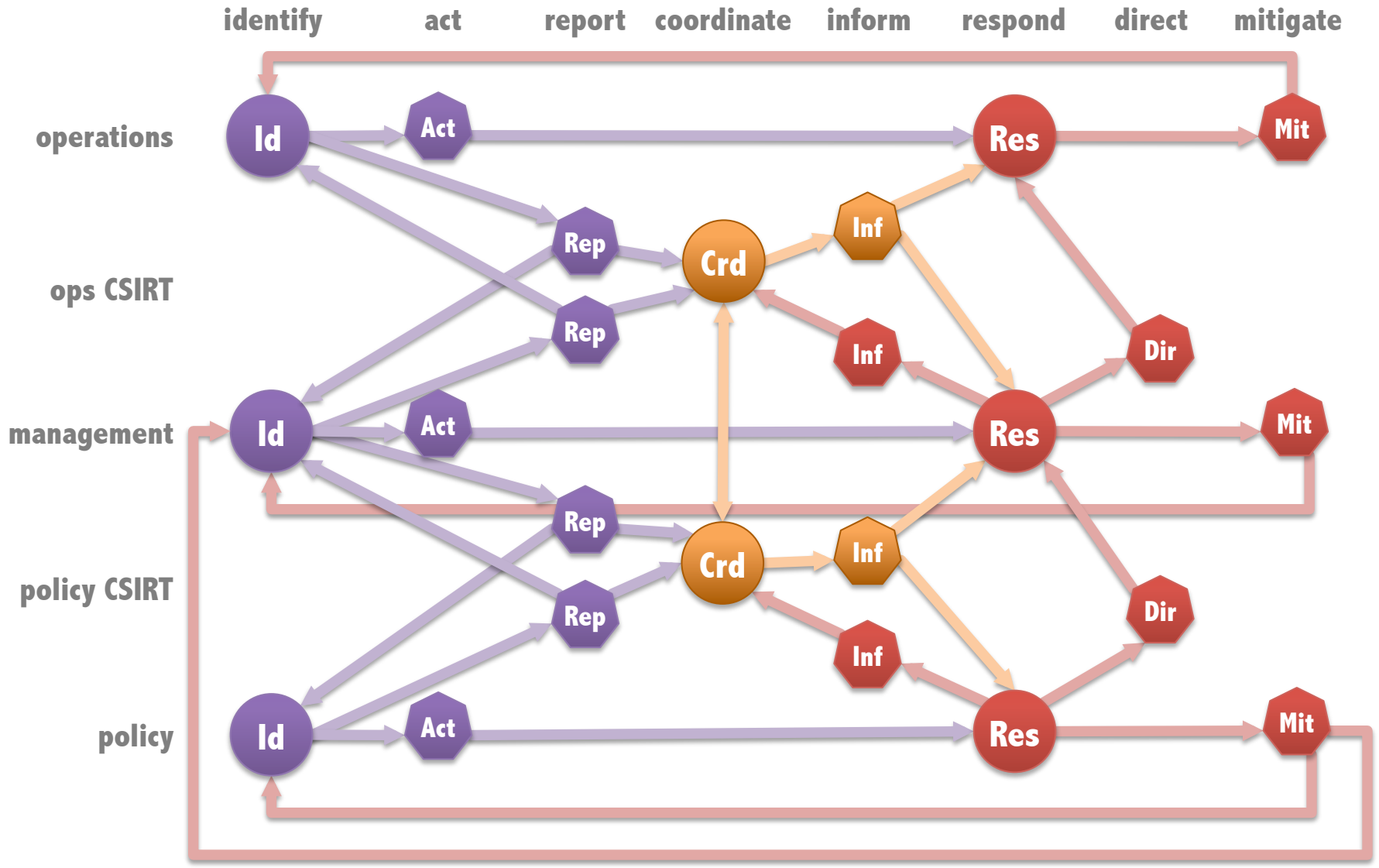


2. Reduce locking dependencies

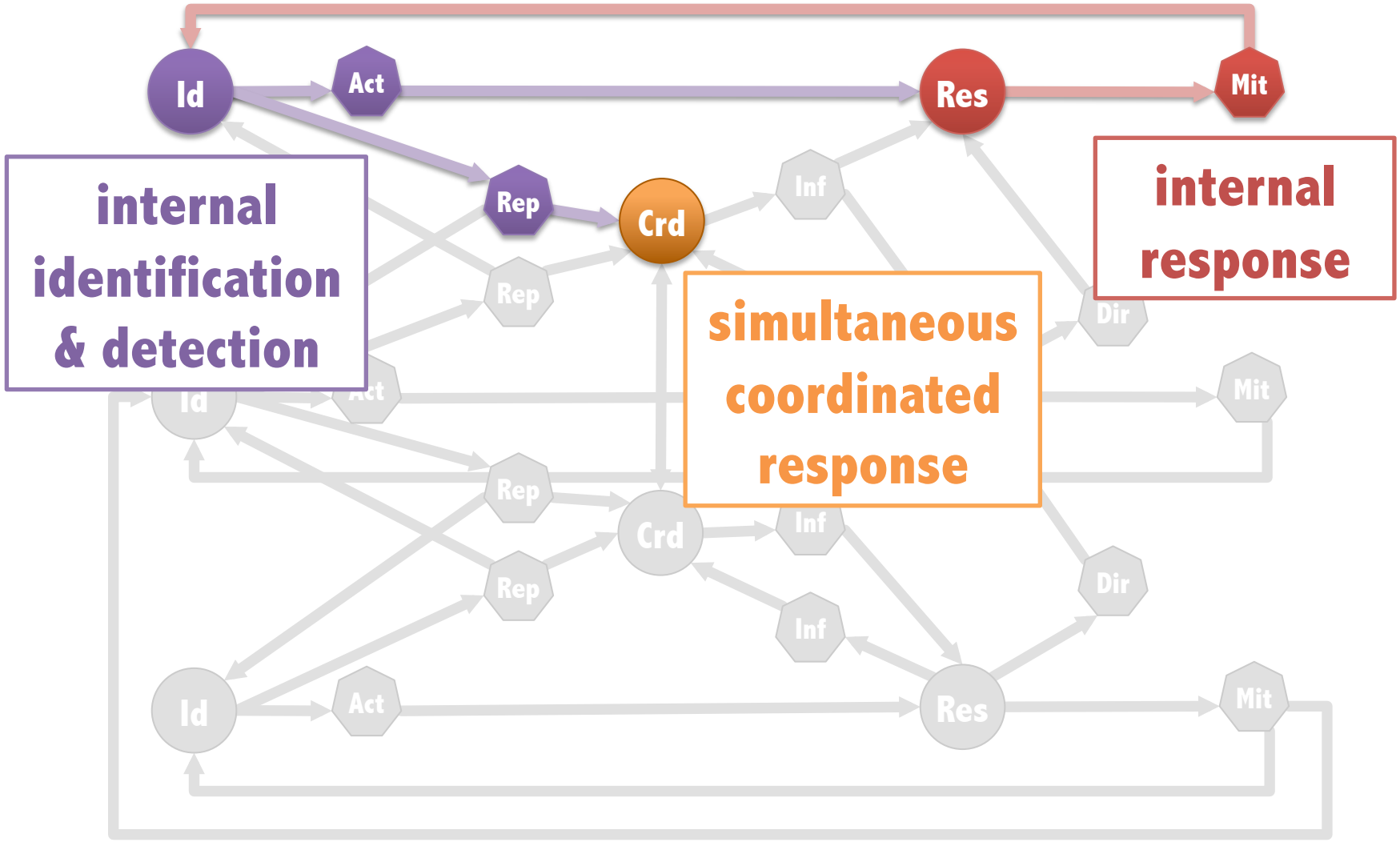
different speeds? reduce locking dependencies



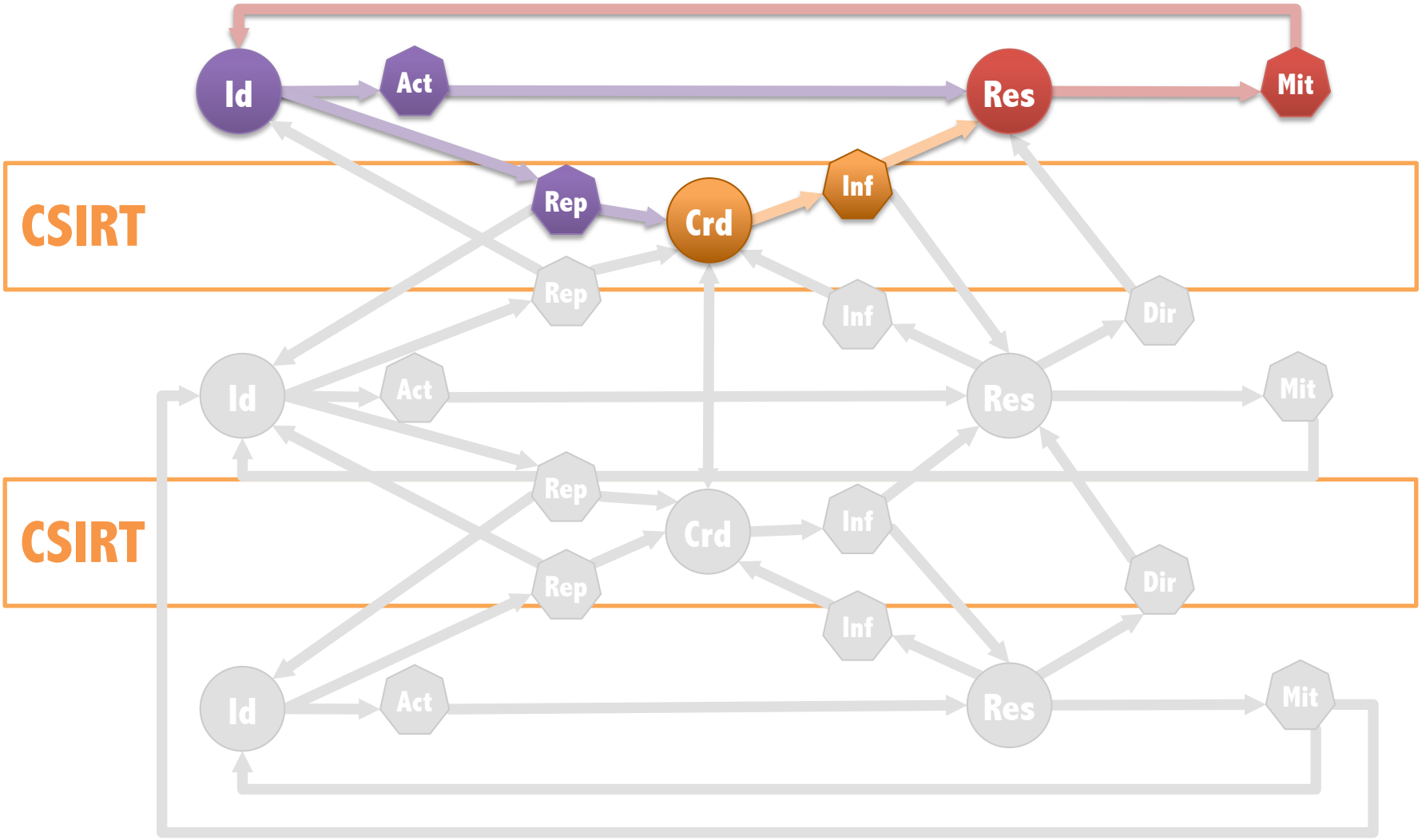
Which: allows for complex system



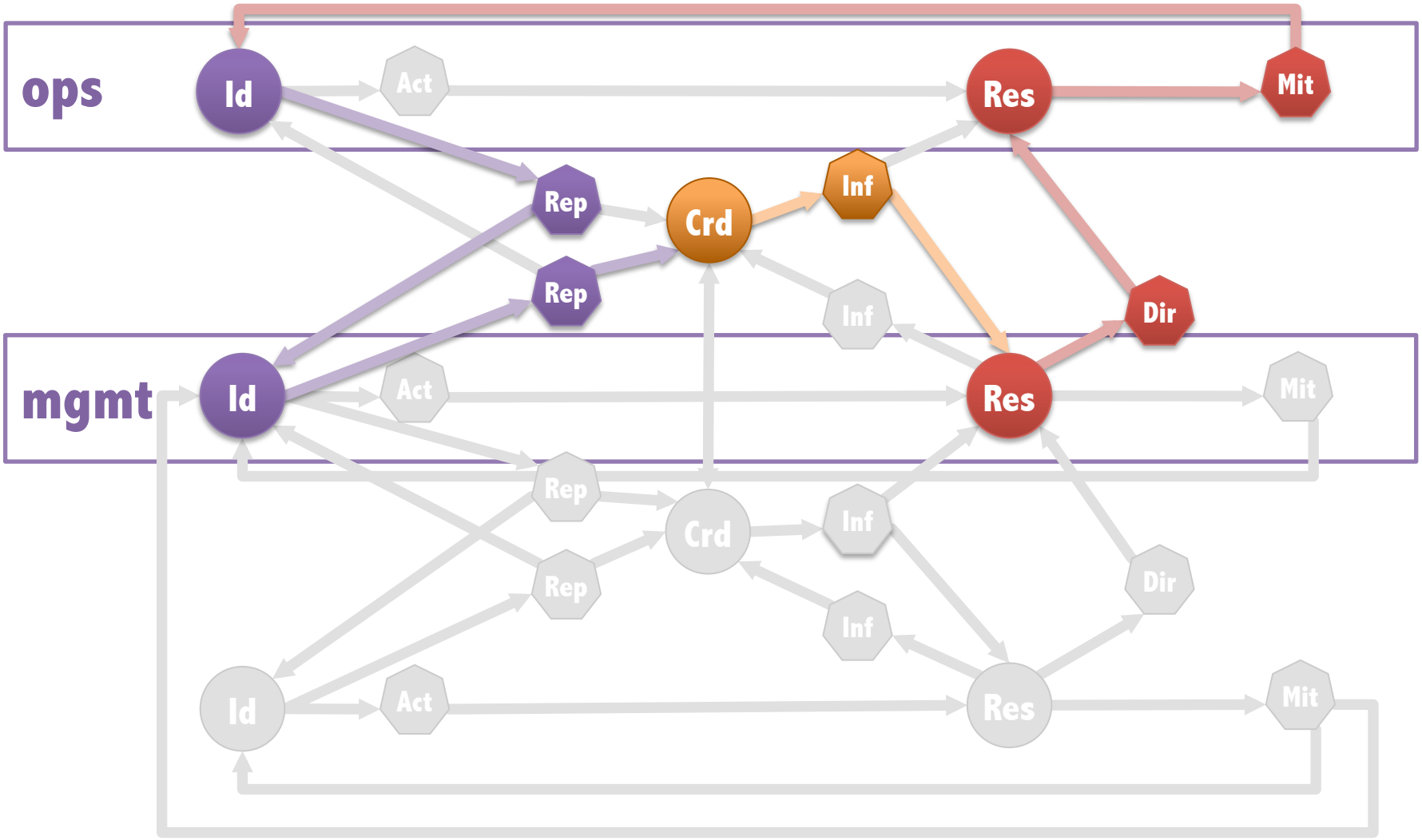
Allows for multiple, concurrent flows



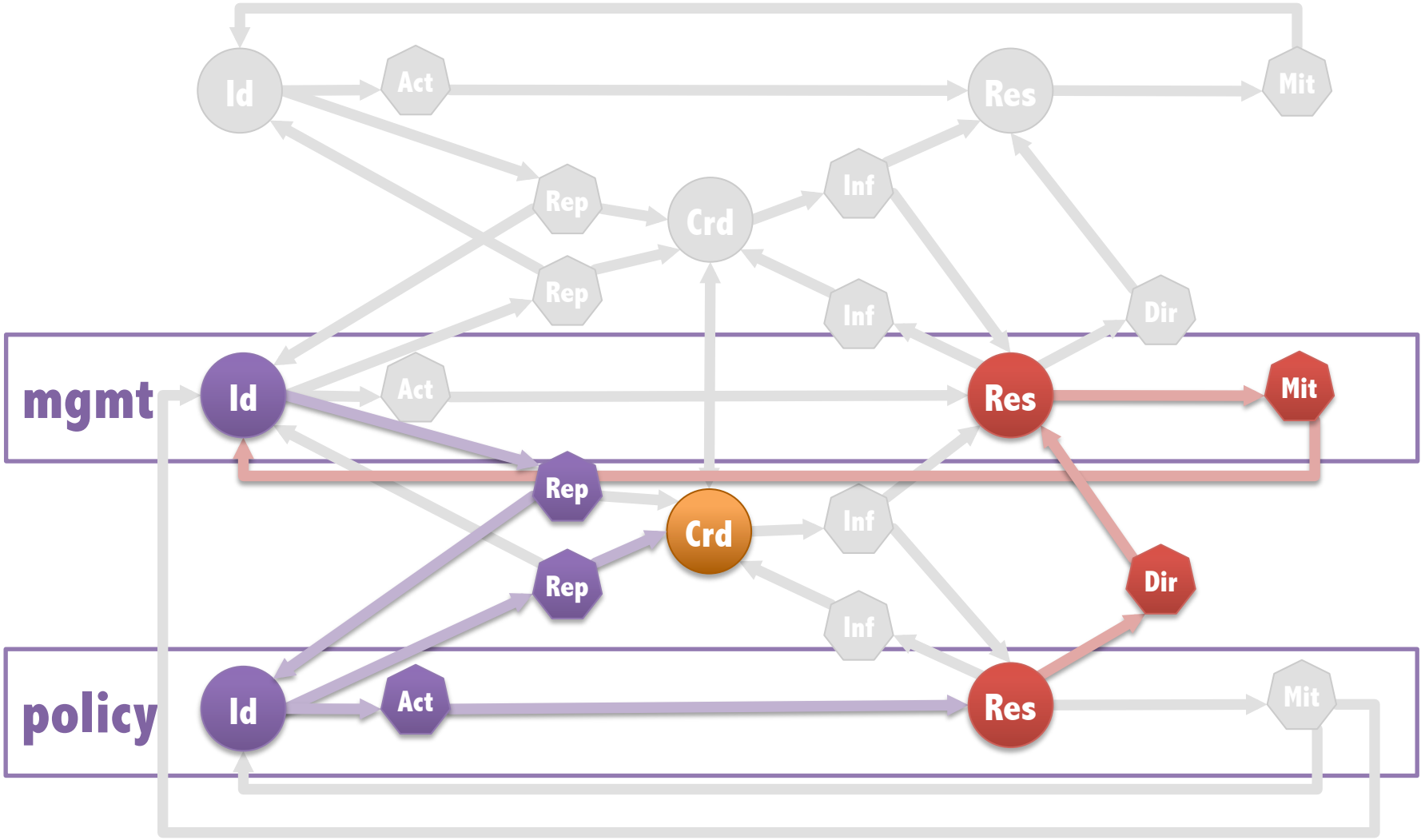
Accounts for role of CSIRT



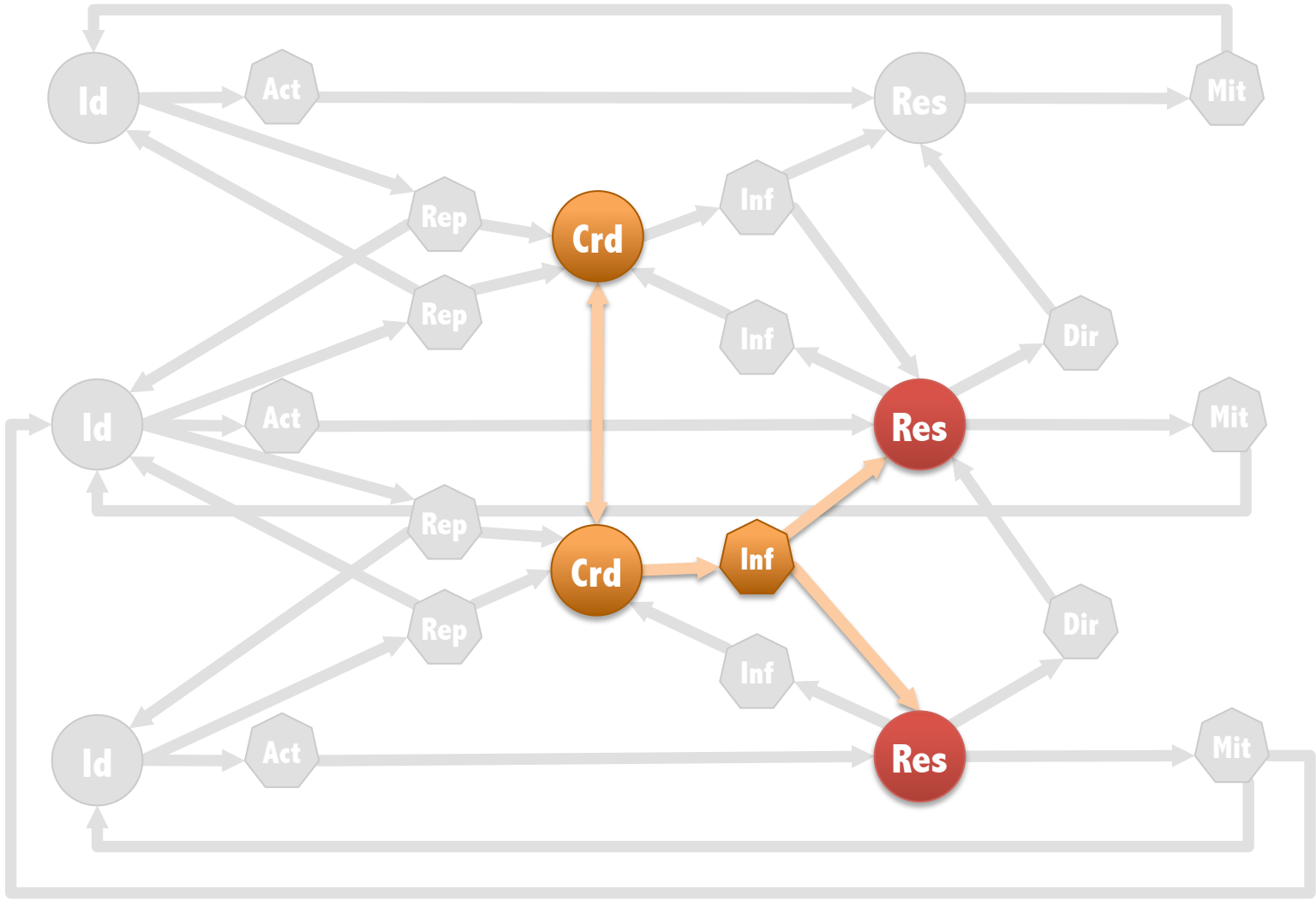
Allows for integration of management



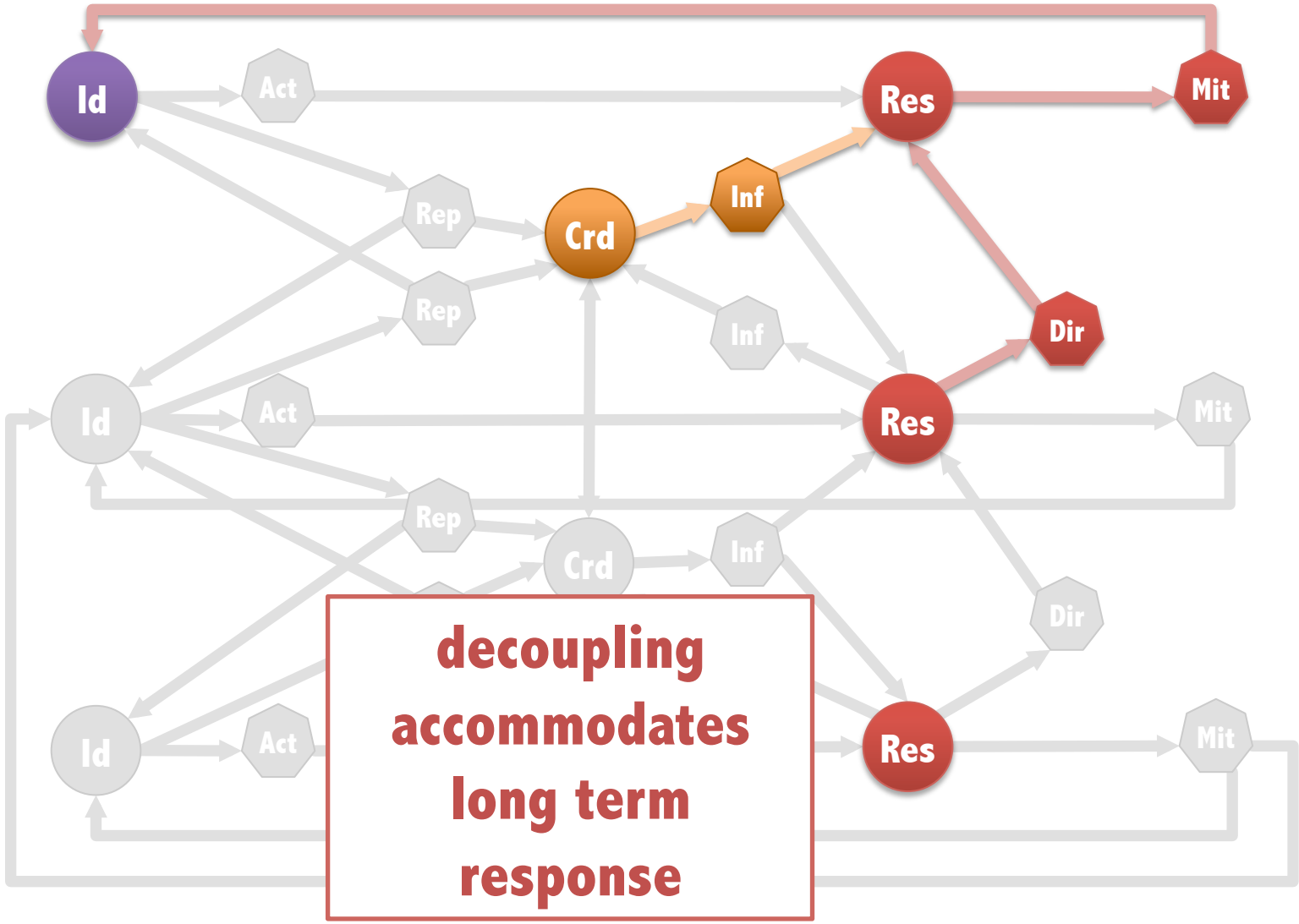
Allows for integration of policy



Uses CSIRTs to drive dissemination

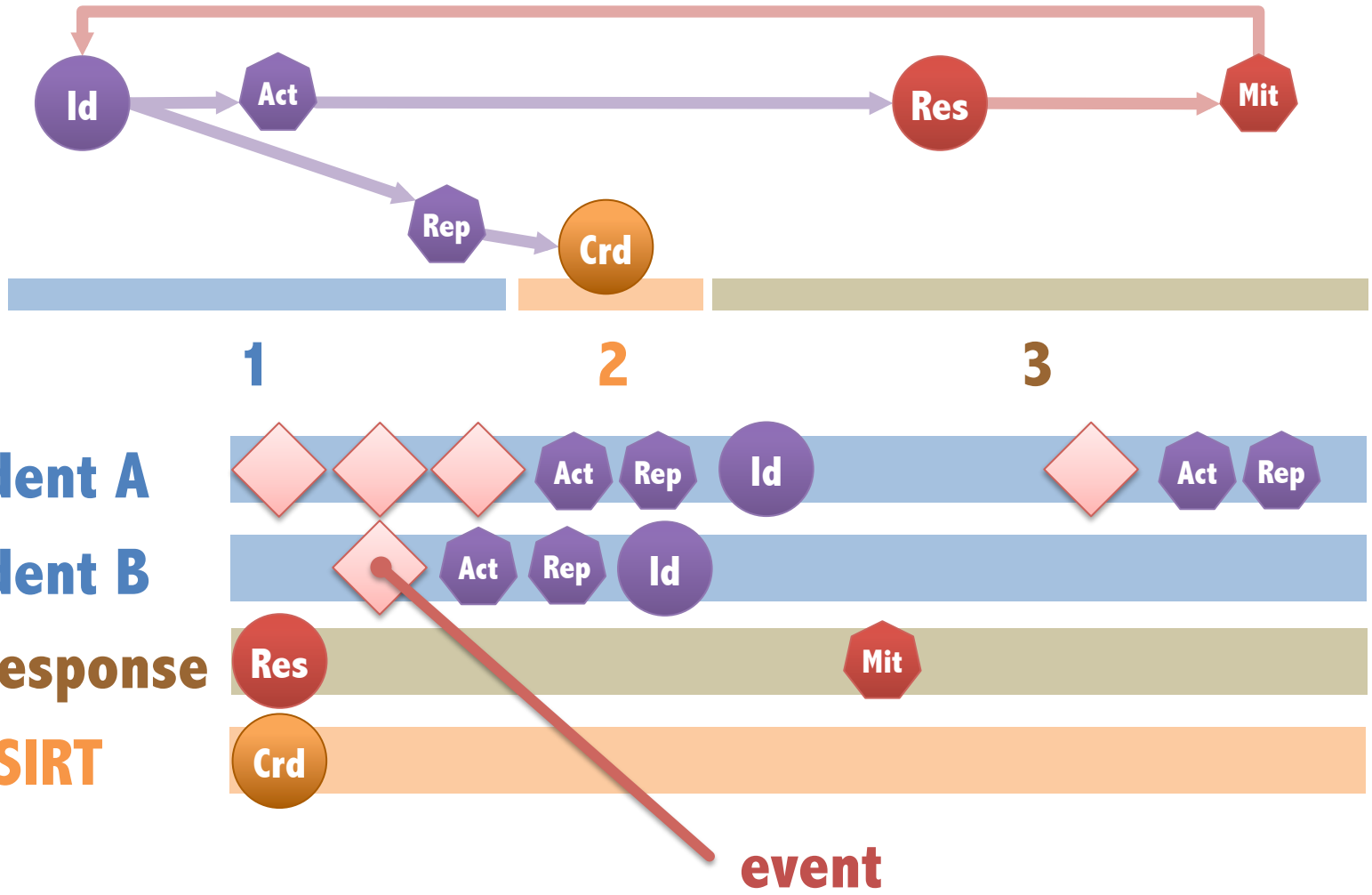


And accounts for long-term impact



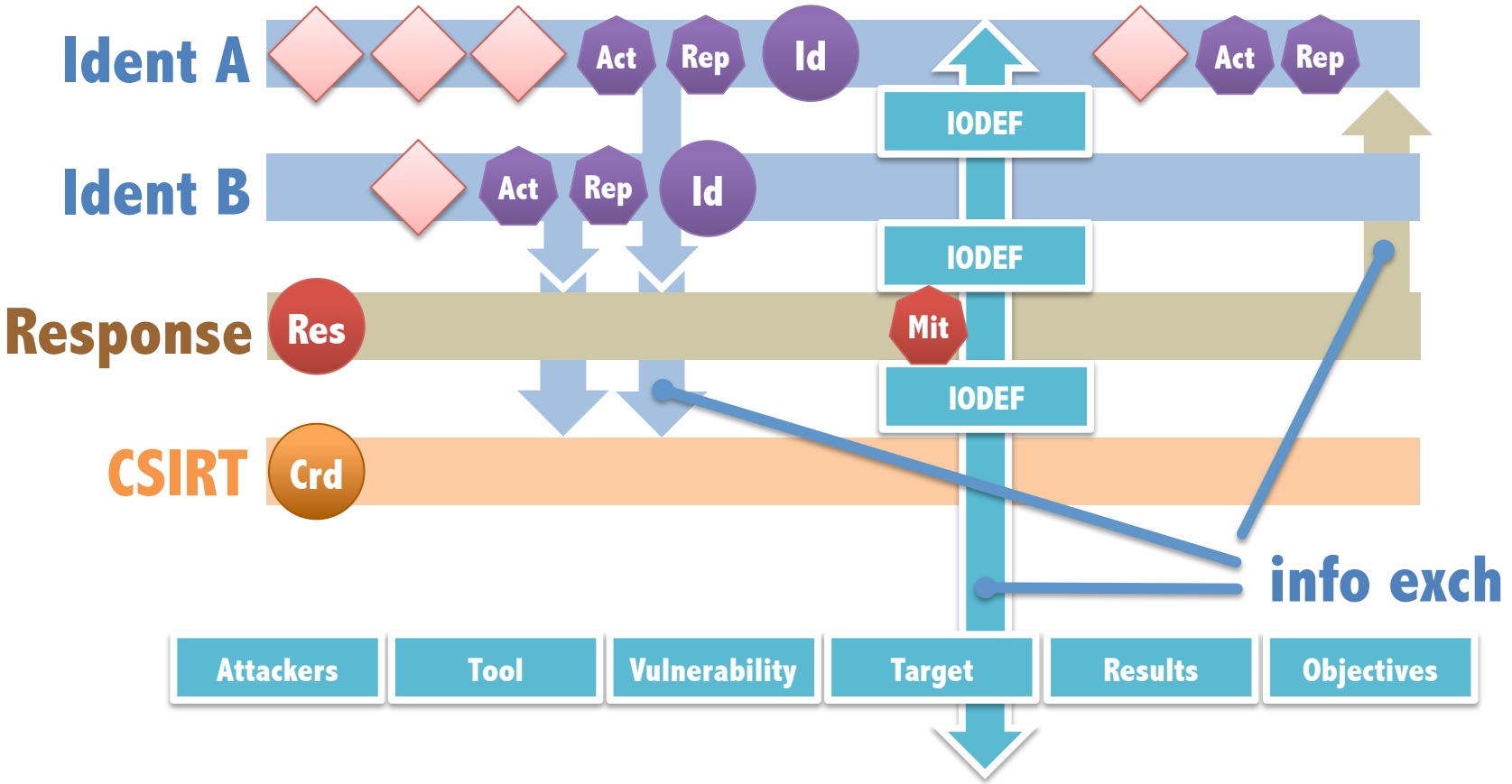
3a. Mapped to common activities

Information and sharing? standard data, common activities

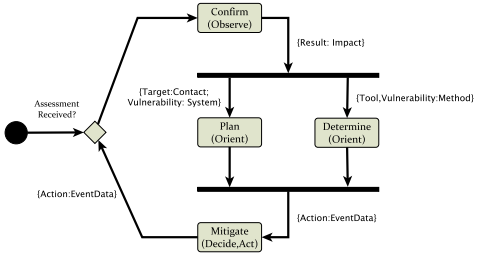


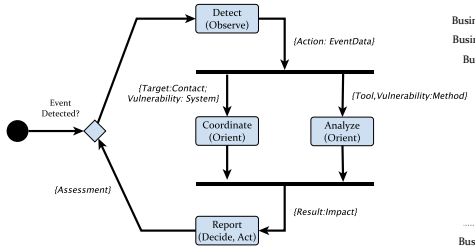
3b. Using standards to communicate

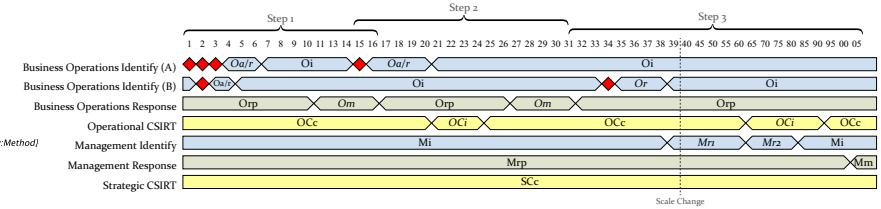
Information and sharing? standard data, common activities

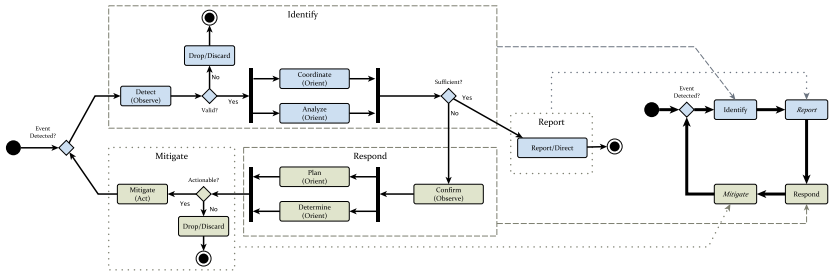


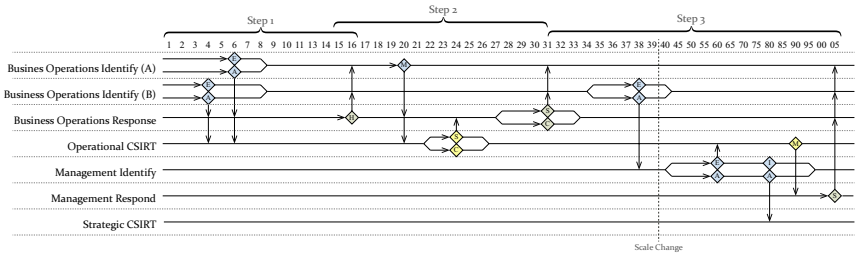
More Detail in Paper

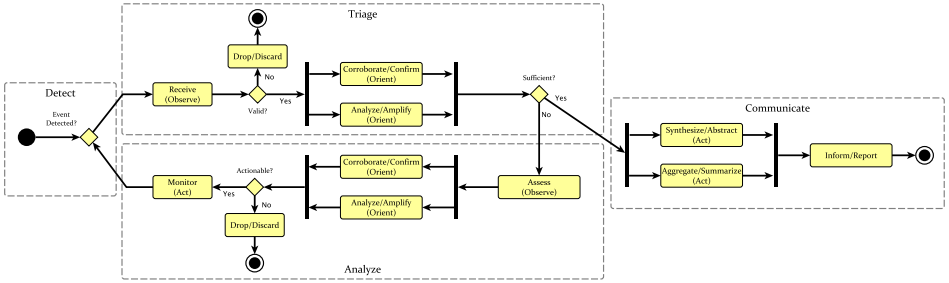


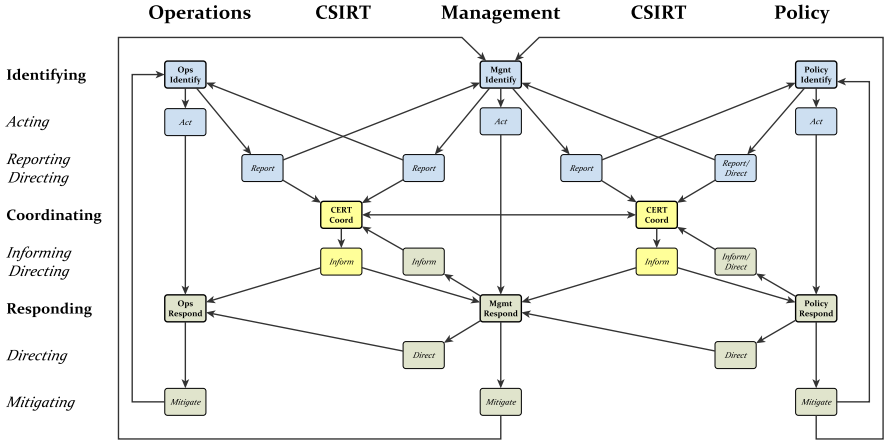








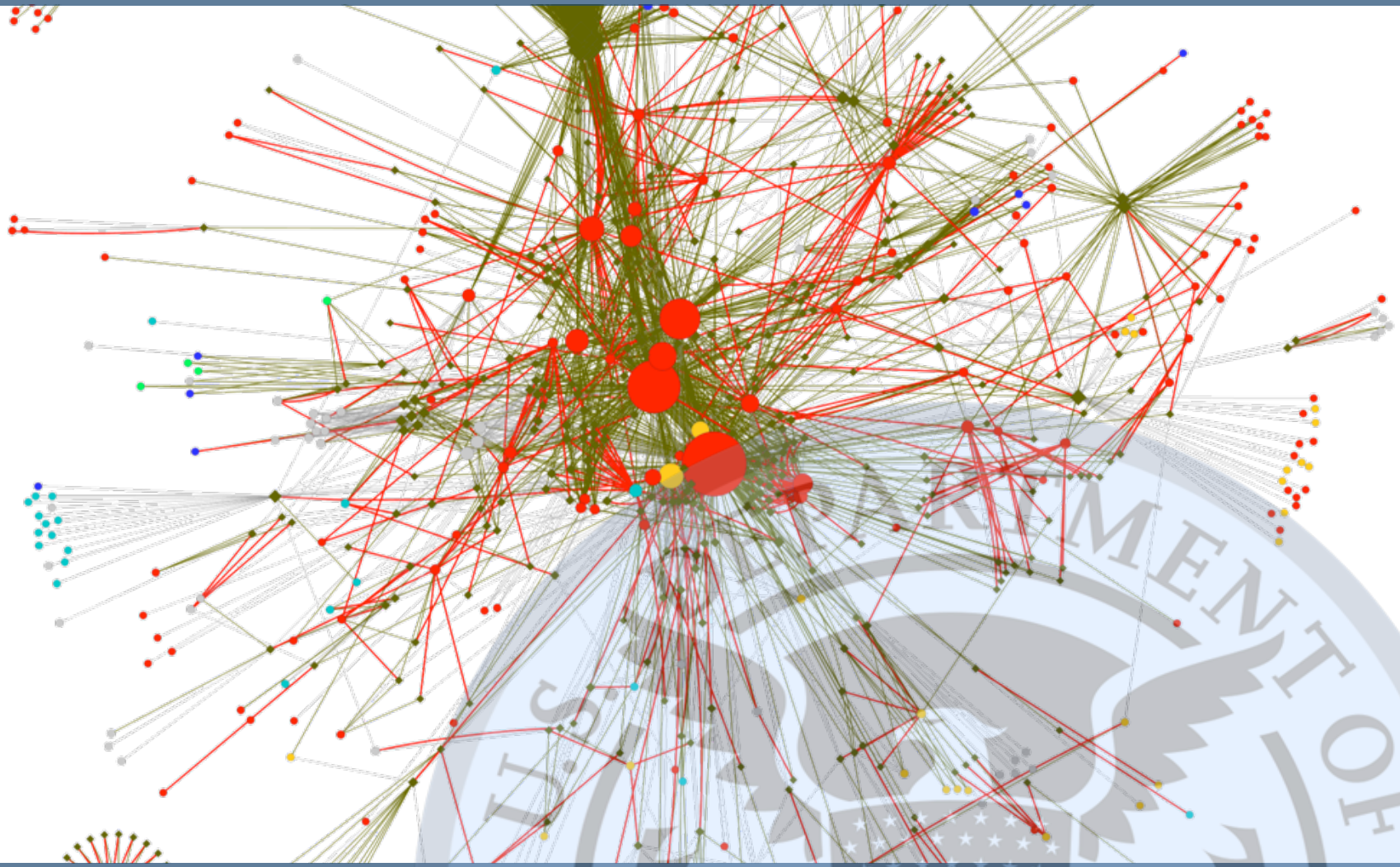




What Difference Will It Make?

- **Accounts for roles and concurrence**
  - No longer just IT/CSIRT
  - Coordination function of CSIRT
  - Multiple ways to “handle” events
- **Allows modeling and simulation**
  - Drive toward better modeling
- **Informs design and architecture**
  - Helps integrate multiple data formats
  - Helps find the “verbs”

What's next: Exercise/Model Analysis



Questions?

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

marcos.osorno@jhuapl.edu
(443) 778-9187

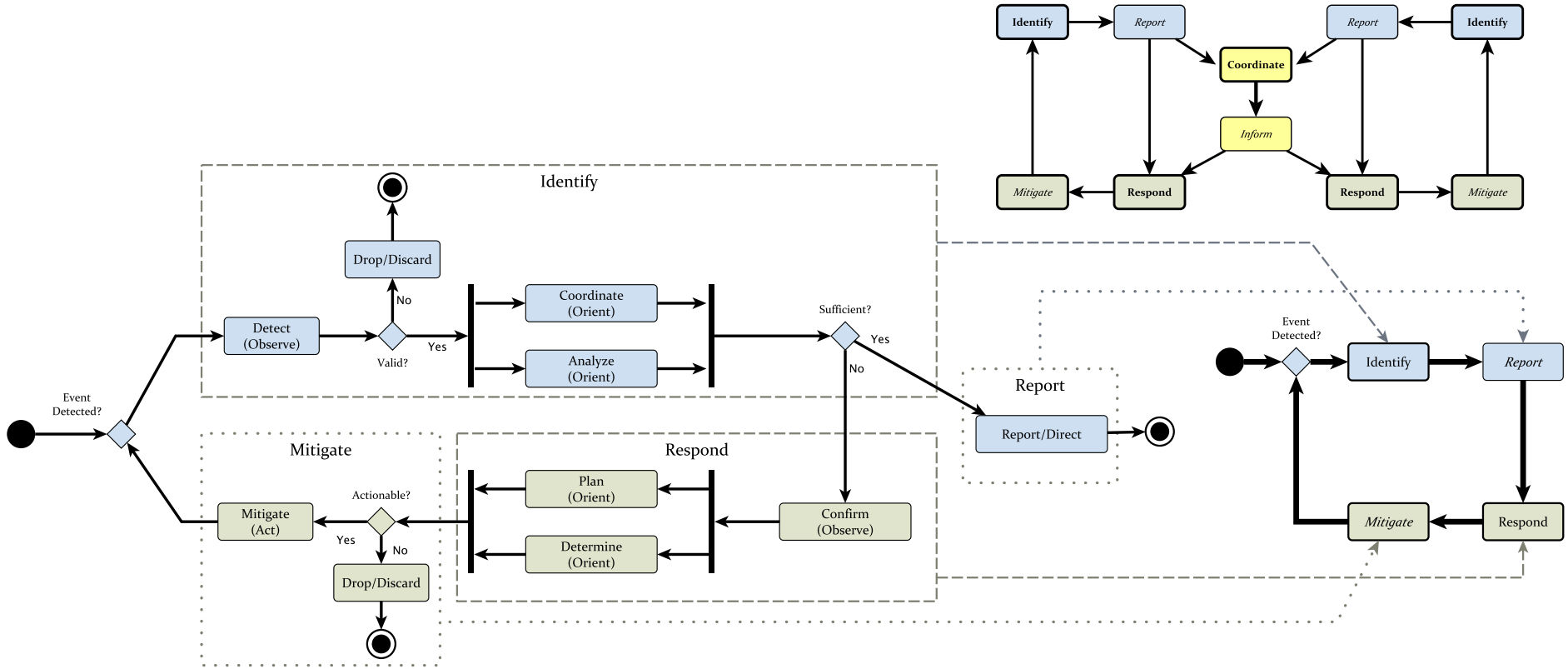
US-CERT
UNITED STATES COMPUTER EMERGENCY READINESS TEAM

APL

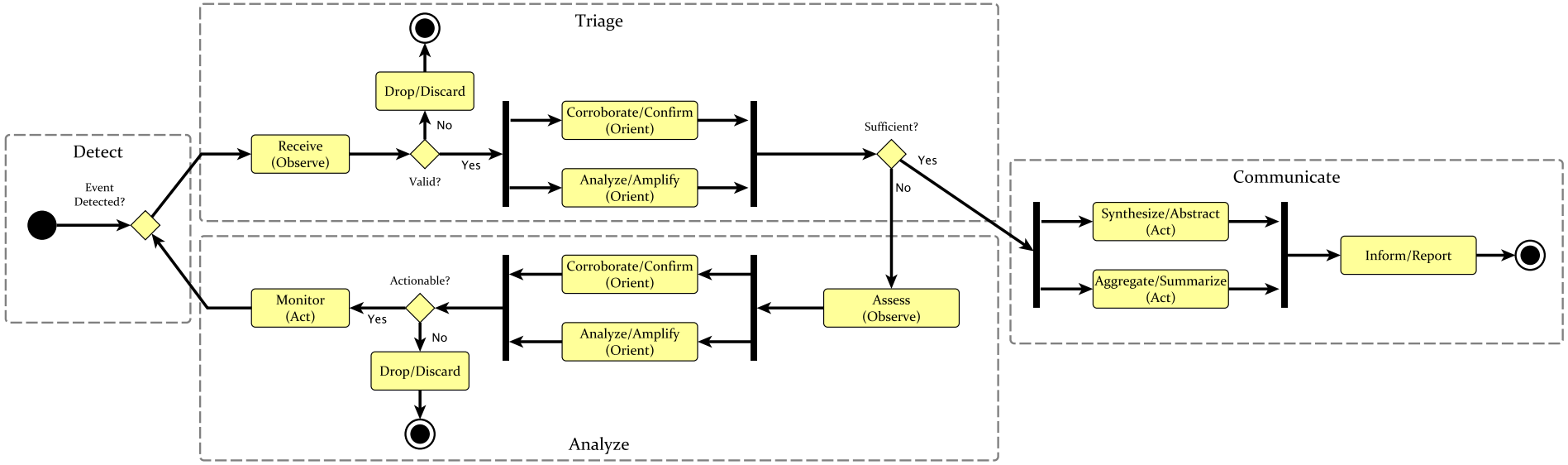
Issues with current approaches

- **Linear processes**
  - Limited concurrence
  - Phases challenging/subjective
  - Mostly "folk models" used for documentation
  - Exclusion of management and policy
- **Knowledge and Information**
  - *Multiple* taxonomies
  - A whole lot of data-formats
  - A few exchanges

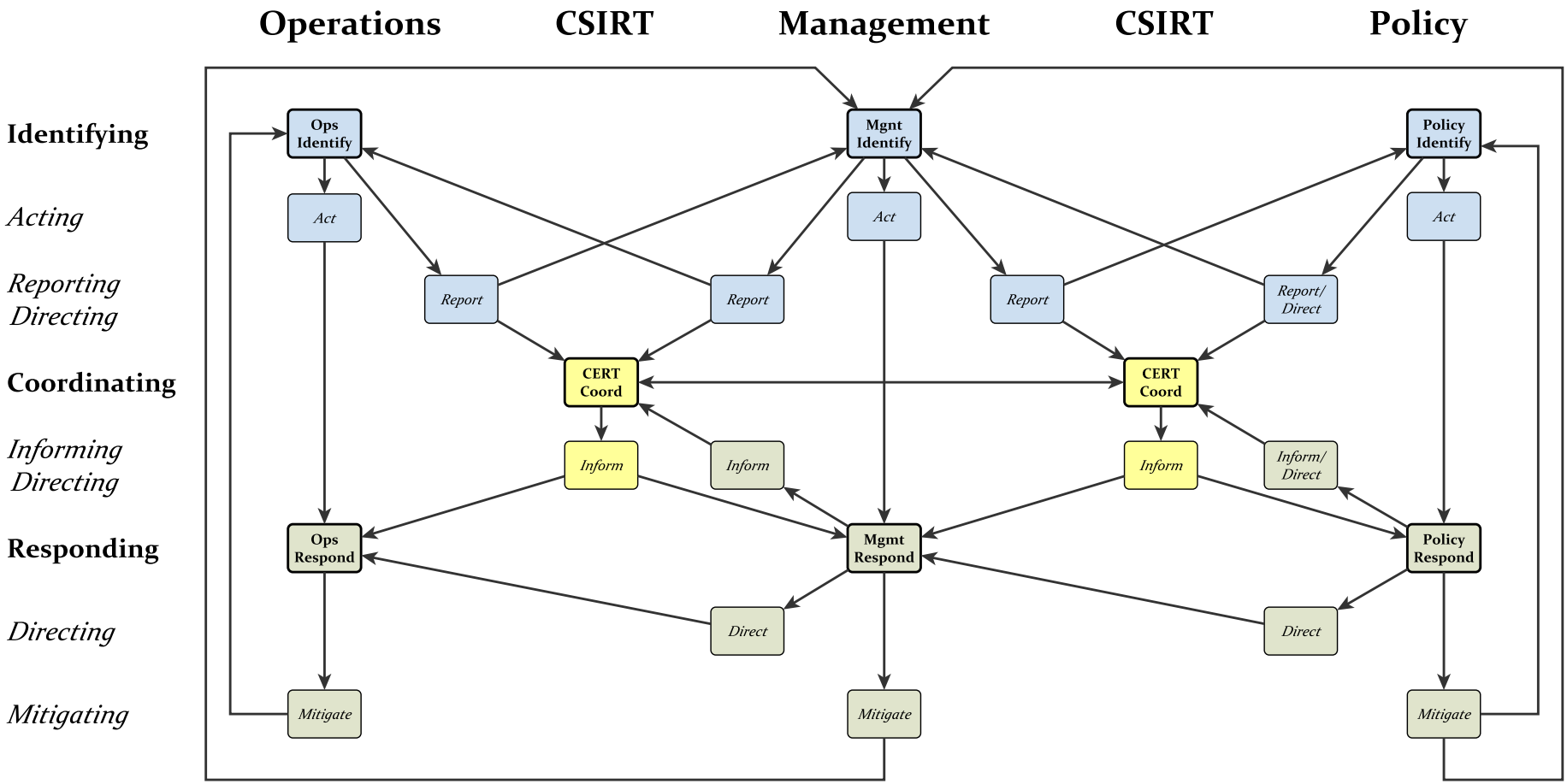
Defend Cycle



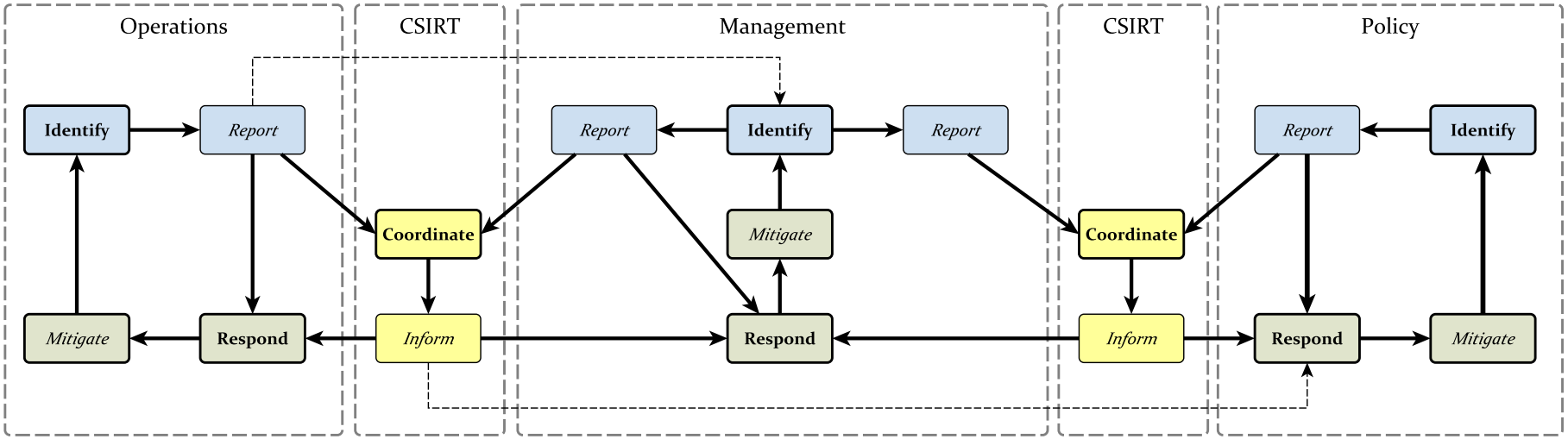
Coordinate Cycle



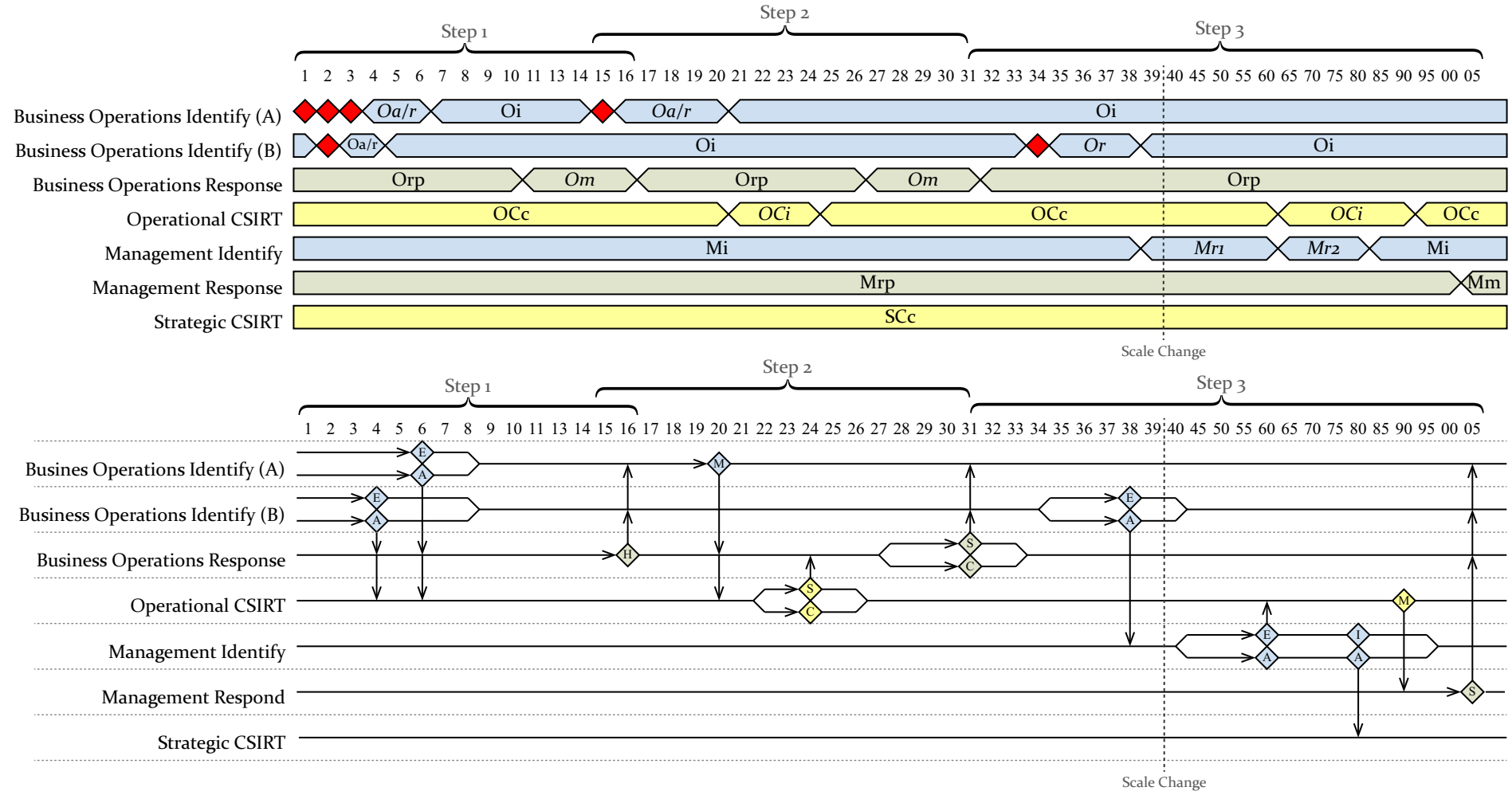
Complete coordination model



Simplified coordination model



Timing and Activity Diagrams



Multi-phase scenario