16th ICCRTS

"Collective C2 in Multinational Civil-Military Operations"

Title of Paper

Coordinated Cybersecurity Incident Handling
Roles, Processes, and Coordination Networks for Crosscutting Incidents

Topic(s)

Primary
• Cyberspace Management
Alternates
• Networks and Networking

Name of Author(s)

Marcos Osorno	Thomas Millar	Danielle Rager
Johns Hopkins University Applied Physics Laboratory	United States Computer Emergency Readiness Team	Johns Hopkins University Applied Physics Laboratory
11100 Johns Hopkins Road Laurel, MD 20723	245 Murray Lane SW Bldg 410 Washington, DC 20598	11100 Johns Hopkins Road Laurel, MD 20723
Marcos.Osorno@jhuapl.edu	Thomas.Millar@dhs.gov	Danielle.Rager@jhuapl.edu

Point of Contact

Marcos Osorno
Marcos.Osorno@jhuapl.edu
(240) 228-9187

Name of Organization

Johns Hopkins University Applied Physics Laboratory
11100 Johns Hopkins Road
Laurel, MD 20723

Report Documentation Page

Form Approved
OMB No. 0704-0188

1. REPORT DATE	2. REPORT TYPE	3. DATES COVERED
JUN 2011		**00-00-2011 to 00-00-2011**

4. TITLE AND SUBTITLE	5a. CONTRACT NUMBER
Coordinated Cybersecurity Incident Handling: Roles, Processes, and Coordination Networks for Crosscutting Incidents	5b. GRANT NUMBER
	5c. PROGRAM ELEMENT NUMBER
6. AUTHOR(S)	5d. PROJECT NUMBER
	5e. TASK NUMBER
	5f. WORK UNIT NUMBER
7. PERFORMING ORGANIZATION NAME(S) AND ADDRESS(ES) **Johns Hopkins University,Applied Physics Laboratory,11100 Johns Hopkins Road,Laurel,MD,20723**	8. PERFORMING ORGANIZATION REPORT NUMBER
9. SPONSORING/MONITORING AGENCY NAME(S) AND ADDRESS(ES)	10. SPONSOR/MONITOR'S ACRONYM(S)
	11. SPONSOR/MONITOR'S REPORT NUMBER(S)

12. DISTRIBUTION/AVAILABILITY STATEMENT
Approved for public release; distribution unlimited

13. SUPPLEMENTARY NOTES
Presented at the 16th International Command and Control Research and Technology Symposium (ICCRTS 2011), Qu?c City, Qu?c, Canada, June 21-23, 2011. U.S. Government or Federal Rights License.

14. ABSTRACT
To aid in the practice of securing computing systems and managing related incidents, the United States government cybersecurity community has proposed and promulgated a variety of incident handling life cycles, taxonomies, and data formats. However, current incident handling life cycles are limited to a set of discrete, ordered, and sequential steps executed for a specific security incident that is assumed to be identifiable knowable, and resolvable. These life cycles have not been reconciled with existing taxonomies and data formats nor have they been designed for concurrency or compatibility with business, military, or situational awareness process models. We propose building on existing work in the cybersecurity field by modifying linear life cycles into a distributed, concurrent loosely coupled, and action driven framework that can manage multiple, simultaneous, and complex events. By reevaluating existing processes, mapping them to relevant decision support process models, identifying functional user roles, and incorporating information elements from existing taxonomies and data formats, we describe a coordination network process model for crosscutting cybersecurity incidents.

15. SUBJECT TERMS

16. SECURITY CLASSIFICATION OF:			17. LIMITATION OF ABSTRACT	18. NUMBER OF PAGES	19a. NAME OF RESPONSIBLE PERSON
a. REPORT **unclassified**	b. ABSTRACT **unclassified**	c. THIS PAGE **unclassified**	**Same as Report (SAR)**	**49**	

Coordinated Cybersecurity Incident Handling

Roles, Processes, and Coordination Networks for Crosscutting Incidents

Marcos Osorno
Johns Hopkins University
Applied Physics Laboratory
Laurel, MD
Email: Marcos.Osorno@jhuapl.edu

Thomas Millar
United States Computer
Emergency Readiness Team
Washington, DC
Email: Thomas.Millar@dhs.gov

Danielle Rager
Johns Hopkins University
Applied Physics Laboratory
Laurel, MD
Email: Danielle.Rager@jhuapl.edu

***Abstract*—To aid in the practice of securing computing systems and managing related incidents, the United States government cybersecurity community has proposed and promulgated a variety of incident handling life cycles, taxonomies, and data formats. However, current incident handling life cycles are limited to a set of discrete, ordered, and sequential steps executed for a specific security incident that is assumed to be identifiable, knowable, and resolvable. These life cycles have not been reconciled with existing taxonomies and data formats nor have they been designed for concurrency or compatibility with business, military, or situational awareness process models.**

We propose building on existing work in the cybersecurity field by modifying linear life cycles into a distributed, concurrent, loosely coupled, and action driven framework that can manage multiple, simultaneous, and complex events. By reevaluating existing processes, mapping them to relevant decision support process models, identifying functional user roles, and incorporating information elements from existing taxonomies and data formats, we describe a coordination network process model for crosscutting cybersecurity incidents.

I. Introduction

Current policy and cybersecurity community documents enumerate a variety of incident handling processes [1][2][3]. These processes generally describe a series of sequential steps that aim to resolve a cybersecurity incident within an individual organization. Such a process, as described by the National Institute of Standards and Technology in the current incident handling guide, is shown in Fig. 1 [1]. Given the crosscutting, persistent nature of many contemporary cybersecurity threats and related incidents, coordination between computer security incident response teams (CSIRTs) is often required [4][5]. We use the term *crosscutting incidents* to describe those incidents simultaneously affecting multiple organizations, various sectors, or different types of organizations. Because of the critical role that data and computing resources have on day-to-day business processes, incidents can have negative impacts on the successful execution of business operations and require decision-making from cognizant policy makers.

For these reasons and to allow for crosscutting, inter-organizational, and concurrent incident handling, we propose a set of incident handling roles, related actions, relevant process cycles, crosscutting activities, and affiliated coordination networks. A simplified version of this framework is shown in Fig. 2. Building on current and previous efforts in process definition, taxonomy development, and data format standardization, this paper surveys and selects from relevant prior work, demonstrates mapping of concepts to this model, and illustrates how incident data might be exchanged using current standards. Because of the prevalence of decision support and situational awareness models in contemporary literature, we map actions and process cycles to these paradigms. Finally, we demonstrate how such networks might function during an incident and suggest how future work might further formalize this framework through systems architecture, process modeling, and network state estimation.

II. Current State of Practice

To support the coordinated, distributed cybersecurity approach described in recent documents by the Department of Homeland Security [4] and articulated by National policy [5], the United States Computer Emergency Readiness Team (US-CERT) recently reevaluated existing processes and information management approaches. Based on that analysis, this paper describes an incident handling approach appropriate for coordinated incident response.

The United States government's incident handling paradigms have provided general methodologies for internal coordination, documenting incident handling processes, and providing a procedural model of a linear incident handling process [2] [3]. In addition, many documented incident handling processes are similar to or have been derived from

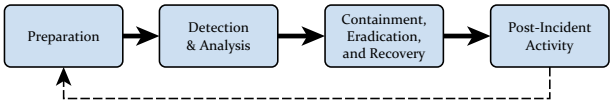


Figure 1. Isolated incident handling process.

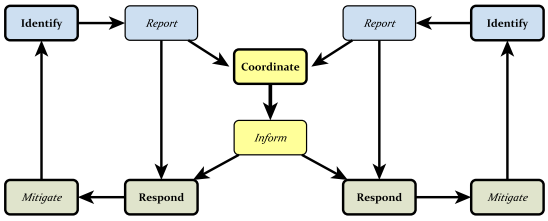


Figure 2. Top level coordinated incident handling process.

multi-phased approaches such as the Department of Energy's protection, identification, containment, eradication, recovery, and follow-up process (PICERF) [1] [6] [7]. These linear, ordered, discrete, and sequential processes may originally have been sufficient. However, both the National Institute of Standards and Technology's (NIST) process described in Fig. 1 and the Department of Defense's (DoD) equivalent process show that these processes may recur continuously by restarting from the first step once the incident is mitigated [2] [3]. Furthermore, other government publications [4] [8] have recommended generalized, cyclical incident management approaches or drawn similarities to approaches such as the military's observe, orient, decide, and act (OODA) paradigm [3]. This move toward continuous, cyclical processes is also reflected in academic research in the fields of cybersecurity situational awareness [9] [10], information fusion [11] [12], and general decision support [13] [14] [15].

In addition to the variety of cybersecurity processes identified in the publications of the incident management community, a variety of schemas, ontologies, and data formats have been drafted to aid in the execution of cybersecurity processes by facilitating the exchange of data and information [16]. Similarly, large-scale efforts such as the National Information Exchange Model (NIEM) [17] have been undertaken to facilitate information exchange between particular domains. However, our review of the relevant literature found very little information about how to integrate cybersecurity processes and information management formats for incident handling. For all these reasons, we determined a need to develop a non-linear distributed cybersecurity incident handling process and examined various modeling methodologies that could describe process, data flow, and concurrency.

In order to develop a coordinated, distributed incident handling process, we surveyed existing incident life cycles, taxonomies, and data formats. We subsequently mapped a set of taxonomies and data formats to a cyclical process compatible with decision support and situational awareness paradigms. Based on this mapping, we defined two incident management cycles, *identify* and *respond*, that can be subsequently combined into a *defend* cycle. Because large-scale incident handling requires inter-organizational coordination across organizations of various and distinct functional roles, we defined a *coordinate* cycle that serves to facilitate incident handling between multiple organizations and across organizations of different functional types resulting in an incident handling model for coordinated cybersecurity incident handling. Since the described approach focuses on information sharing and decision support rather than on individual incidents, it provides the flexibility necessary for mapping to existing incident handling processes while accommodating generalized, persistent, or ambiguous threats.

Several models, schemata and frameworks already exist within the cybersecurity domain to serve a wide variety of purposes. We have divided these efforts into three broad categories based on their intended purposes: (1) incident life cycles, (2) incident taxonomies, and (3) data formats. In addition to these cybersecurity domain-specific frameworks, we surveyed multiple decision and situational awareness models for their potential application to coordinated incident handling.

A. Incident Life Cycles

Incident life cycles describe the incident handling process, breaking it into discrete phases. Table I shows a selection of incident handling life cycles. Incident life cycles describe specific activities associated with each phase but do not explicitly assign categories or specify data formats for capturing and sharing information.

B. Data Formats

Data formats facilitate cybersecurity-related knowledge sharing and discovery. A multitude of languages and schemata

TABLE I. INCIDENT LIFE CYCLE INVENTORY

CJCSM 6510.01A [a]
Detection of Events
Preliminary Analysis and Identification
Preliminary Response Action
Incident Analysis
Response and Recovery
Post-Incident Analysis
NIST SP 800-61 [b]
Preparation
Detection and Analysis
Containment, Eradication, and Recovery
Post-Incident Activity
SANS/Schultz [c]
Preparation
Identification/Detection
Containment
Eradication
Recovery
Follow-up

a. See Ref. [3]
b. See Ref. [2]
c. As described in Ref [1], Appendix B

TABLE II. INCIDENT DATA FORMAT INVENTORY

	Internet Engineering Task Force [a]
Name	***Description***
RFC 3067	IODEF Requirements
RFC 4765	Intrusion Detection Message Exchange Format
RFC 5070	Incident Object Description Exchange Format
RFC 5901	Extensions to the IODEF for Reporting Phishing
RFC 5941	Sharing Transaction Fraud Data
	Security Content & Automation Protocol [b]
Name	***Description***
CVSS	Common Vulnerability Scoring System
OCIL	Open Checklist Interactive Language
XCCDF	Extensible Configuration Checklist Description Format
	Making Security Measurable [b]
Name	***Description***
ARF	Asset Results Format
CAPEC	Common Attack Pattern Enumeration and Classification
CCE	Common Configuration Enumeration
CEE	Common Event Expression
CPE	Common Platform Enumeration
CVE	Common Vulnerabilities and Exposures
CWE	Common Weakness Enumeration
OVAL	Open Vulnerability Assessment Language
MAEC	Malware Attribute Enumeration and Characterization

a. Selected from http://tools.ietf.org/html/
b. Based on http://measurablesecurity.mitre.org/list/index.html

exist for sharing software vulnerability and exposure information, attributes and behavior of malicious code, observable details or indicators of attacks, system state and configuration information, and more. A selection of schemata is provided in Table II. These specifications explain how cybersecurity information can be presented and stored in a standardized format but do not address the process or functions related to the information nor how the information may be shared.

Unfortunately, our review exposed no commonly agreed upon model to describe how these data formats may be applied in the process phases of an incident handing life cycle.

C. Incident Taxonomies

Incident taxonomies describe the fundamental elements of a cybersecurity incident and categorize incidents according to various characteristics such as the means of compromise or severity of impact. Table III shows a selection of incident taxonomies. While incident taxonomies may provide a means to share information about a cybersecurity event using commonly understood terminology, they do not define the processes behind the capture of incident information or provide specifics regarding how the information should be exchanged and used.

D. Decision and Situational Awareness Models

To design a distributed, scalable, and concurrent process, we minimized the emphasis on linear incident handling processes to instead focus on the generalized way in which incident handlers might make decisions and pass information from organization to organization. Not only are linear processes challenging to model concurrently [18], but incidents might be prone to subjective definition and transition between phases might be similarly difficult to identify or standardize. By far the most common situational awareness paradigm cited in our review was Mica Endsley's perception, comprehension, projection, decision, and performance model [19]. In the military literature, John Boyd's observe, orient, decide, and act (OODA) cycle has been similarly incorporated into military decision literature [20]. Both Endsley and Boyd have been mapped to data fusion paradigms [12] and extended to the cybersecurity incident management domain [9] [21]. While the reconciliation of decision support models to cognitive neuroscience or neuropsychology is limited and debate exists if these approaches serve as more than folk models [22], the mapping to basic cognitive models such as the perception-action cycle [23] is sufficient for our definition of two basic cycles, an *identify* cycle and a *respond* cycle. Similarly, this two-cycle process is compatible with the approach documented for the intelligence community in John Bodnar's logistics and operational cycles [24] and consistent with Anders Dahlbom's comprehensive approach for modeling decision support [25].

III. Mapping Taxonomy to Process

It is possible to synthesize an integrated incident management model that combines elements of an incident life cycle and incident taxonomy with the efficiencies enabled by a standard data format. Due to the breadth of available models illustrated in Tables I, II and III, we determined that it would be best to attempt to select the most commonly used, abstract, and comprehensive models for each and develop a high-level correspondence between them.

A. Selected Taxonomy

For our incident taxonomy we selected Howard and Longstaff's *A Common Language for Computer Security Incidents* to broadly describe the families of information that a computer security incident response team (CSIRT) would likely need to ingest, refine, and share [26]. In their taxonomy, depicted in the left column of Fig. 3, cybersecurity incidents are described as having seven discrete facets: (1) *attacker*, (2) *action*, (3) *target*, (4) *tool*, (5) *vulnerability*, (6) *unauthorized result*, and (7) *objective*.

B. Mapping to the IODEF Data Format

While various data formats exist which could be mapped to the taxonomic elements identified above, the Incident Object Description Exchange Format, IODEF [26], the Abuse Reporting Format (ARF), and Common Event Expression (CEE) are the most germane to incident management; of those, IODEF is the most widely adopted [16]. Because of the standard's adoption, relevance, object-oriented nature, and conduciveness to modeling, IODEF was selected for this incident management framework. For the examples presented, only a subset of the IODEF is used. A more comprehensive view of IODEF classes is provided in Fig 4. For simplicity, we have limited the number of IODEF entities included to the minimum required to describe the coordination network. Therefore, we recommend the creation of a more comprehensive mapping of IODEF to the coordination model as future work.

TABLE III. Incident Taxonomy Inventory

CJCSM 6510.01.A	Common Language	NIST SP 800-61	VERIS
Incident Tracking Information	Attackers Tool	Contact Information for the Incident	Agent
Reporting Information	Vulnerability	Report and Handler	Action
Categorization Information	Action	Incident Details	Asset
Incident Status	Target	General Comments	Attribute
Technical Details	Unauthorized Result	General Status of the Incident Response	
Sites Involved	Objectives	Summary of the Incident	
Impact Assessment Coordination		Incident Handler Comments	
		Cause of the Incident	
		Cost of the Incident Business	
		Impact of the Incident	

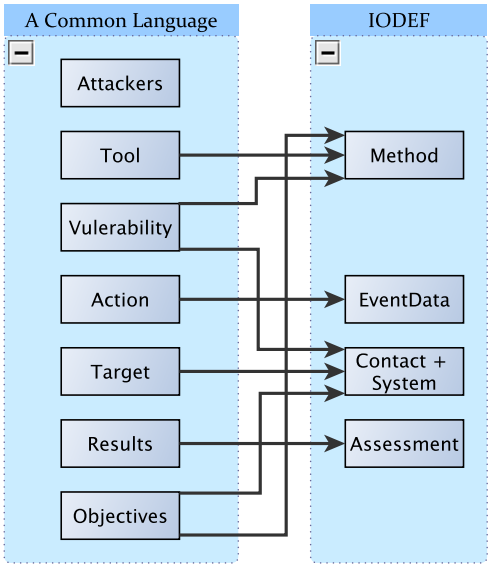
a. Sample of a Table footnote. (Table footnote)

C. Attackers, Objectives, and Vulnerabilities

In the design process of our integrated model, two of the above incident characteristics, *attackers* and *objectives*, were determined to be out of scope for most CSIRT operations. Positive attribution of attackers is outside of the authority of most CSIRTs' operational mission. While CSIRTs and other similar organizations may provide circumstantial details or descriptions of an attacker's characteristics, the ultimate determination of identity and culpability is the responsibility of law enforcement, the intelligence community, and the justice system. For this reason, attackers are not mapped to IODEF elements in Fig. 3.

The same reasoning applies for the limiting the scope of objectives; while incident management teams are certainly not prevented from hypothesizing about the potential goals of a cyber attack, the business of drawing authoritative conclusions about an attacker's intentions is more appropriately handled by judiciary, intelligence, and diplomatic authorities. For this reason, *objectives* influence the content of *Method* and illuminate relevant *Contacts*, but are not directly mapped to either object. An attacker's perceived *objectives* may help incident handlers predict or identify the *Method* and bound the scope of an incident while helping identify the relevant *Contacts* to notify.

An additional element from the taxonomy, *vulnerability*, was determined to be an attribute associated with two other elements rather than a stand-alone data type. For an incident to occur, a vulnerability or weakness of some kind must exist as both a characteristic of the attacker's *target* and of the attacker's technique, or *tool*. In addition, in many cybersecurity incidents it is possible for the set of vulnerabilities on the targeted system or systems and the set of vulnerabilities exploited by the attack tool to be heterogeneous. Isolating and identifying a single vulnerability from the intersection of both sets may not be the most useful approach for extracting and sharing critical network defense information during an emergent cybersecurity incident. With the six remaining



elements from the original Howard and Longstaff taxonomy, we were able to identify a correspondence with major classes of the IODEF. This mapping is shown in Fig. 3 and described below:

- The *tool* element corresponds to the *Method* class of the IODEF serving as a container for descriptions and references relating to vulnerabilities and attack techniques associated with the incident.
- The *vulnerability* element is mapped to both the *Method* and *System* classes. Since we associate the *System* class with the *Contact* class, the *vulnerability* information may also be transitively associated with the *target*.
- The *action* element corresponds to the child elements of the *EventData* class within the IODEF which

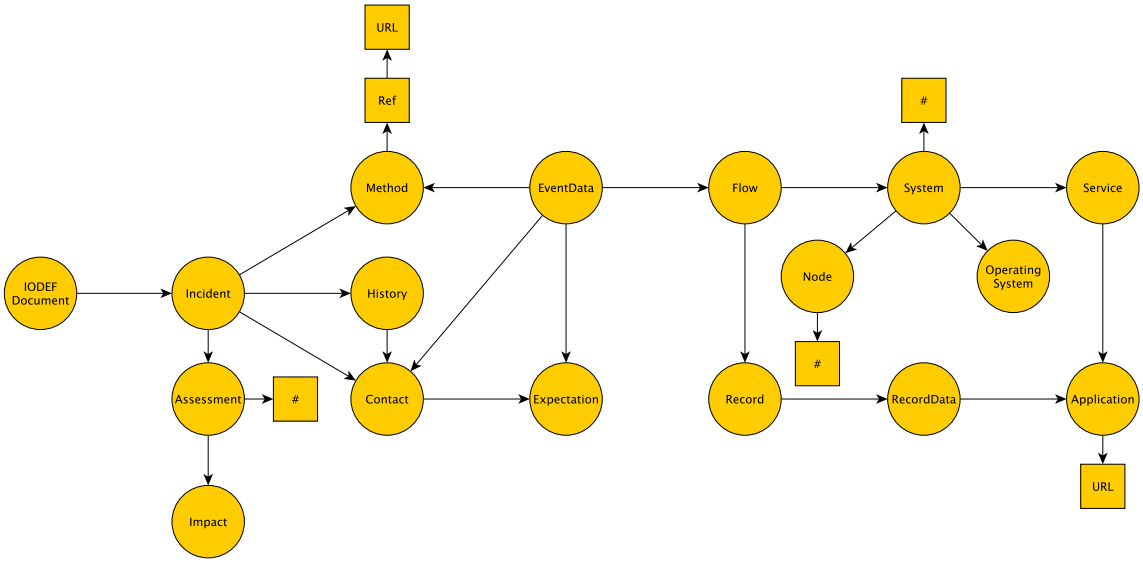


Figure 4. Major Inicident Object Definition Exchange Format (IODEF) classes

contain the records of occurrences (e.g. log files, samples of network traffic, security scan results) associated with a cybersecurity incident.

- The *target* element primarily corresponds to the *Contact* class, describing a constituent, responsible service provider, or security staff associated with the potentially affected *System* through the corresponding class.
- The unauthorized *result* element corresponds to the *Assessment* class of the IODEF. This class is intended as a container for estimates or findings of the potential and/or actual impact of a cybersecurity incident.
- The *objectives* are not directly mapped to the *Method* and *Contacts* classes but help augment the *vulnerability* and *target* information that have already been mapped to those elements.

It is important to note that the *EventData* and *System* classes are complex classes that may include data from various other IODEF classes.

IV. CROSSCUTTING COORDINATION NETWORK

Rather than focus on individual steps that might describe managing discrete phases within one incident, this model focuses on independent but related cycles that can work across multiple incidents and that are managed by diverse organizations at different speeds and volumes. To this end, the basic coordination network includes *identification* elements, *response* elements, and *coordination* elements. These elements, shown in bold text in Fig. 5, represent cycles and are described in more detail in following sections. For the simple network, we have three major supporting activities: *mitigating*, *reporting*, and *informing*. These three activities, depicted in italics in Fig. 5, will be augmented in the more complete network shown in Fig. 6. The network is further divided into *operations*, *management*, and *policy* roles. A computer security incident response team (*CSIRT*) represents a fourth role and facilitates information flow within the network. These four roles are shown as dashed lines in Fig. 5.

A. Roles

The distinction between organizational roles is important in order to (1) identify variations in how incident information is managed, (2) model variations in information routing based on role, and (3) account for differences in the number and duration of *identify*, *respond*, and *coordinate* cycles. Incident management for large events or organizations is likely to involve not only incident management and information technology personnel, but may also include the managers of those business processes affected by computer incidents as well as the responsible policy makers. For this reason, we have modeled three execution roles and two support roles:

1) Execution Roles

a) Business Operations (Operations/Ops): includes users of computing systems used for the execution of sub-components of business processes. Operations also includes the Information Technology (IT) service and support roles responsible for providing and maintaining the systems and capabilities critical to business operations.

b) Management includes those users and organizations responsible for the overall execution of business processes within one organization or inter-organizationally.

c) Policy includes those individuals and organizations responsible for the overall execution and governance of business processes.

2) Support Roles

a) Computer Security Incident Response Team (CSIRT) facilitates the exchange of incident data between the three organizational roles by processing information as described in the *coordinate* cycle.

b) Other Roles: An incident may involve various other support roles such as intelligence, legal, and law enforcement. However, for the sake of simplicity, coordination with these entities is assumed to be happening within the execution roles and relevant CSIRTs.

In general, events may trickle up based on severity, Ops → Management → Policy, while policy will flow down in the opposite direction. As information moves from *ops* to *management* and subsequently to *policy*, the IT/IS and *CSIRT* roles help facilitate information exchange and synchronize CSIRT decision cycles.

The IT/IS role will not been depicted and is assumed to be integrated into the cycles of the corresponding organizations. In

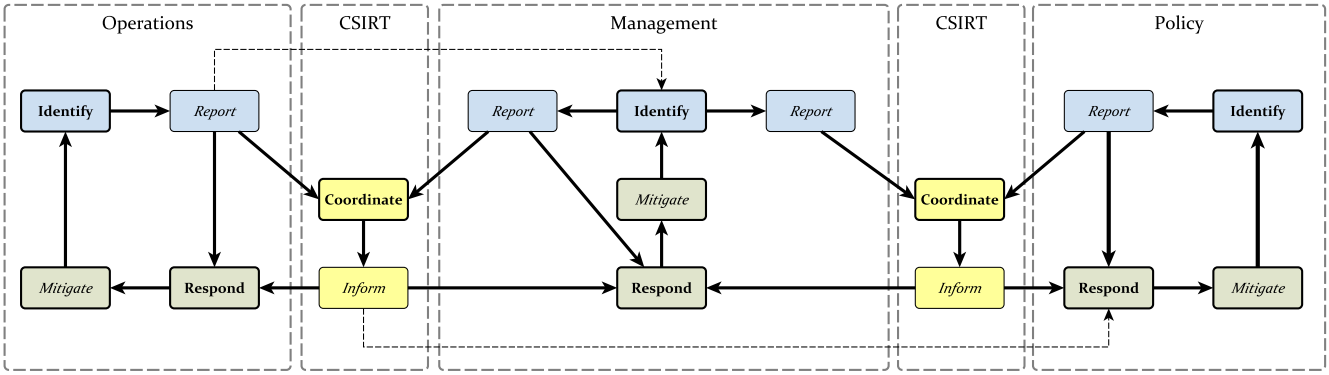


Figure 5. Simplified coordination network

addition, communications between the CSIRT and IT/IS will not be shown, but are assumed to be within the relevant *identify*, *coordinate*, and *respond* cycles.

B. The Extended Coordination Framework

While this simple model accounts for the different organizational roles found in large scale incident management, the dashed lines in Fig. 5 show one of many possible information flows not accounted for in this model. For example, it is possible that at the end of a identify cycle an operational organization or incident handler might decide to forward the information to the manager of the business process affected by the incident but not to the CSIRT organization. In order to create more flexible model and account for such scenarios, a more fully connected model is provided in Fig. 6.

While the extended model still includes the same roles and basic processes, it also includes general activities relevant to sharing incident handling information leaving us with the following activities:

1) Identifying: Described in detail in Sec. IV. C., identification consists of recognizing events that might be associated with a cybersecurity incident.

2) Acting: If the identified anomaly or event is actionable without further coordination, an organization's identification mechanism might inform action from the response elements.

3) Reporting/Directing: Reporting is intended to communicate an organization's understanding of an event and covney related expectations to the relevant CSIRT or organizational elements. While most *identify* entities report descriptive information, policy's identification activity might provide directive guidance in terms of explicit actions to be taken. This information may be specifically targeted to the CSIRT or intended for further dissemination throughout the community via the CSIRT.

4) Coordinating: Described in detail in Sec. VI., coordination activites include managing the receipt of incident information, working with relevant support organizations, processing incident information, or coordinating with other CSIRTs

5) Informing/Directing: The informing cycle is critical to incident handling by allowing information coordinated by the CSIRT to flow to the organizational response elements. Similarly, it allows the response mechanisms to give feedback to the rest of the community via the CSIRTs. Unlike the *reporting* activity, *informing* is intended to drive response. From within the policy role, those communications may not just inform response actions but require specific actions. These directives may be specific to the CSIRT or intended for further dissemination via the CSIRT.

6) Responding: Described in more detail in Sec. IV. D., the respond cycle represents those organizational elements involved in incident response. From within operations this might include end users as well as IT personnel. Within management, this might include business process owners or sector specific organizations such as Information Sharing and Analysis Centers.

7) Directing: Depending on the nature of the incident, organizations in an execution role should take into account CSIRT information to provide direction from policy down to management and likewise from management to business operations This direction might include general guidance or specific mitigation directives.

8) Mitigating: Once direction has been promulgated,

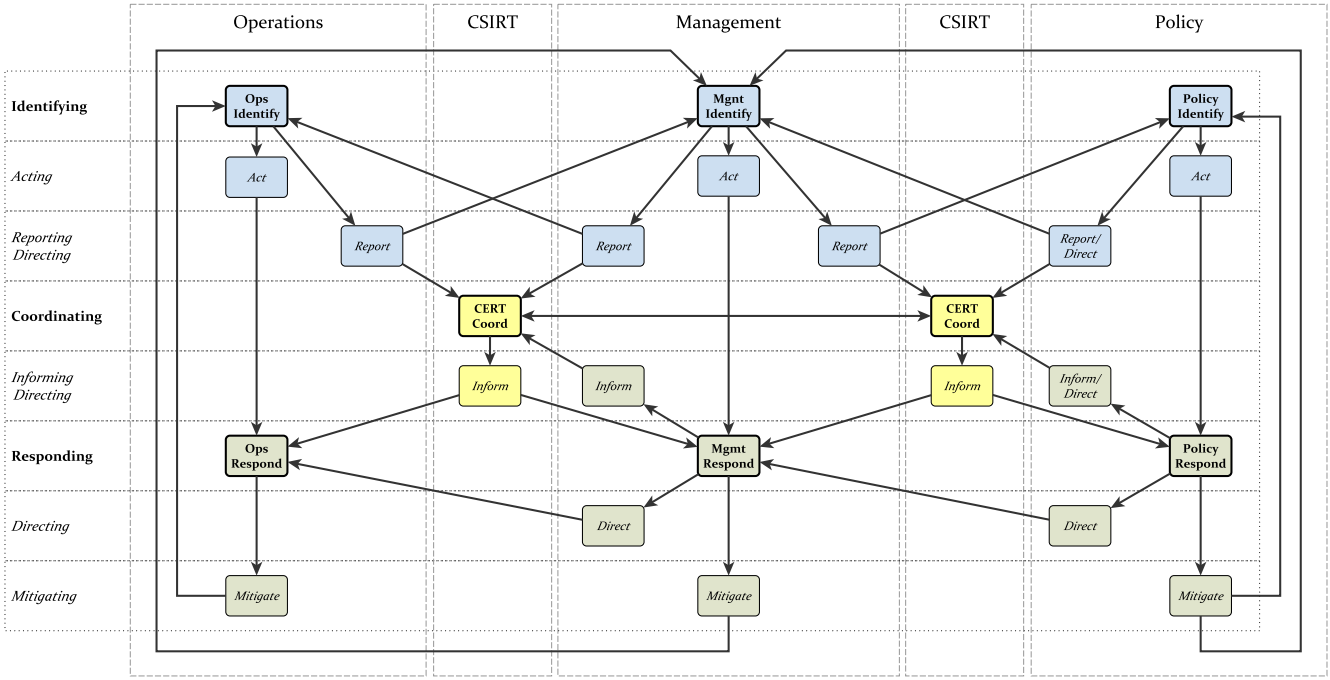


Figure 6. Extended coordinated incident handling network

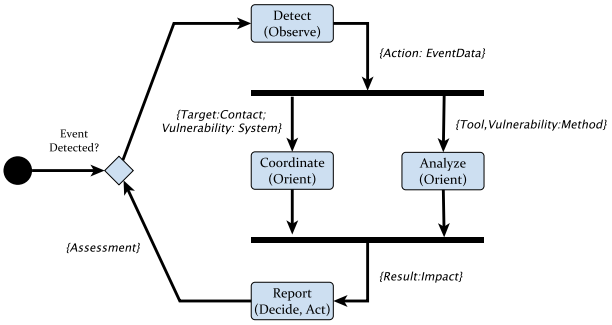


Figure 7. *Identify* process cycle

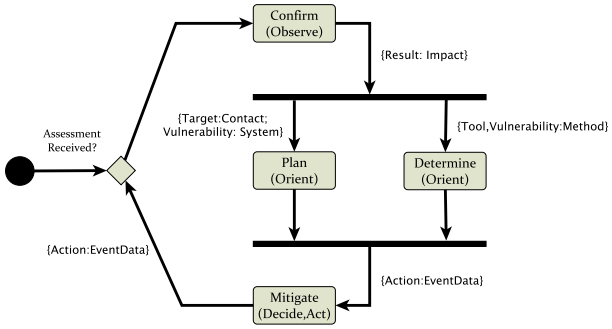


Figure 8. *Respond* process cycle

organizations may implement mitigation measures and enter monitoring. In addition, policy might monitor the effectiveness of management's migitation efforts who might similarly monitor mitigation within business operations.

For the reasons described in Sec. II, both the *identify* and *respond* cycles are mapped to the observe, orient, decide, and act paradigms (OODA).

C. The Identify Cycle

In the *identify* cycle depicted in Fig. 7, an event is *detected* which may be indicative of a cyber security incident. The event detection stage may consist of wide variety of real-world activities, such as a user encountering an unresponsive service, an analyst discovering an anomalous traffic pattern, an antivirus application identifying a suspicious file, or an intrusion detection system flagging a query for a domain name which is member of a watch list. In our model, this *detection* stage is considered equivalent to the Observe phase of the OODA loop. Information gathered from the Observe phase of the loop feeds forward into an Orient phase.

In addition, Orient is split into two parallel functions pursued by the CSIRT members: (1) *coordinating* with the contacts at the target site or other responsible parties in order to notify them of the event as well as to surmise the status of the potentially affected system(s); and, (2) *analyzing* the characteristics of the event to determine the attack technique and implications. Once the Orient phases are complete, enough information should have been assessed to Decide on a preliminary impact assessment for the event or incident. This may be simply that no incident has occurred — the target system is operating normally and the detected event was a false alarm — or that further investigation is warranted to determine the extent of a system compromise. Thus, the result of the impact assessment decision determines the act of moving on to the next task.

The Action might be to continue to monitor for detection events perhaps adding *Assessment* information to an IODEF *Incident* or *History*. More complicated actions that include spawning a response cycle or forwarding information to an incident handling team will be described in more detail with a use case. In any case, the fundamental action is to *report* the information to the relevant CSIRT or organizational response elements.

D. The Respond Cycle

To complement the identify cycle, we appended and extended the OODA-based model by adding a second set of activities that reuse the same data elements in a different set of operational activities. This extension of the process model is presented in Fig. 8.

These process phases comprise the functions of incident response and recovery management, again mapped against the OODA loop, although in this extension the data types are used in an inverse order from the incident identification process. This process begins with *confirming* an impact from an identified cybersecurity incident in the response cycle's Observe phase. The confirmed impact feeds forward into the Orient phase, which again consists of two parallel activities: (1) the original analysis of the methods and techniques employed to cause the incident is amplified and corroborated in order to *determine* an appropriate set of defensive countermeasures; and (2) additional coordination is *planned* with the contact responsible for the targeted system to ensure that the mitigation countermeasures are deployed successfully.

At this point, the combined knowledge captured during the previous loop and successive observation and orientation phases are employed through monitoring in order to Decide whether to continue actively gathering more information about the incident — if, for example, no effective countermeasures can be recommended at the current juncture — or whether to move on to a more passive monitoring situation in which the countermeasures are considered successful and become part of the new steady state of the involved parties. The final phase of this cycle, mapped to Act, works to *mitigate* negative effects and monitor identification activities as appropriate.

V. THE COMBINED DEFEND CYCLE

While the individual *respond* and *identify* cycles are useful for describing a decision-cycle view of portions of the incident handling process, it useful to show how both cycles might be combined for those situations where the organizational elements executing these missions are somewhat dependent on each other. In Fig. 9 a combined *defend* cycle is depicted. As with the individual *identify* cycle, the process is still initiated by an event, but the combined cycle is expanded to include a check for *validity* before starting the *coordinate* and *analyze* processes. If the determination is made that sufficient

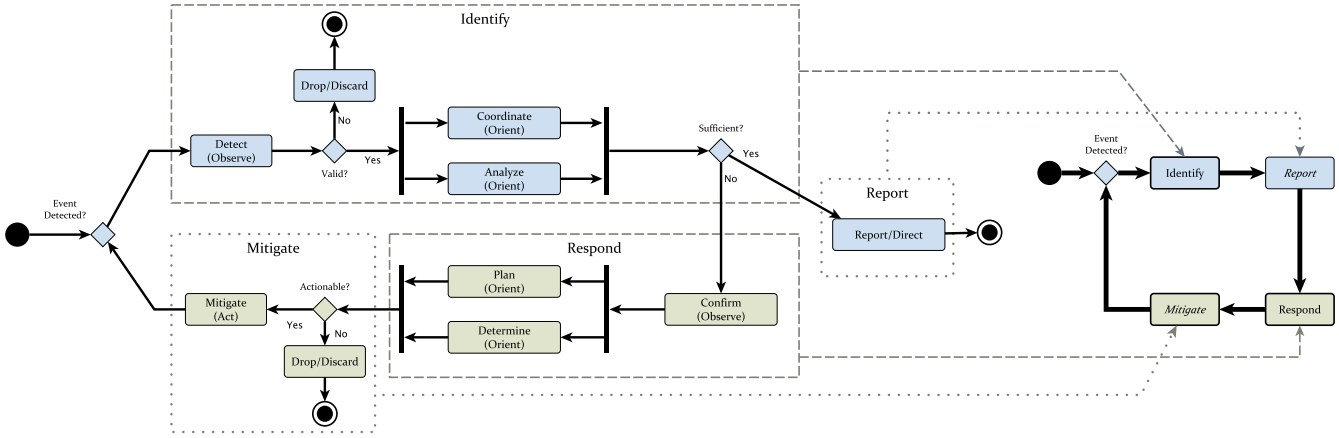


Figure 9. Combined *defend* cycle composed of *identify* and *respond* subcoments and abstracted

information is available to direct further action or reporting to the relevant organization or CSIRT, then the process ends with the appropriate information sent forward. It is critical to note that this does not mean that the incident is resolved as this process model is not tied to any particular incident but is focused on handling various incidents concurrently.

If further action is required, then the relevant IODEF information is passed to the respond loop, which is largely the same as before. However, after orienting on the data, the organization *determines* if the information is actionable. If so, the organization reports as appropriate or directs *mitigation* accordingly and then continues to *monitor*. If the information is not actionable, monitoring still continues, but special attention is given to collecting information that may lead to finding information that is sufficient to develop an actionable plan for mitigation.

VI. The Coordinate Cycle

As shown in Fig. 6, CSIRTs are central to managing reported information and informing the response effort. Within this model there are two types of CSIRTs: an *operational CSIRT* that coordinates between business operations and management and a *strategic CSIRT* that coordinates between management and policy. Differing vocabularies and cultures as well as differences in incident management volume and processing speeds requires CSIRTs that can manage event data, track crosscutting incidents, manage expectations, and assess the state of the overall coordination network. This process cycle is shown in Fig. 10.

The CSIRT coordination process has *triage* and *analyze* phases that are very similar to the *identify* and *response* phases of other roles. However, the functions differ since CSIRTs focus on working across various incidents and organizations. In addition to the *triage* and *analyze* cycles, the *detection* step is separated to account for varying CSIRT detection modalities ranging from simple help desk systems to complicated sensor networks. Similarly, a more comprehensive *communicate* step is added to allow for tailored information processing targeted to the intended audience.

1) Detection and Triage: Initially the CSIRT may receive various types of IODEF objects such as *Incidents*, *Assessments*, *EventData*, *Flows*, or *Records*. Similarly, a CSIRT may control or have access to specialized *detection* sensor networks. In addition, the CSIRT should be particularly attentive to the *Expectation* information as a critical component to coordination. Upon receipt of the information, the validation step is designed to manage incomplete data or

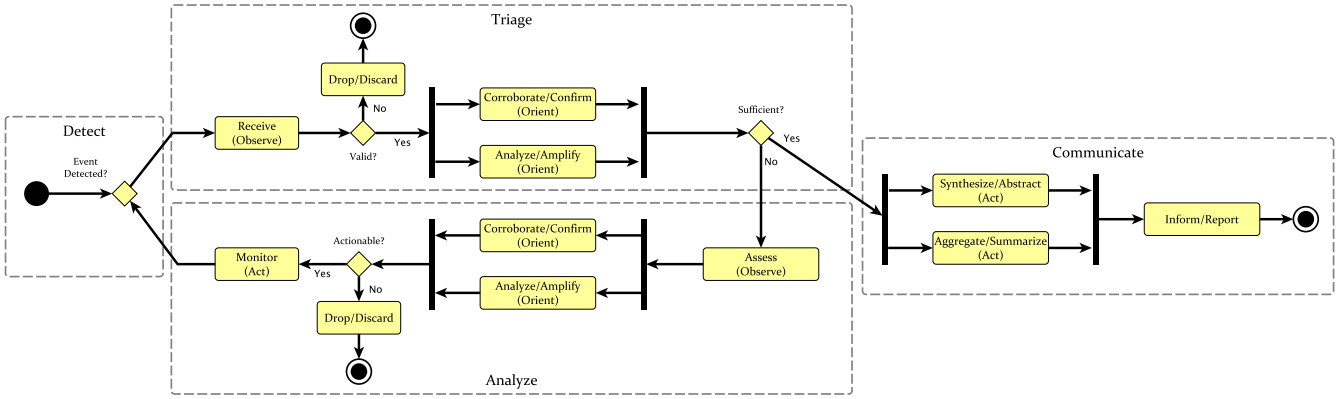


Figure 10. CSIRT *coordinate* loop

data that cannot be accepted for other reasons such as legal restrictions. Once the validation is complete, the CSIRT verifies the information by corroborating the data with other information and confirming plausability of the data and the organization's intent via the relevant IODEF *Contact*. Simultaneously, the CSIRT may draw on its analytic capabilities to gather more information or determine if this *Event* or *Incident* is part of ongoing activity and *triage* accordingly. Finally, the CSIRT determines if the data is sufficient to drive *communications* to external organizations. If so, the processes described in the *communications* phase are executed. If not, further *analysis* is conducted until enough information is available for developing mitigation approaches or advising better *detection* methodologies.

2) Communications: If information is sufficient to drive reporting and actionable enough to support specific mitigation and monitoring efforts, it may be supplemented by other information through synthesis or generalized through abstraction. In addition, aggregation or summarization may result in trend reporting or in combining IODEF elements into larger groups. Once these steps are completed, information can be passed forward to the appropriate parties.

3) Analysis: Should further analysis be required, the CSIRT continues to corroborate and analyze until a determination can be made as to the actionability of the data. If the analysis does not result in a reasonable course of action, the CSIRT might notify the *Contact* or coordinate with system and sensor owners to get more data. If the information is actionable, it is processed as described in step two and the CSIRT continues to monitor for related activity for a resonable amount of time.

VII. Example Use Case

Fig. 11 shows how the coordination network might work during a crosscutting incident with some steps enlarged in Fig. 12. In addition, the timing and communication diagrams in Fig. 13 and Fig. 14 illustrate how IODEF information could flow in a coordinated incident handling model. For our example, we will use a distributed denial of service (DDoS) attack against the government occurring over a holiday weekend. Only the first three steps will be described in detail with steps four through six described more generally in order to illustrate the

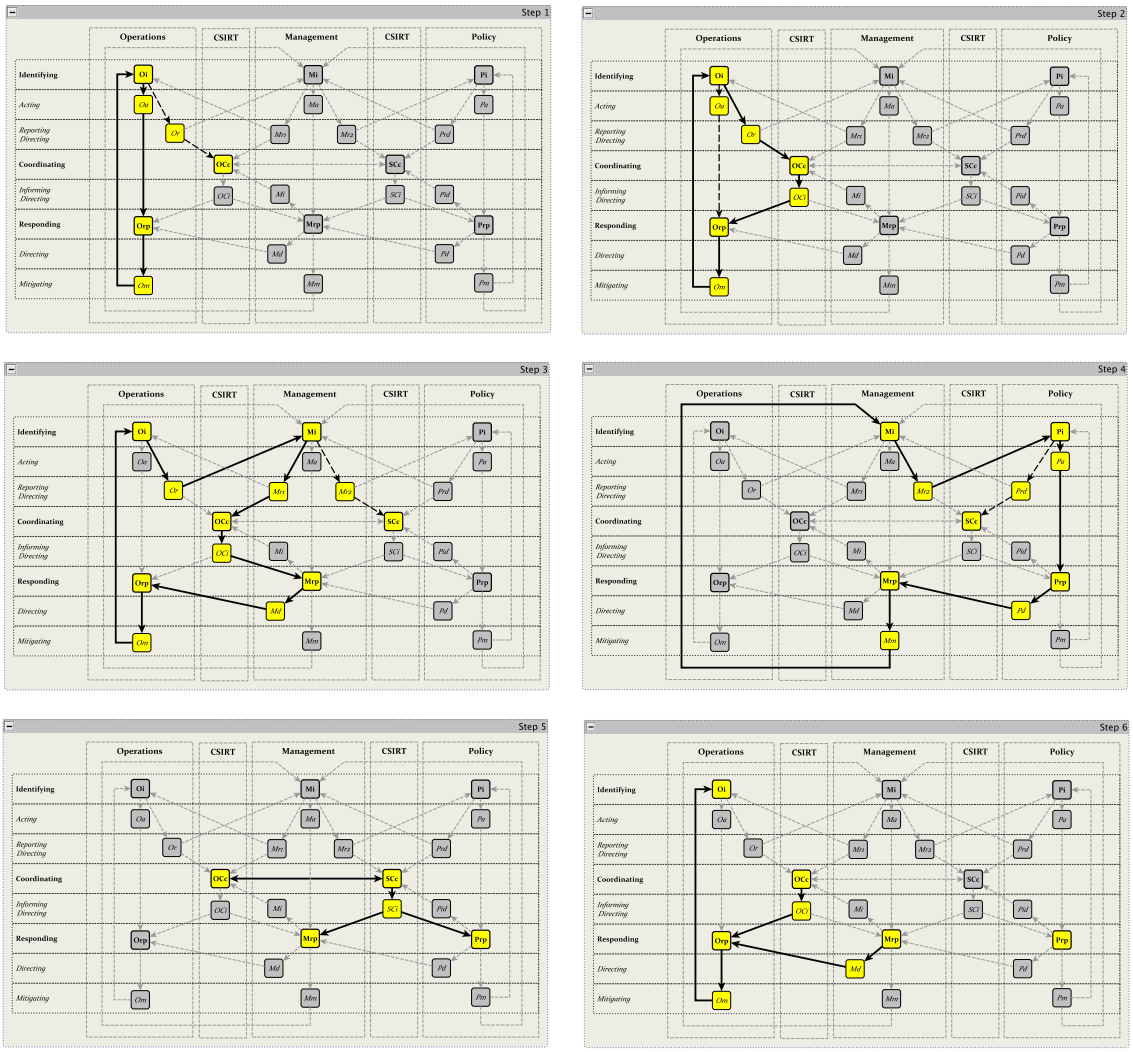


Figure 11. Use case coordination network steps

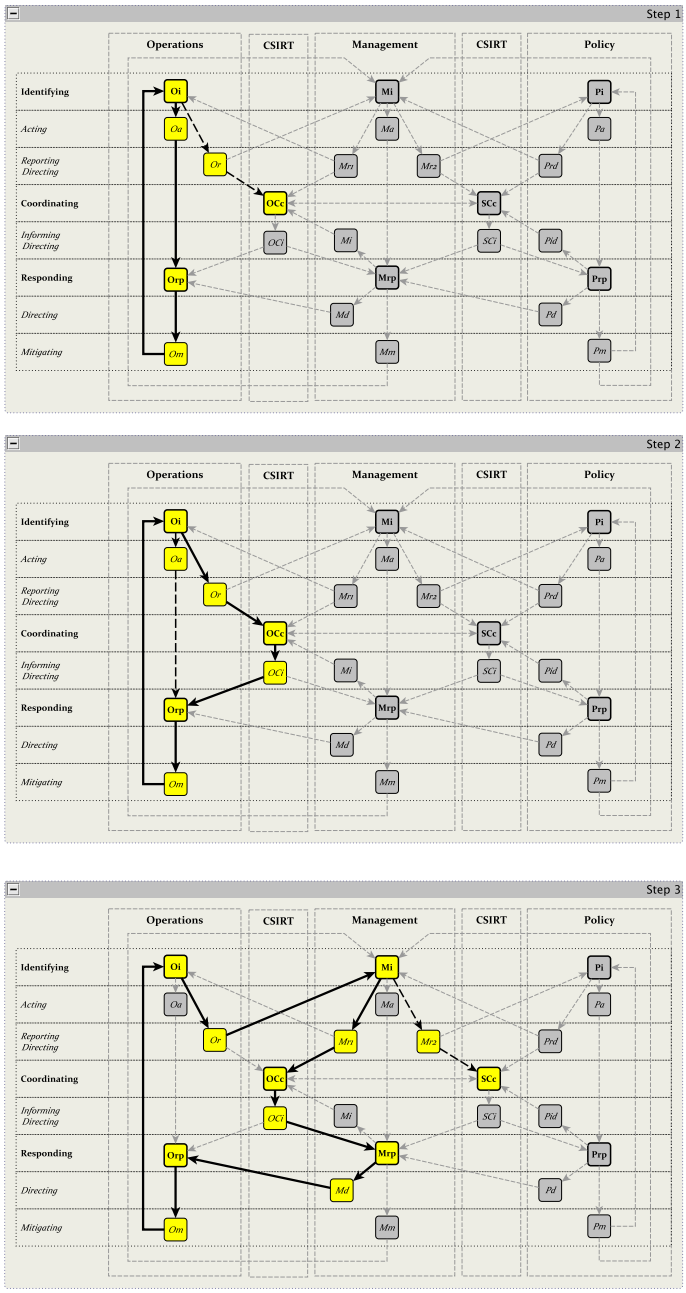


Figure 12. Steps one through three for a distributed denial of service scenario

integration of policy rather than the mechanics of the coordination network. For this reason the timelines in Figs. 13 and 14 only span through step three.

A. Step one: Ops defense & CSIRT communications

Initially two separate organizations identify that their public facing websites have been overwhelmed and are unresponsive. As shown in the Fig. 13, Ops A identifies three separate website attacks, depicted as red diamonds, at t_1, t_2, and t_3. Ops B is hit simultaneously at t_2. Both of these organizations are depicted in Fig. 12 as *Oi* nodes. In a full simulation of the network one might have various organizations executing the functions represented by the nodes in the network. For simplicity in this scenario, only the *Oi* node represents two separate organizations. Both Ops A and B immediately invoke their internal incident management procedures, represented by *Oa*, and notify their common response (*Orp*) personnel at t_4 and t_6 by passing *EventData* (◆ in Fig. 14) and *Assessments* ◆. Bundled with the *EventData* ◆, they each include *Expectation* information asking about the extent of the attack. During this process they also submit incent report forms (*Or*) to the operational CSIRT (*OCc*) for coordination. Because the acting and reporting steps happen nearly simultaneously they are shown as one step (*Oa/r*) in Fig. 13. In addition, the same timing diagram shows that the response element (*Orp*) starts processing information every ten cycles and that subsequent action (*Om*) takes five cycles. This is included in the example to show how the coordination network can depict batch processes occurring at regular intervals. In this early stage of the scenario, the response organization simply notifies each

organization at t_{16} about the recent activity via IODEF *History* items.

B. Step two: coordination with the operational CSIRT

While the attacks in step one are winding down, Ops A (*Oi*) is once again attacked at t_{15}. Having already mobilized to work through the first set of attacks, the personnel in charge of public facing web servers are closely monitoring other possible targets and are able to quickly identify the likely IP addresses of the attackers. Because the third DDoS shows a pattern of attacks on websites associated with a particular subset of government websites, Ops A uses a *Method* object at t_{20} to pass the information (*Or*) for dissemination through the CSIRT (*OCc*) and sends a copy (*Oa*) to response (*Orp*). As with step one, acting and reporting are shown as one step (*Oa/r*). Based on the new information, the CSIRT determines other IP ranges that might be attacked and communicates (*OCi*) that information to the business operations response group at t_{24} via a *System* object and also passes relevant *Contact* information. This information is subsequently passed to Ops A and B via *Om* at t_{31}. As is shown in the diagram, as the scope and complexity of the incident increases, the longer that it takes for information to be processed. The fact that step one and two overlap demonstrates concurrent activity within the network allowing Ops A and B to return to identifying events (*Oi*) as soon as acting (*Oa*) or reporting (*Or*) is complete.

C. Step three: working with management and notifying policy

After receiving the potential target list from the CSIRT, in step two, Ops B sees attack on CIDR at t_{34} and passes (*Or*) information (*EventData* , *Assessment*) to the business process owners (*Mi*) at t_{38}. The business process owners subsequently add possible targets of the attack and pass the information (*Mr1*) to the operational CSIRT (*OCc*) at t_{60}. Fearing more sophisticated or malicious attacks, this information is bundled as an *Incident* with a broader *Assessment* and is also forwarded (*Mr2*) at t_{80} to the strategic CSIRT (*OCs*). Based on the information received at t_{60}, the operational CSIRT (*SCc*) passes on more information (*OCi*) to the management response effort (*Mrp*) t_{90} about the *Methods* being used for the attack and possible mitigation strategies.

As a result, at t_{105} management directs (*Md*) operations (*Orp*) to get essential personnel working to check and harden potential targets and in coordination with the CSIRT sends *System* information consisting of the IP addresses and domain names that might be targeted which is subsequently passed from operations response (*Orp*) for mitigation and monitoring.

D. Steps four through six: monitoring the mission, mitigation, and policy planning

Since steps one through three demonstrate the use of the coordination network, timing diagram, and communications diagram, the remaining steps are described more succinctly to describe the role of policy and are not depicted in Figs. 12 through 14.

In step four, having received the expanded *System*

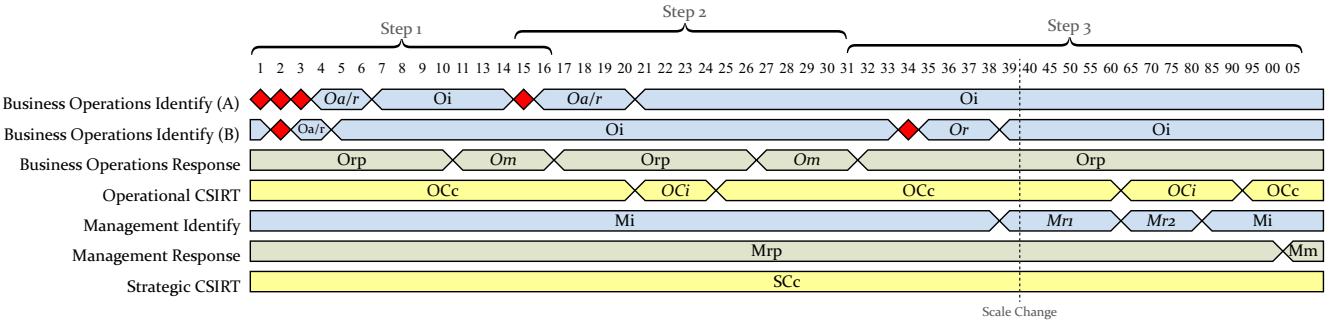


Figure 13. Timing diagram for first three steps of scenario

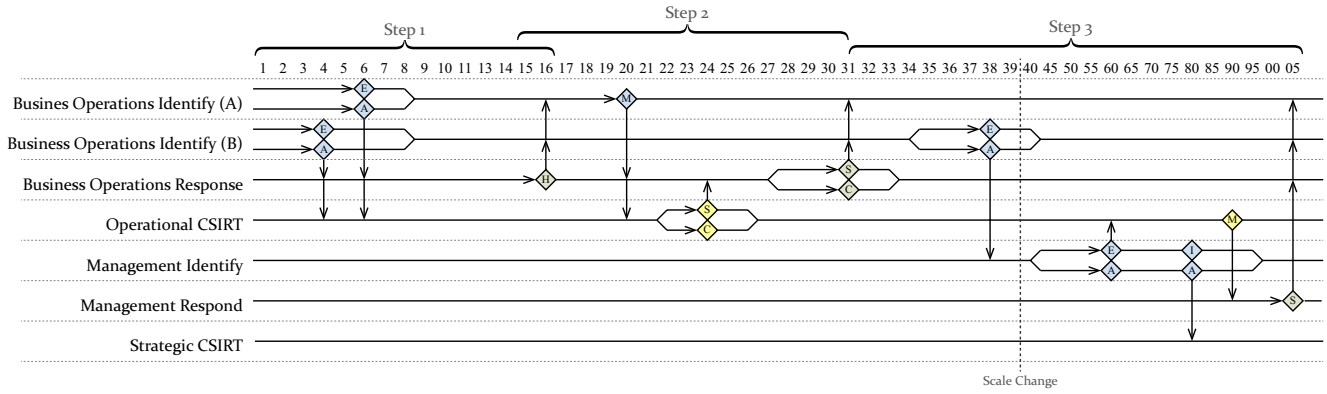


Figure 14. Communications diagram for first three steps of scenario

watchlist, business process owners determine that some of their software application errors could be related to attacks on web services. This information is passed to policy with an *Assessment* that further system degradation could negatively impact that organization's ability to execute one of its business functions. Policy contacts the CSIRT and simultaneously oversees or directs the activation of relevant managerial, operational, or multi-organizational response teams or incident management operations centers. Step 5 represents the actions of this joint response team determining how to respond to the incident. Finally, in Step 6, this guidance is disseminated via the operational CSIRT and management response group. In addition, the policy response elements start long-term work to assess what policy measures might be needed to coordinate such crosscutting incidents in the future.

VIII. Conclusion

While significant effort has been dedicated to designing individual cybersecurity processes, taxonomies, and data formats, little has been done to integrate cybersecurity incident handling processes and determine how existing standards and formats should work within an incident handling system. Similarly, various linear life cycles have been promulgated, but limited progress has been made toward describing how incident handling might happen at scale, with minimal interdependencies, and while allowing for concurrence.

By mapping to an established taxonomy, designing for compatibility with a decision cycle, and allowing for inter-organizational coordination among organizations with different roles, we have outlined the first steps toward an incident handling process model that is simple enough for a wide range of scenarios while formal enough to allow rigorous modeling and simulation. The *identify* and *respond* cycles serve as the building blocks that combined with the *ops*, *management*, and *policy* roles provide for a much more comprehensive model of cybersecurity incident handling than those in current publications. The critical *coordinate* cycle serves to interface between the three identified organizational roles through the *CSIRT* while allowing for information triage and processing of incident data. Using this approach, future work can identify the role of other relevant data formats, continue to formalize the network, simulate incident communications using these models, use the same organizing principles to help inform the software engineering of relevant systems, and explore cybersecurity state estimation using the coordination network model.

References

[1] G. Killcrece, K. Kossakowski, R. Ruefle, and M. Zajicek, "State of the practice of computer security incident response teams (CSIRTs)," Carnegie Mellon Software Engineering Institute, Oct. 2003.

[2] B. Kim, "Computer security incident handling guide," National Institute of Standards and Technology, Jul. 2004, Special Publication 800-61 (SP 800-61).

[3] "Information assurance (IA) computer network defense (CND) volume I (incident handling program)," Chairman of the Joint Chiefs of Staff, Jun. 2009, CJCSM 6510.01A.

[4] "Enabling distributed security in cyberspace," Department of Homeland Security, National Protection and Programs Directorate, March 2011.

[5] "The national strategy to secure cyberspace," Executive Office of the President, February 2003.

[6] E. E. Schultz, D. S. Brown, and T. A. Longstaff, "Responding to computer security incidents: Guidelines for incident handling," University of California, Lawrence Livermore National Laboratory, Jul. 1990.

[7] C. Alberts, A. Dorofee, G. Killcrece, and R. R. M. Zajicek, "Defining incident management processes for csirts: A work in progress," Carnegie Mellon Software Engineering Institute, October 2004.

[8] J. G. Grimes, "National information assurance (IA) approach to incident management (IM)," Committee for National Security Systems (CNSS), Jul. 2004, CNSS-048-07.

[9] C. Blackwell, "Improved situational awarenss and response with enhanced OODA loops," in CSIIRW '10, 2010.

[10] G. M. Schechtman, "Manipulating the OODA loop: The overlooked role of information resource management in information warfare," Ph.D. dissertation, Air Force Institute of Technology, 1996.

[11] A. N. Steinberg, C. L. Bowman, and F. E. White, "Revisions to the JDL data fusion model," B. V. Dasarathy, Ed., vol. 3719, no. 1. SPIE, 1999, pp. 430–441.

[12] E. Shahbazian, D. E. Blodgett, and P. Labbe, "The extended OODA model for data fusion systems," in Fusion 2001, 2001.

[13] P. K. Davis, J. Kulick, and M. Egner, "Implications of modern decision science for military decision-support systems," RAND Corporation, Tech. Rep. MG-360, 2005.

[14] P. Salmon, N. Stanton, G. Walker, and D. Green, "Situation awareness measurement: A review of applicability for C4i environments," Applied Ergonomics, vol. 37, no. 2, pp. 225 – 238, 2006.

[15] K. Wallenius, "Support for situation awareness in command and control," in In Proc. of the Seventh Int. Conf. on Information Fusion FUSION 2004, 2004, pp. 1117–1124.

[16] E. Koivunen, "Effective information sharing for incident response coordination," Ph.D. dissertation, Aalto University, 2010.

[17] "Introduction to the national information exchange model (NIEM)," NIEM Program Management Office, Tech. Rep., February 2007.

[18] J. F. Sowa, Knowledge Representation: Logical, Philosophical, and Computational Foundations. Course Technology, 2000.

[19] M. R. Endsley, "Toward a theory of situation awareness in dynamic systems," Human Factors: The Journal of the Human Factors and Ergonomics Society, vol. 37, pp. 32–64(33), March 1995.

[20] W. S. Angerman, "Coming full circle with boyd's OODA loops ideas: An analysis of innovation diffusion and evolution," Ph.D. dissertation, Air Force Institute of Technology, 2004.

[21] G. P. Tadda and J. S. Salerno, Cyber Situational Awareness, ser. Advances in Information Security. Springer, 2010, ch. Chapter 2 - Overview of Cyber Situation Awareness.

[22] S. Dekker and E. Hollnagel, "Human factors and folk models," Cogn. Technol. Work, vol. 6, pp. 79–86, May 2004.

[23] J. M. Fuster, "Upper processing stages of the perception-action cycle," Trends in Cognitive Sciences, vol. 8, no. 4, pp. 143 – 145, 2004.

[24] J. W. Bodnar, Warning Analysis for the Information Age: Rethinking the Intelligence Process. Center for Strategic Intelligence Research, Joint Military Intelligence College, December 2003.

[25] A. Dahlbom, "Petri nets for situation recognition," Ph.D. dissertation, Orebro University, 2011.

[26] J. D. Howard and T. A. Longstaff, "A common language for computer security incidents," Sandia National Laboratories, Tech. Rep., October 1998.

[27] "The incident object description exchange format," IETF, December 2007, RFC 5070.

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.

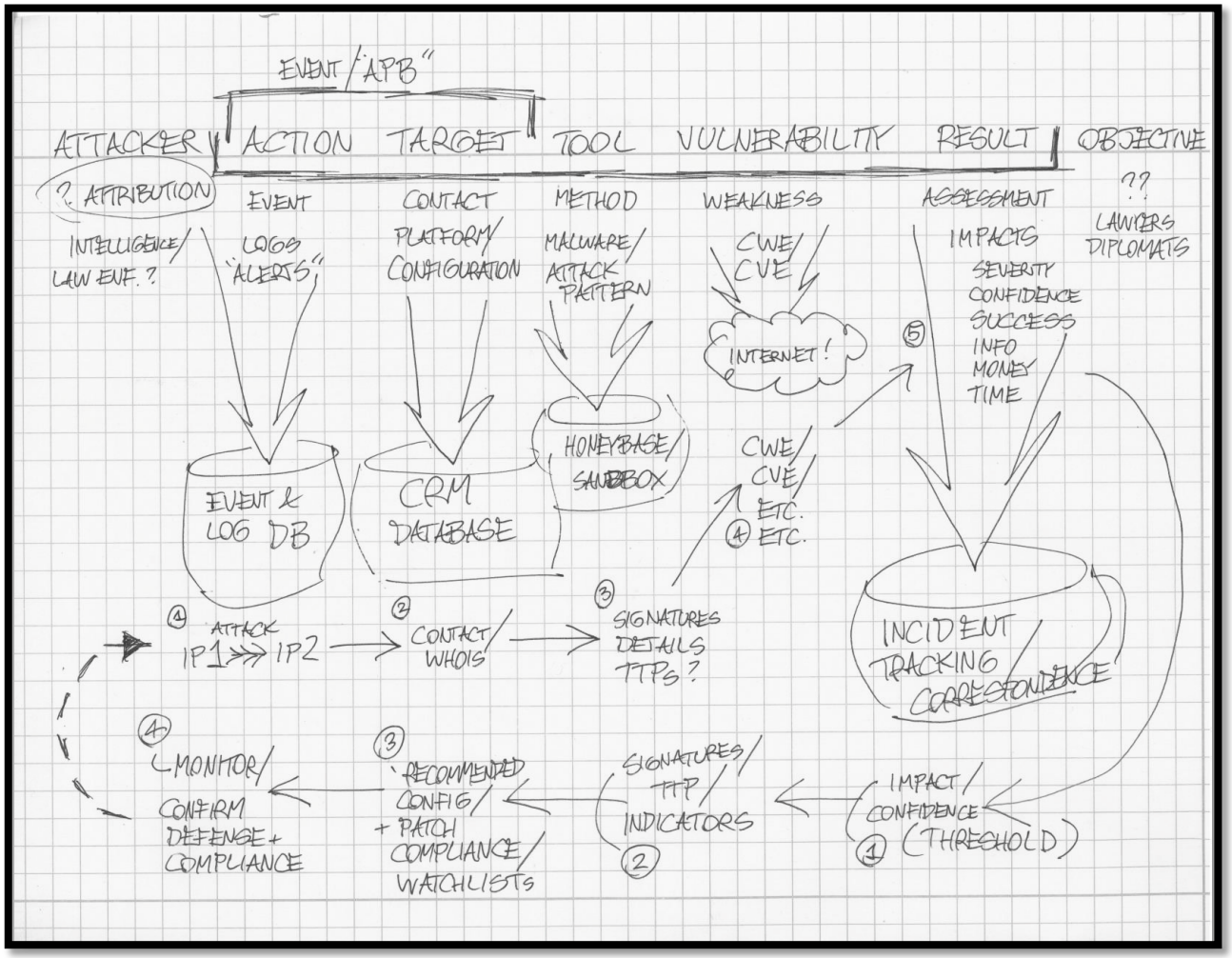
US-CERT + NIST + JHU/APL

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

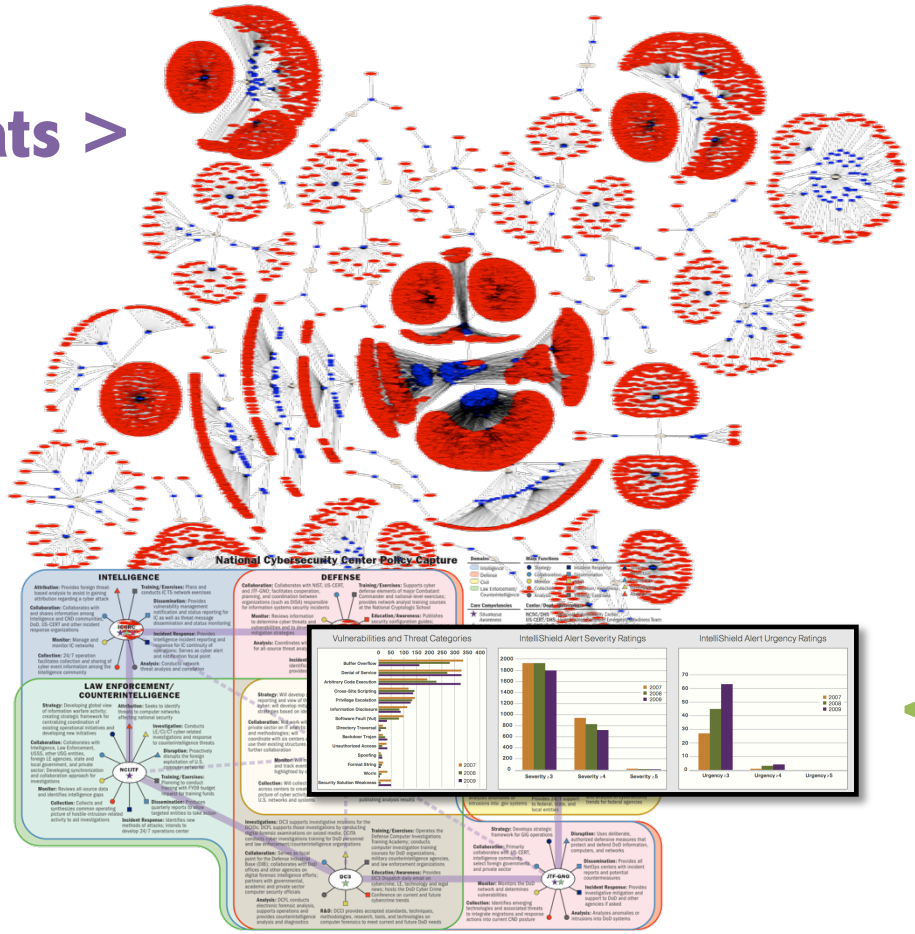
Activities & Processes

Federal-civil network defense

[*] Meadows, *Thinking in Systems*

Complexity & Heterogeneity

complex threats >



cyber centers >

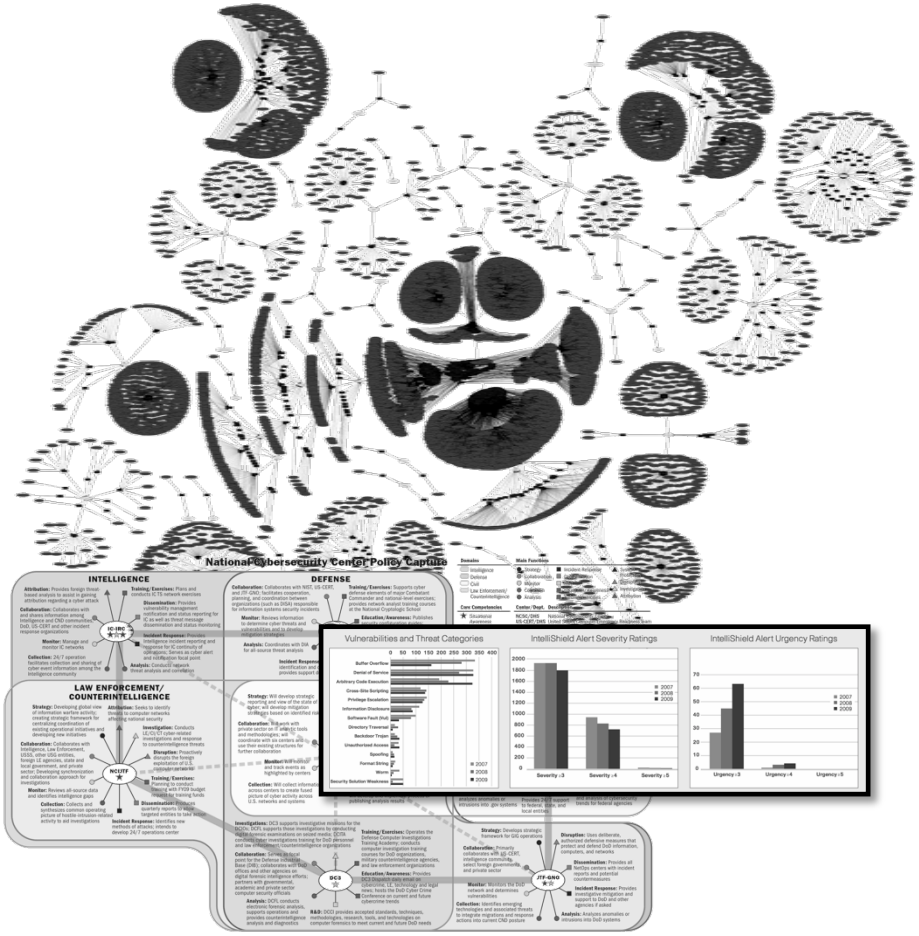
< threat types

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

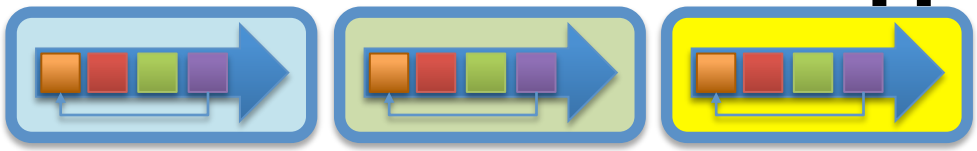
1990: Lawrence Livermore National Labs

2004: US National Institute of Standards and Tech.

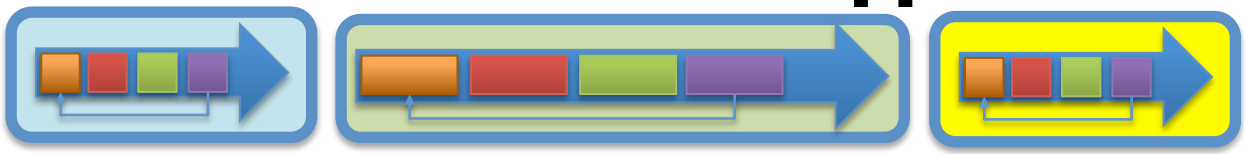
2009: Chairman of the Joint Chiefs of Staff

What about multiple incidents?

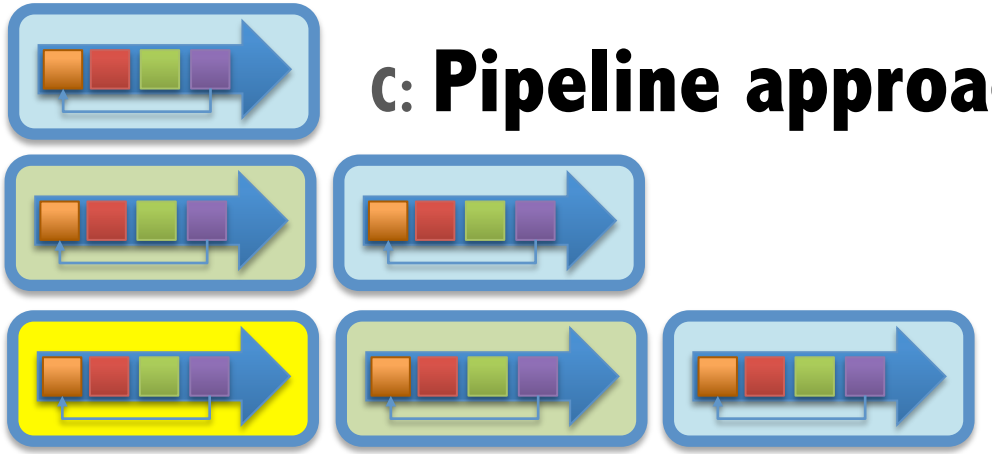
A: Serial constant time approach



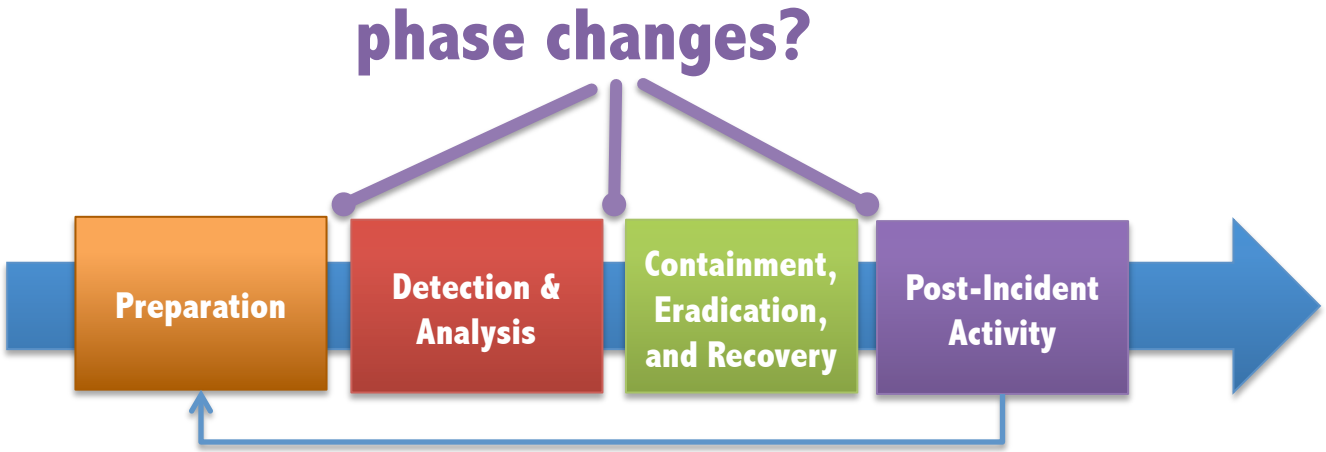
B: Serial variable time approach

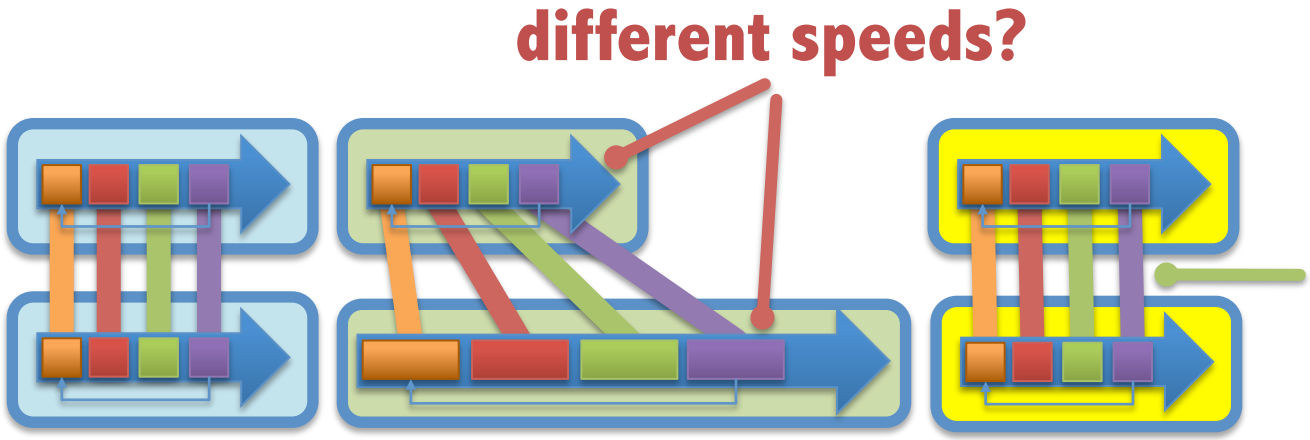


C: Pipeline approach



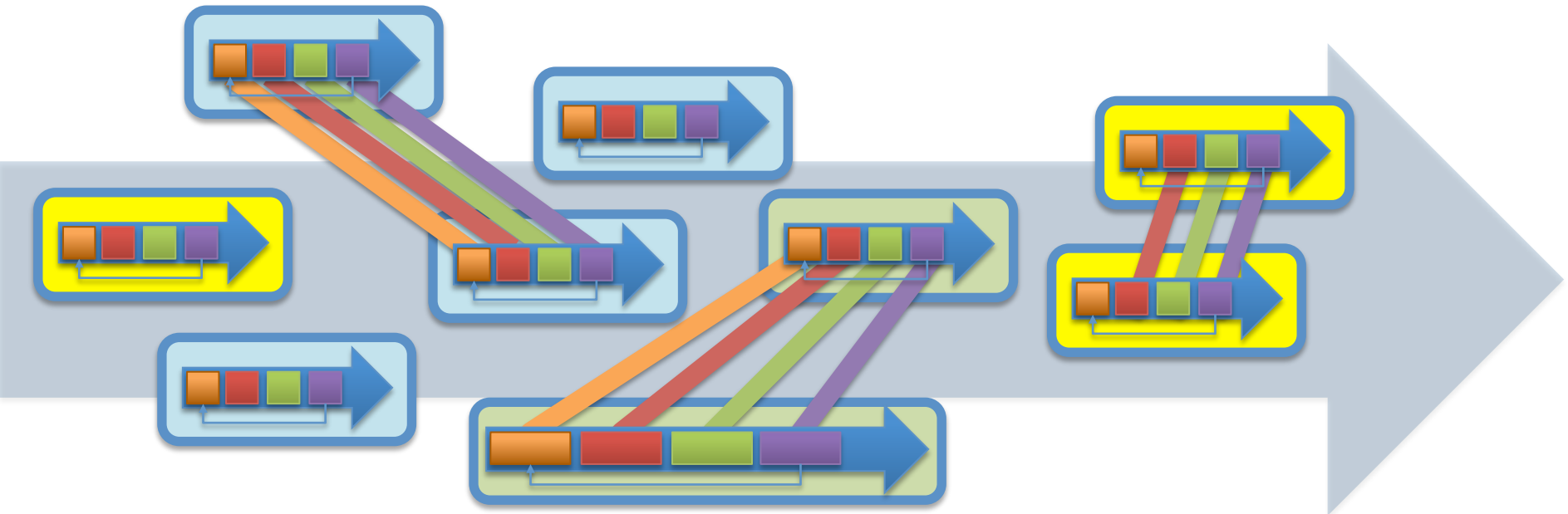
What about cross-cutting incidents?





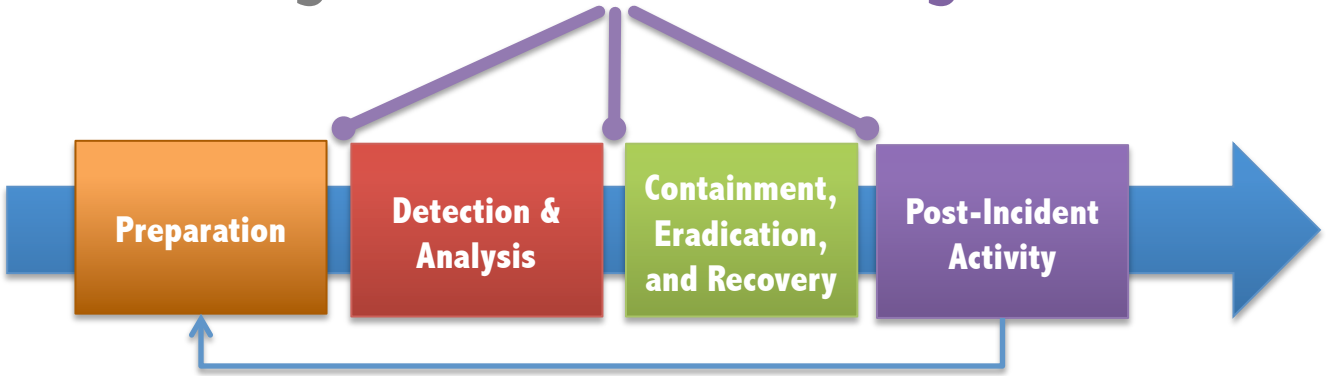
information and sharing?

So how could we deal with it?

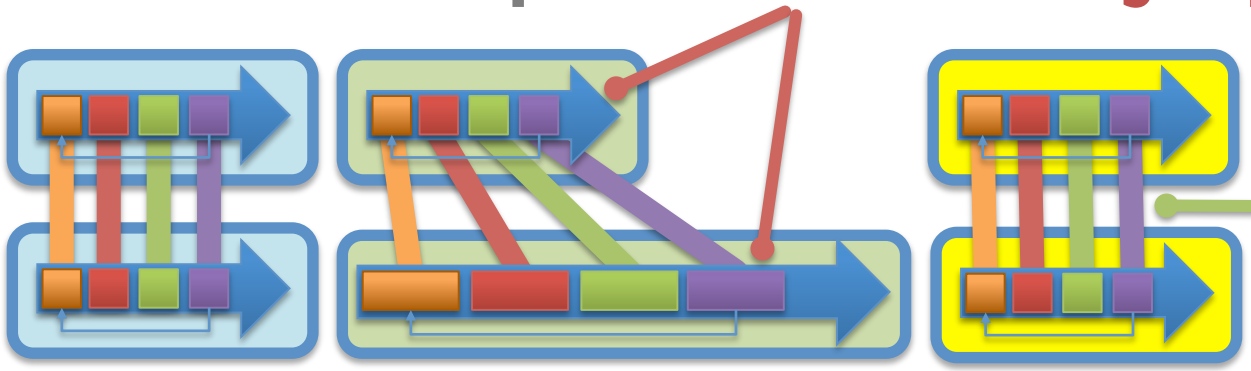


Three broad answers

phase changes? focus on handling activities not an incident



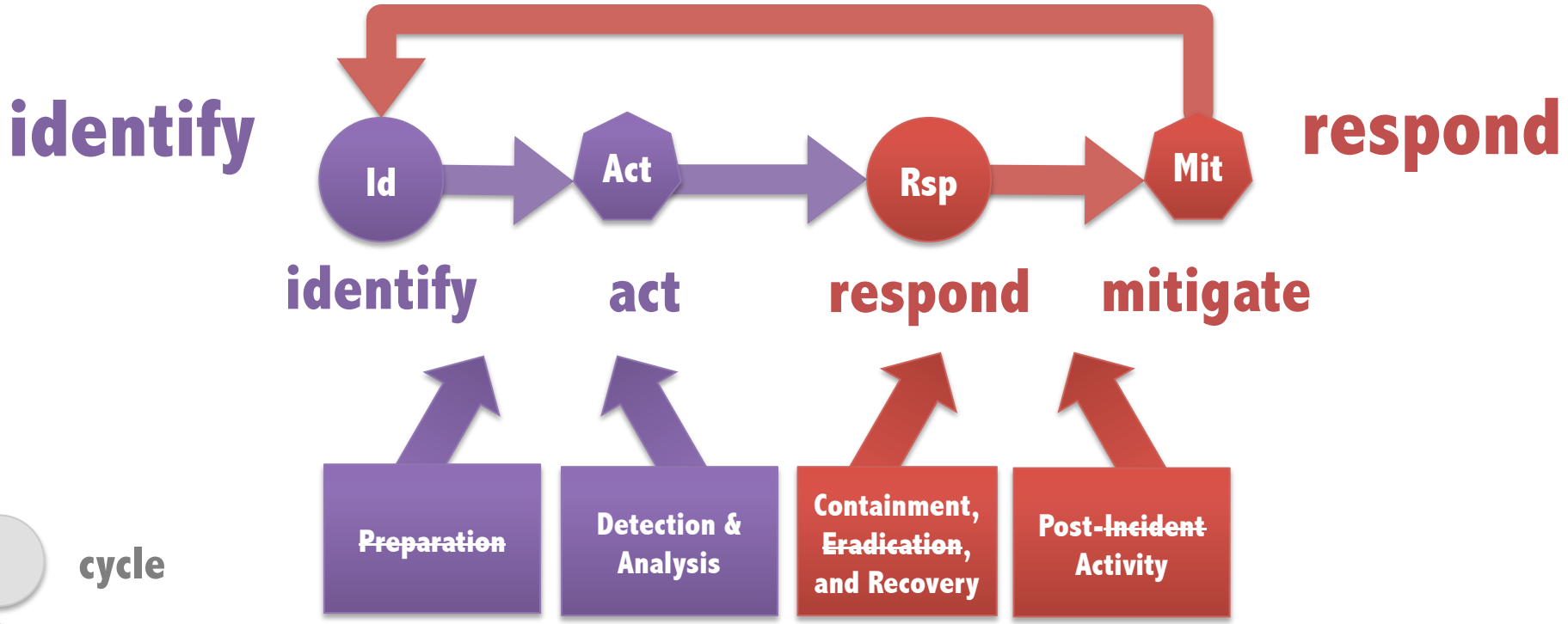
different speeds? reduce locking dependencies



information and sharing? standard data, common activities

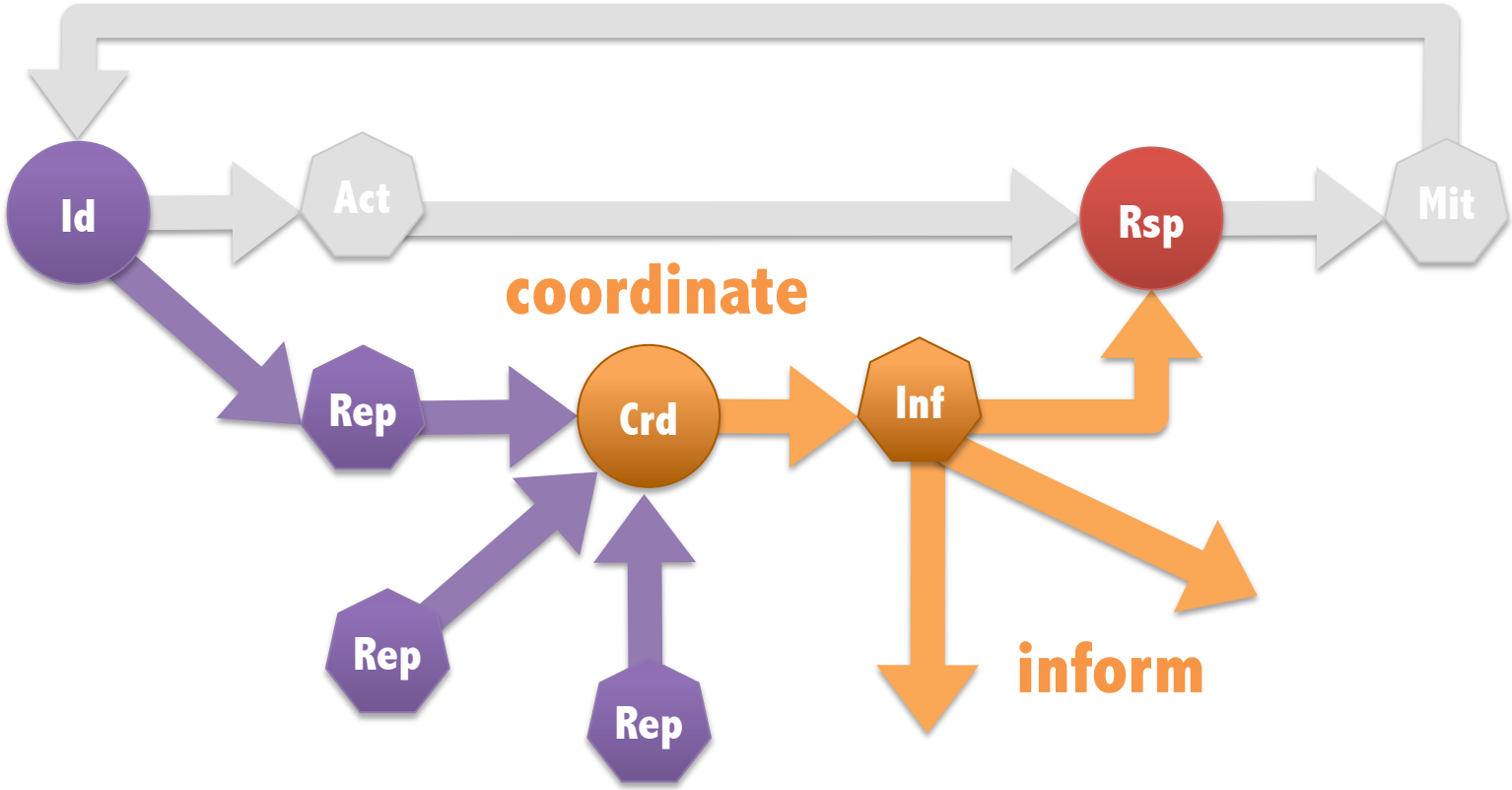
1. Focus on activities

phase changes? focus on handling activities not an incident

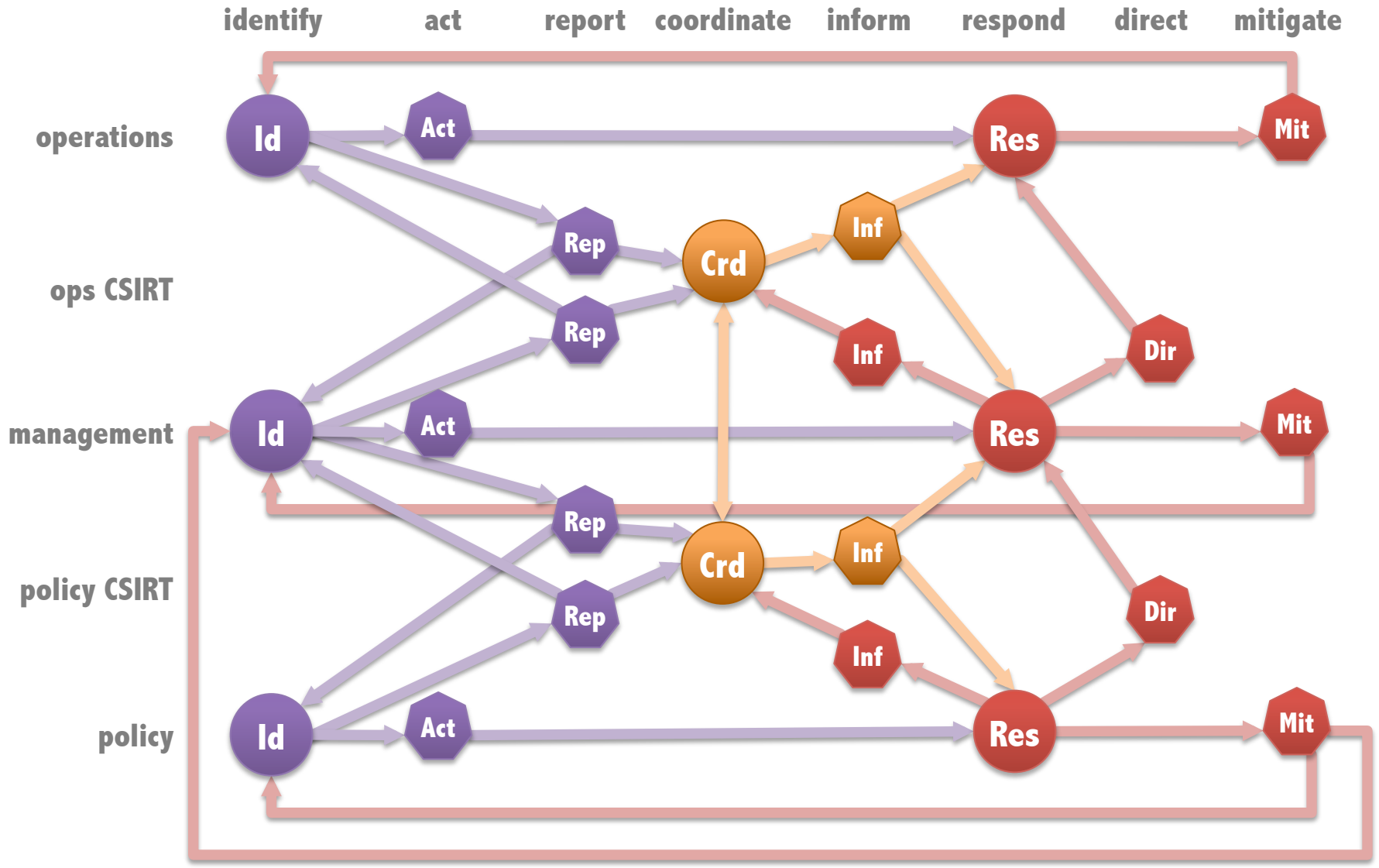


2. Reduce locking dependencies

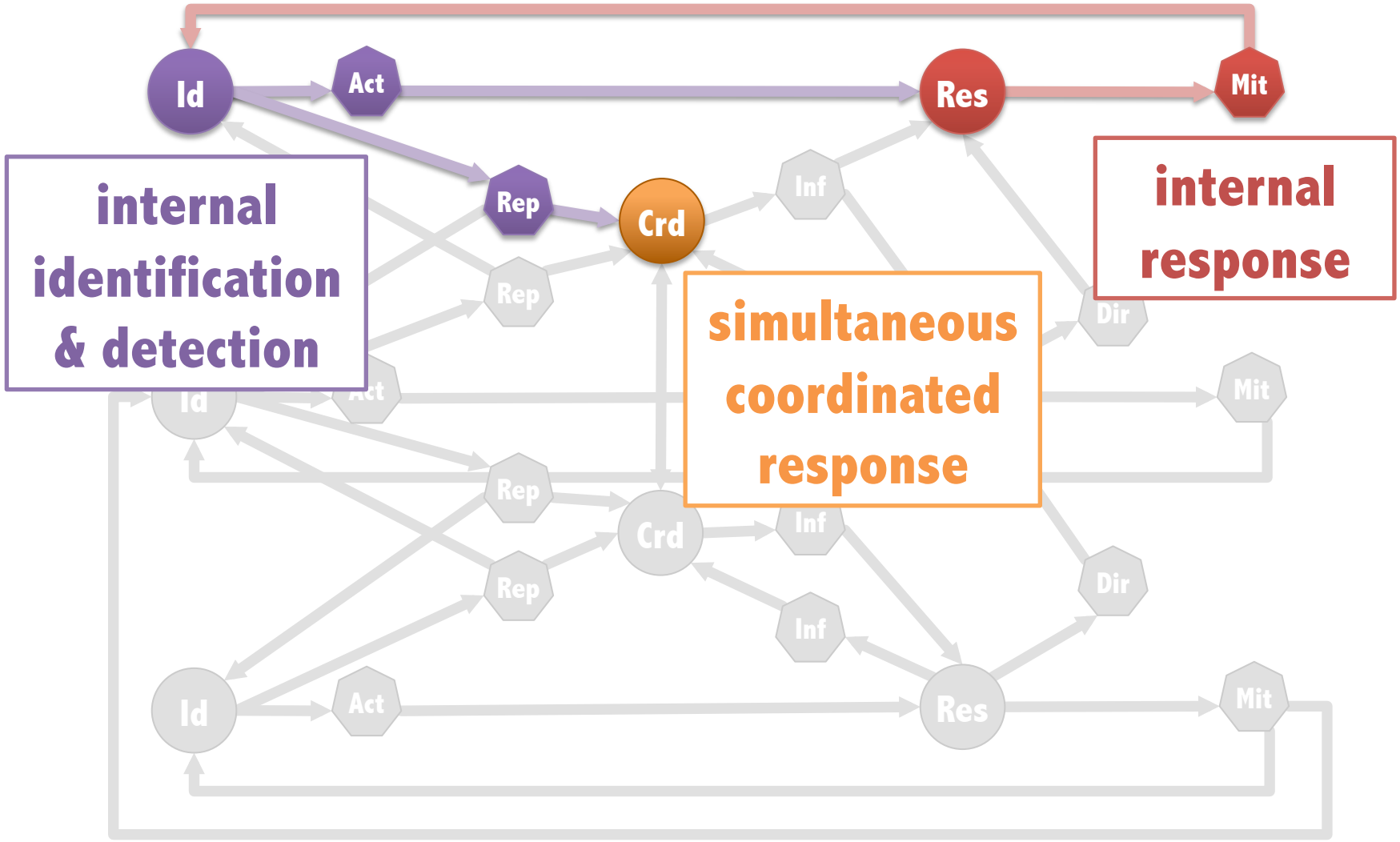
different speeds? reduce locking dependencies



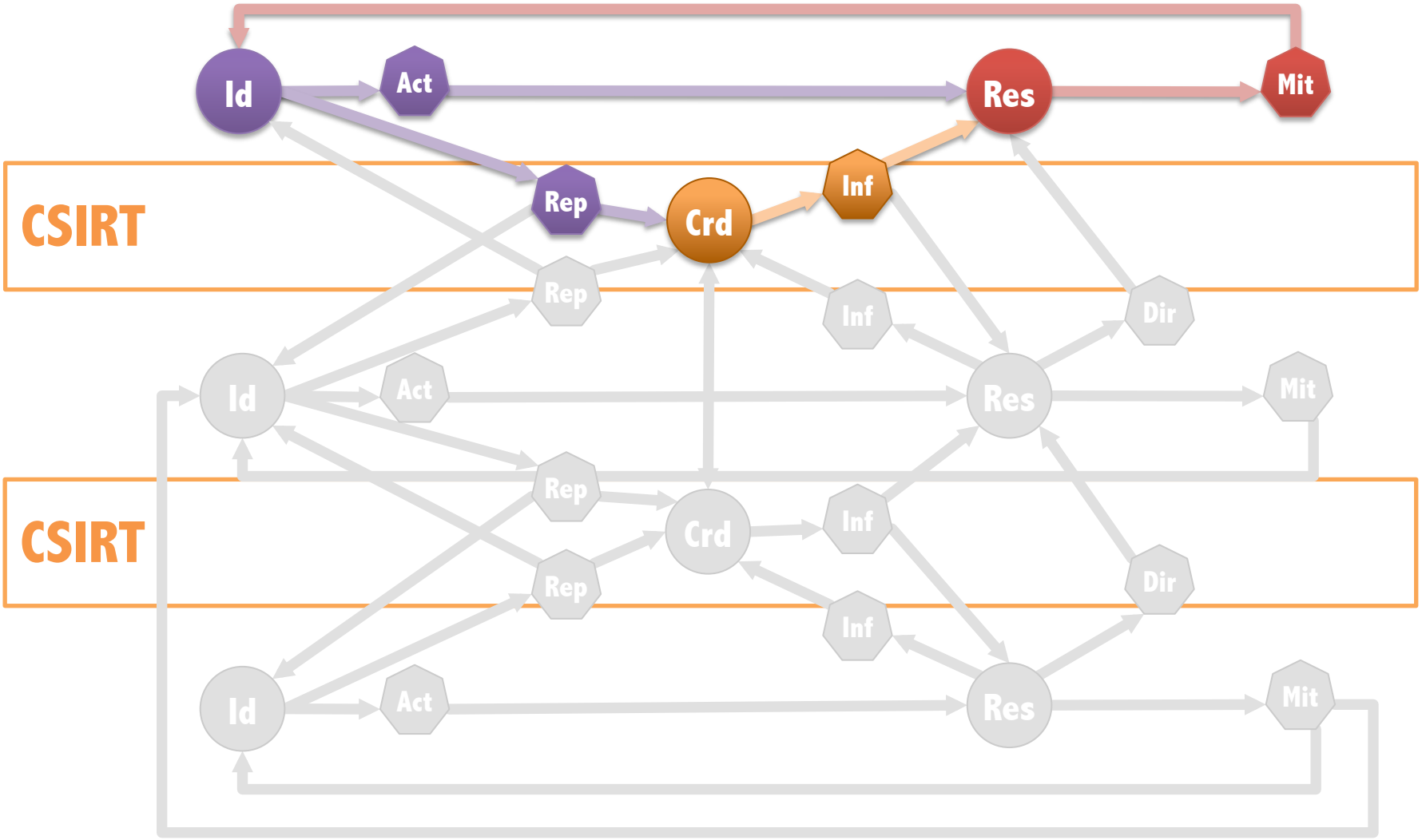
Which: allows for complex system



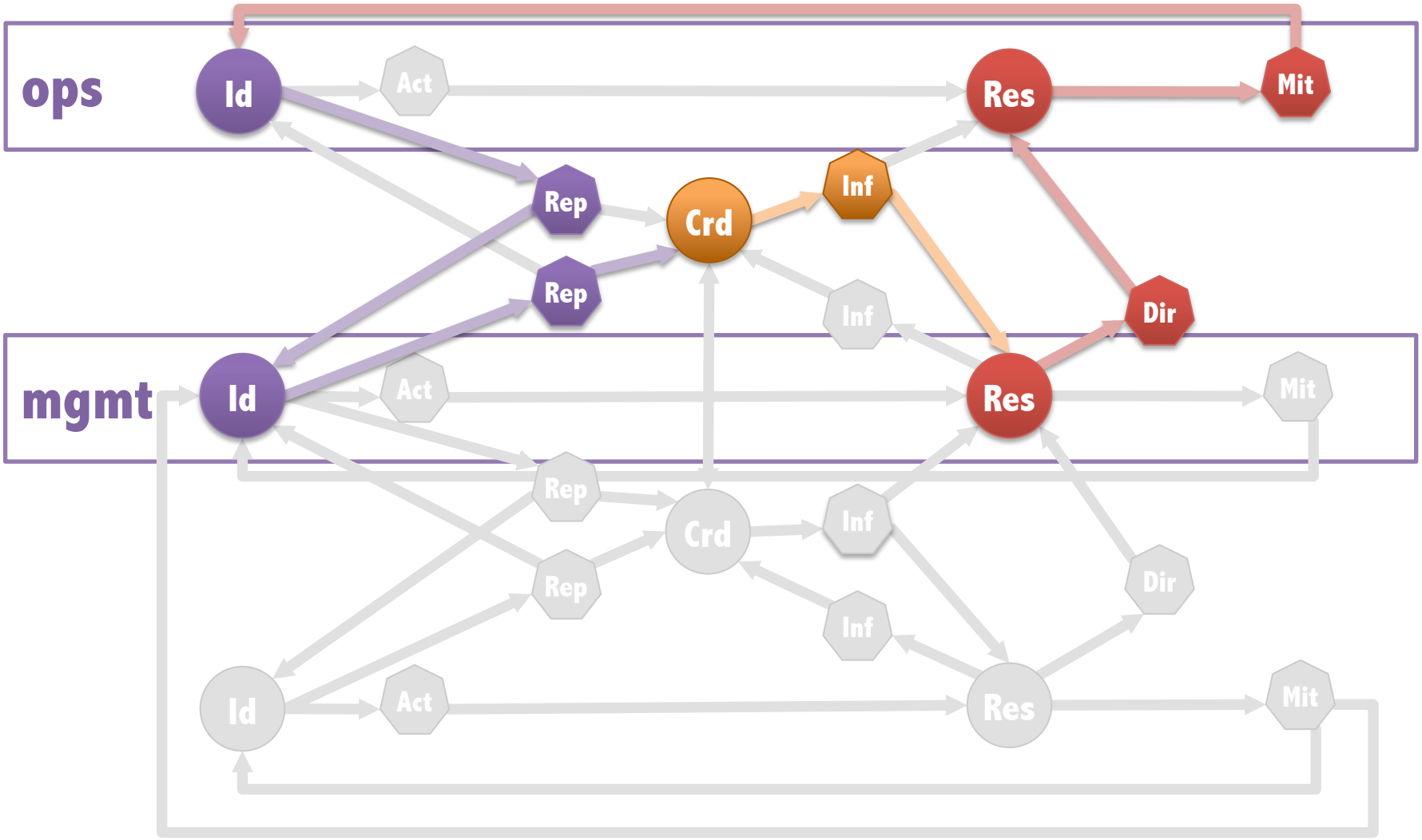
Allows for multiple, concurrent flows



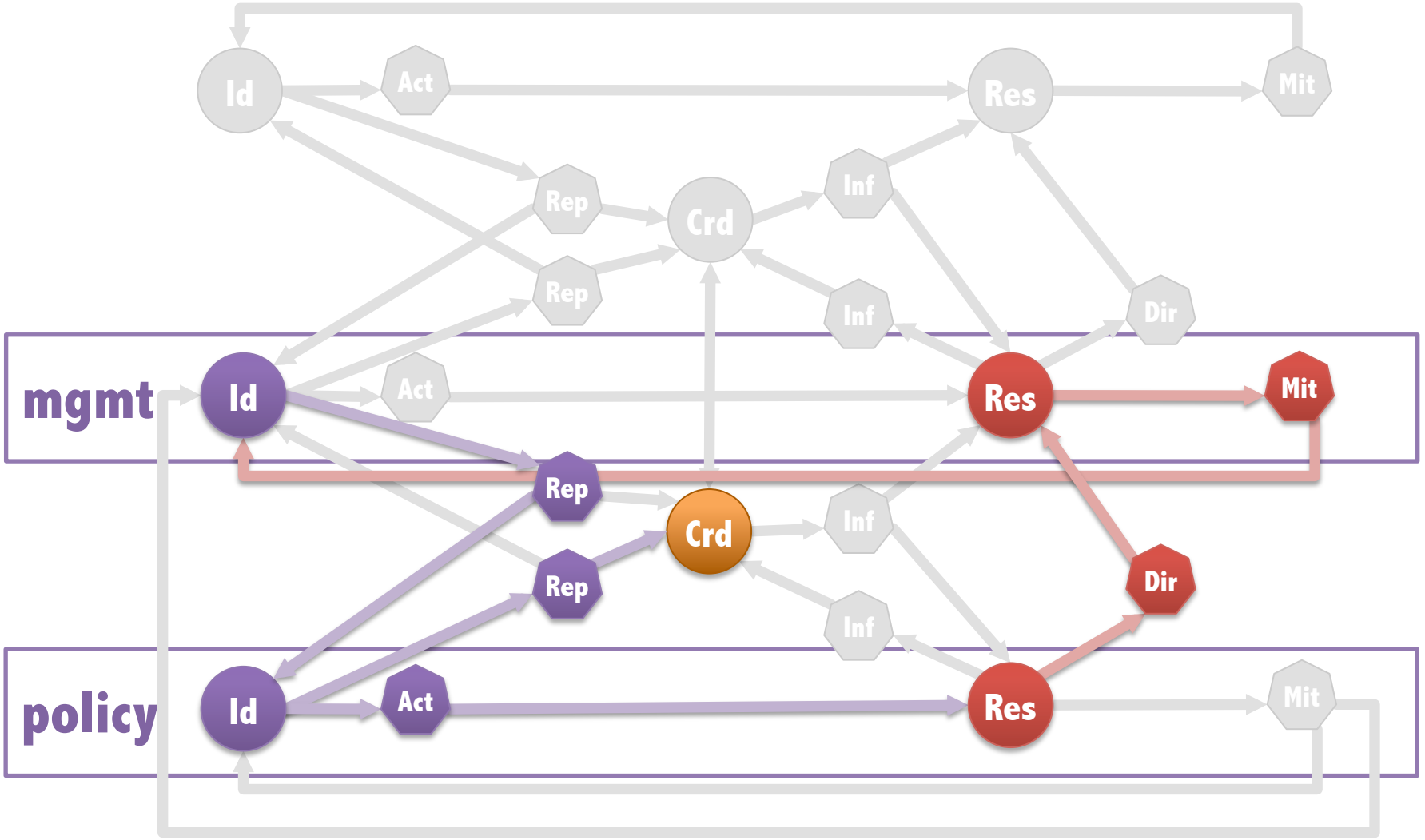
Accounts for role of CSIRT



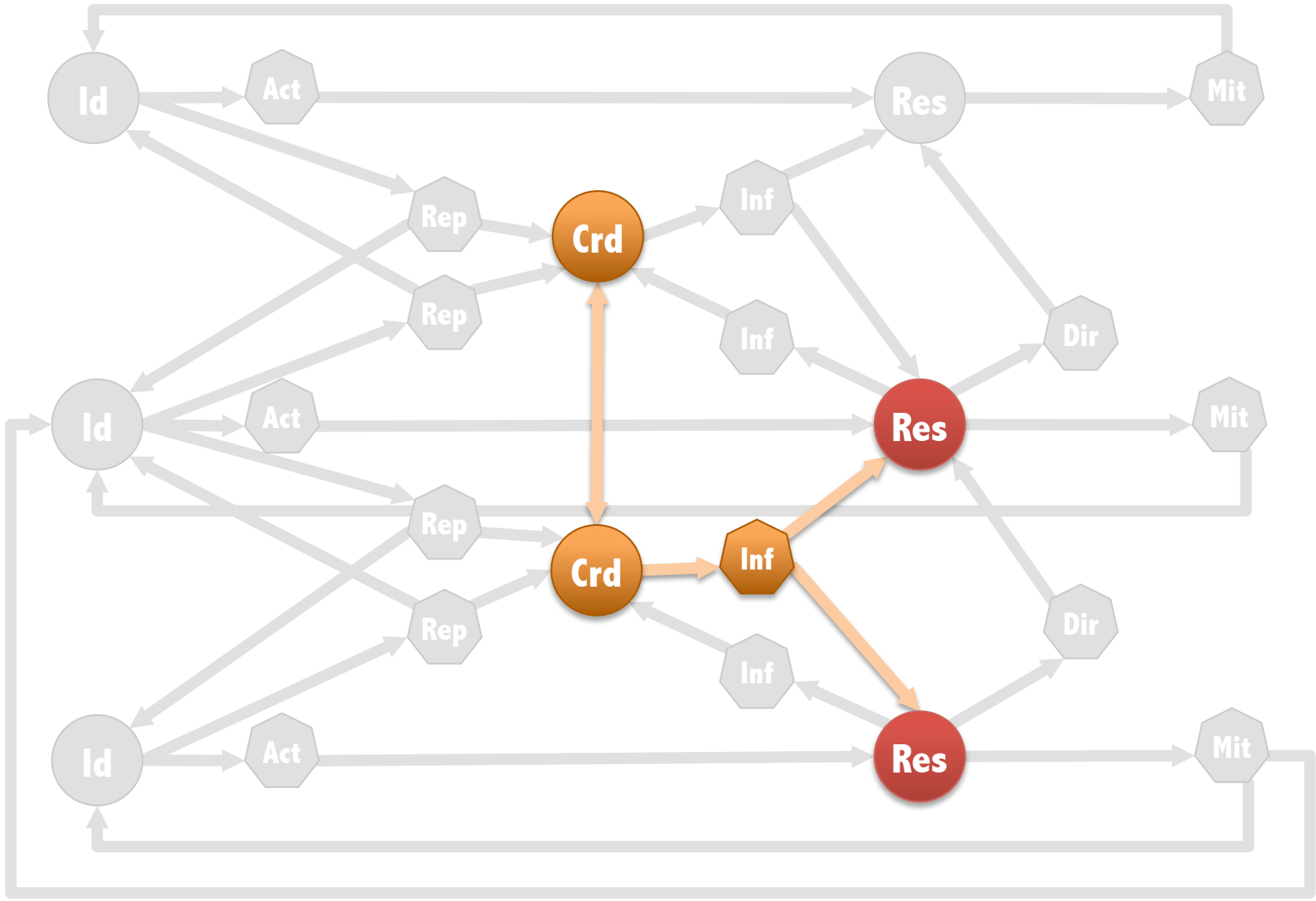
Allows for integration of management



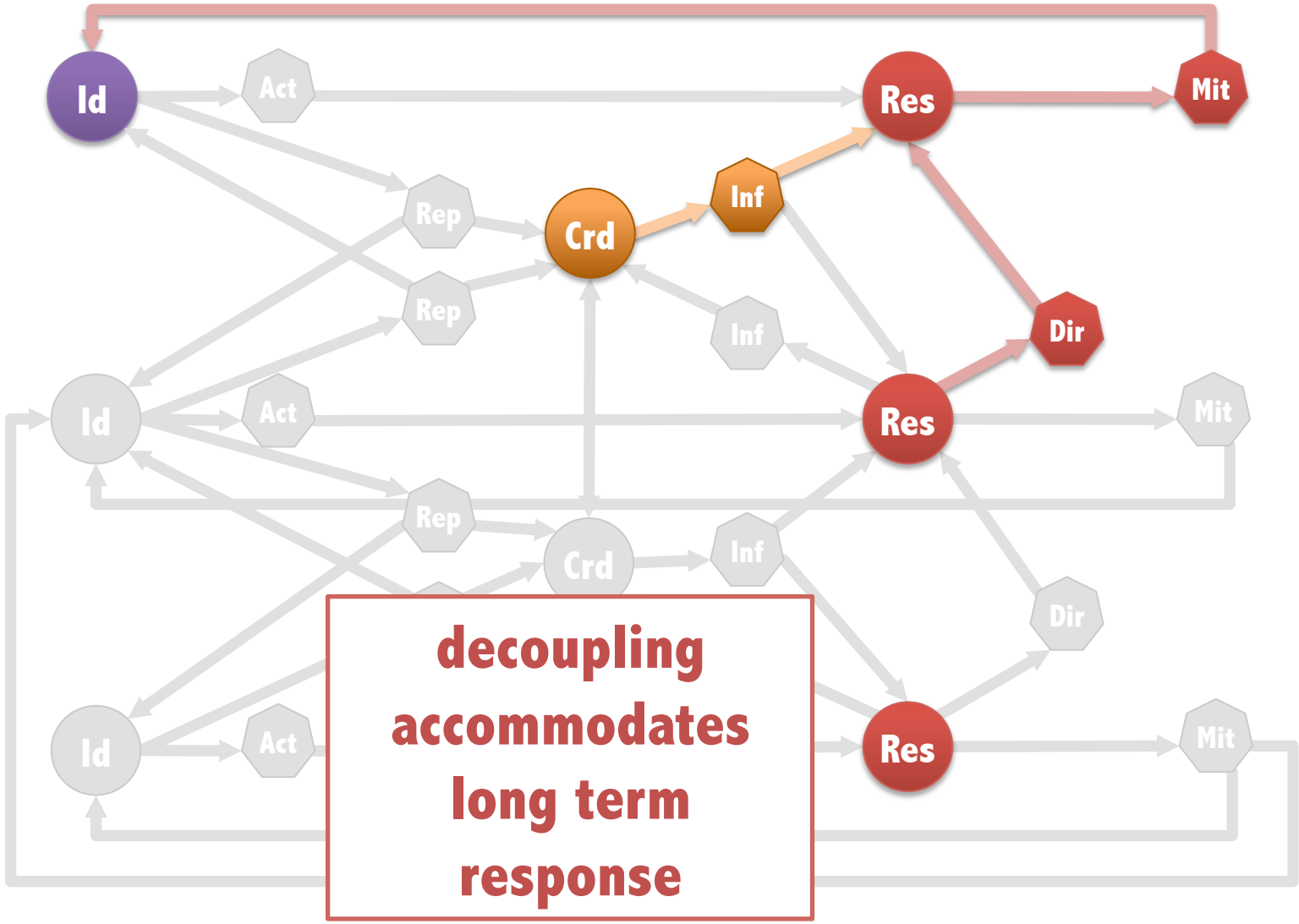
Allows for integration of policy



Uses CSIRTs to drive dissemination

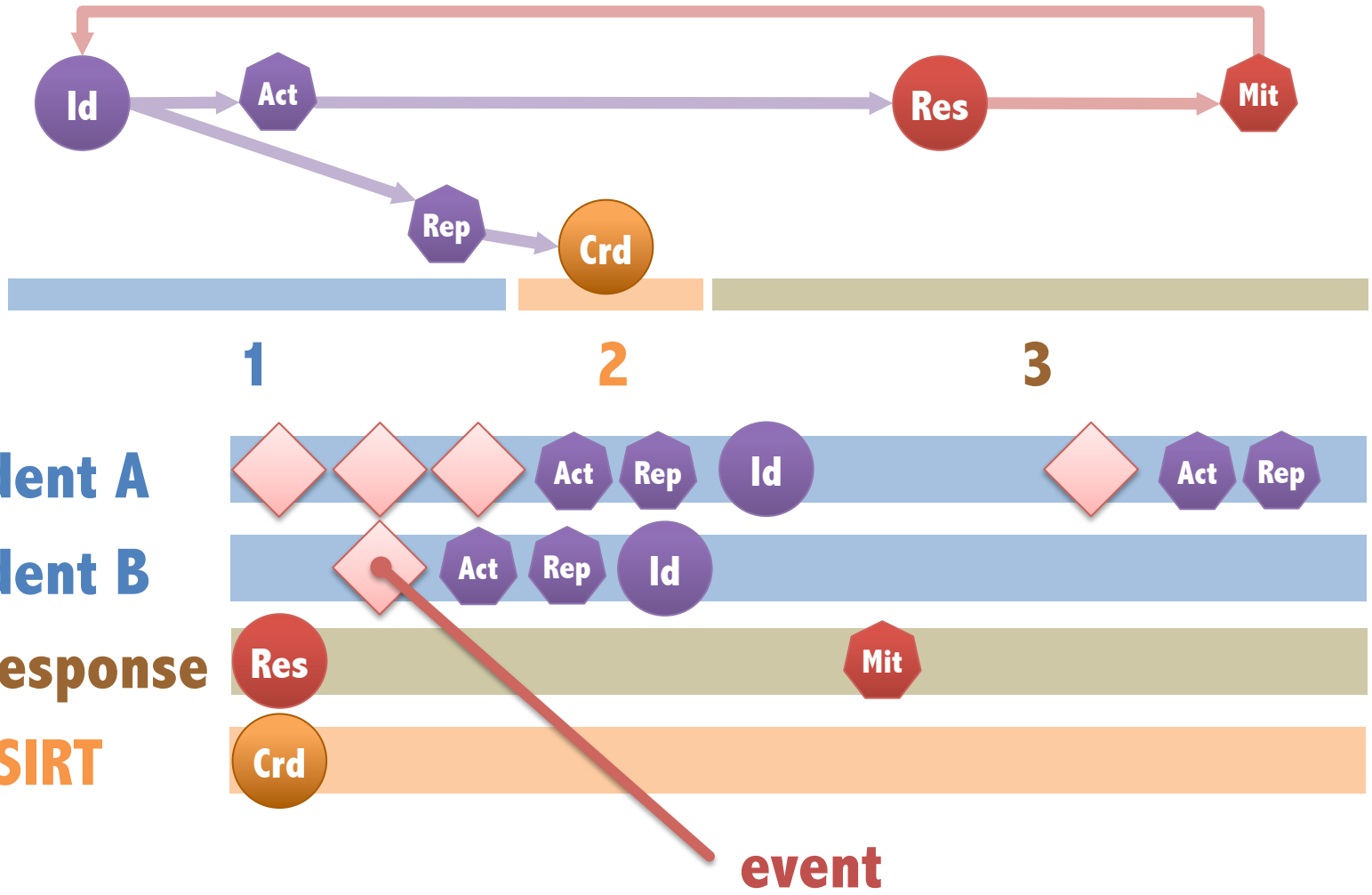


And accounts for long-term impact



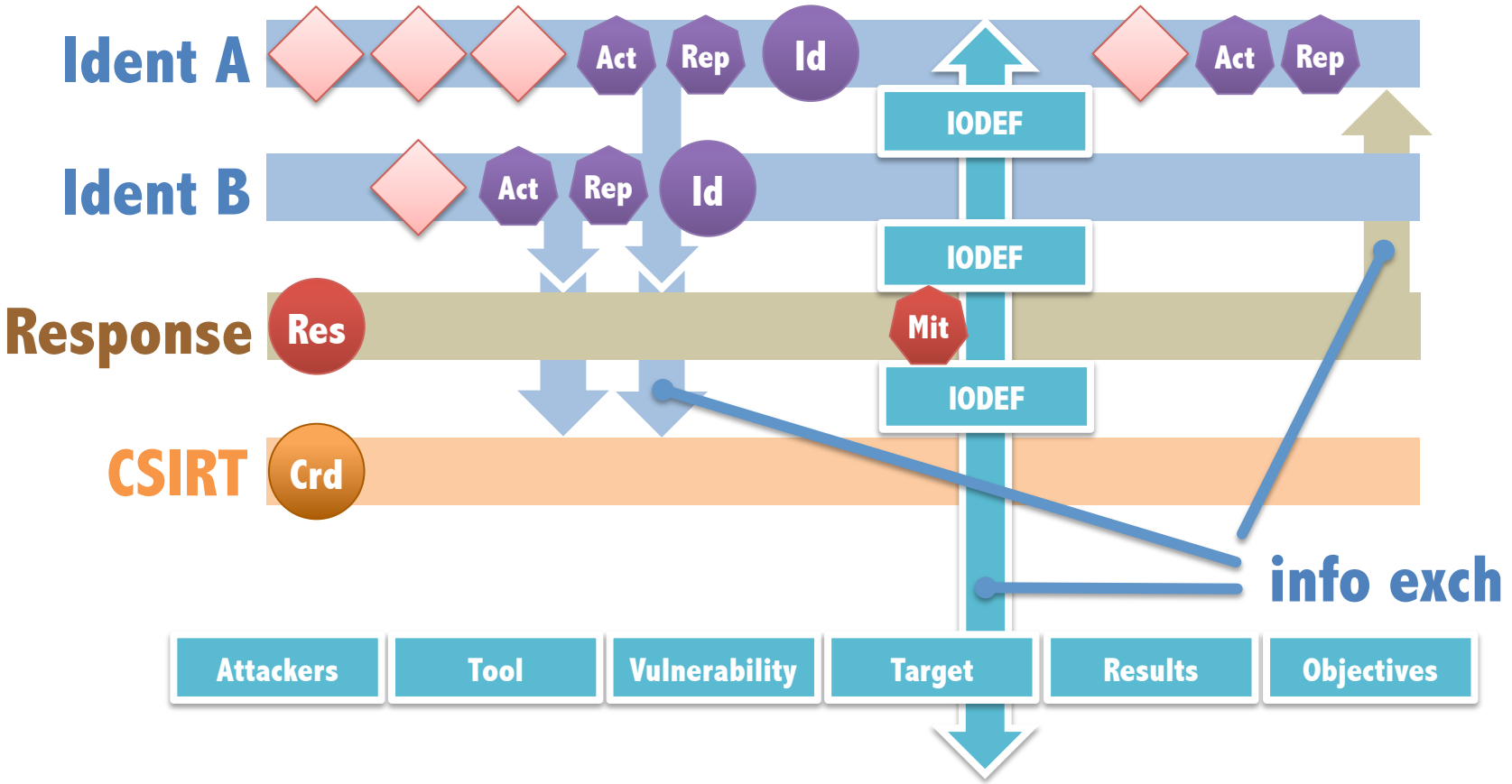
3a. Mapped to common activities

Information and sharing? standard data, common activities

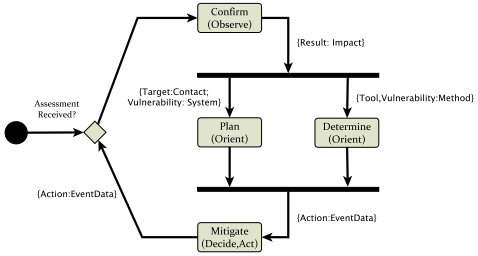


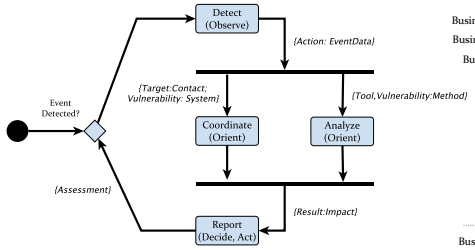
3b. Using standards to communicate

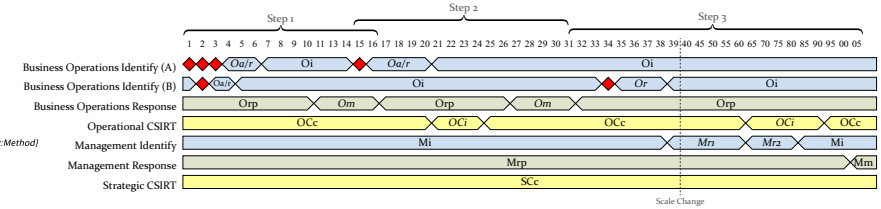
Information and sharing? standard data, common activities

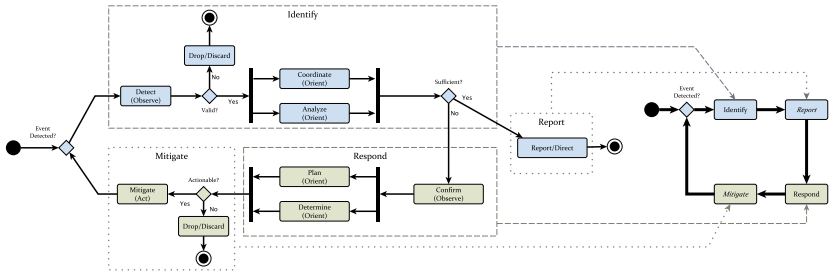


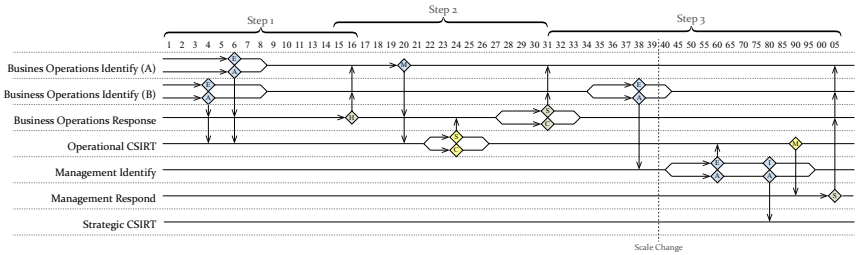
More Detail in Paper

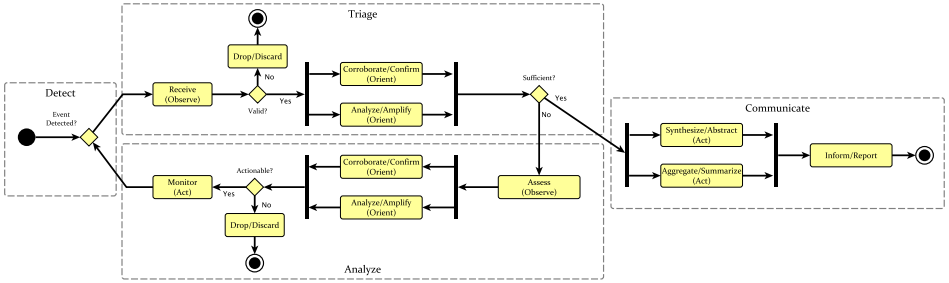


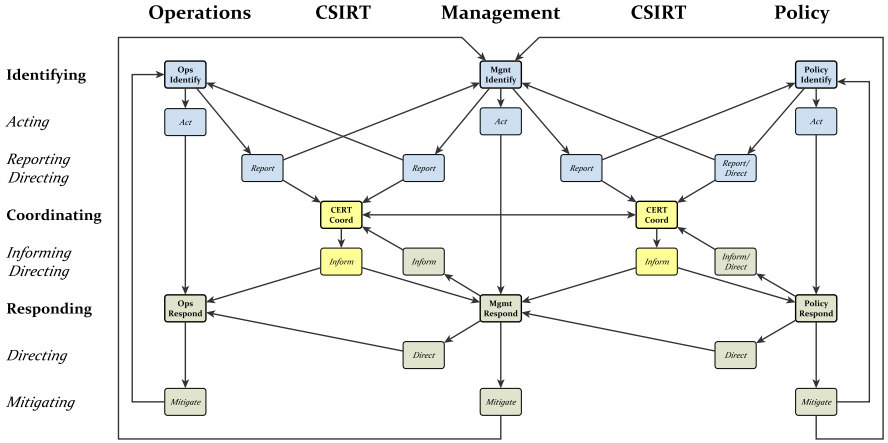








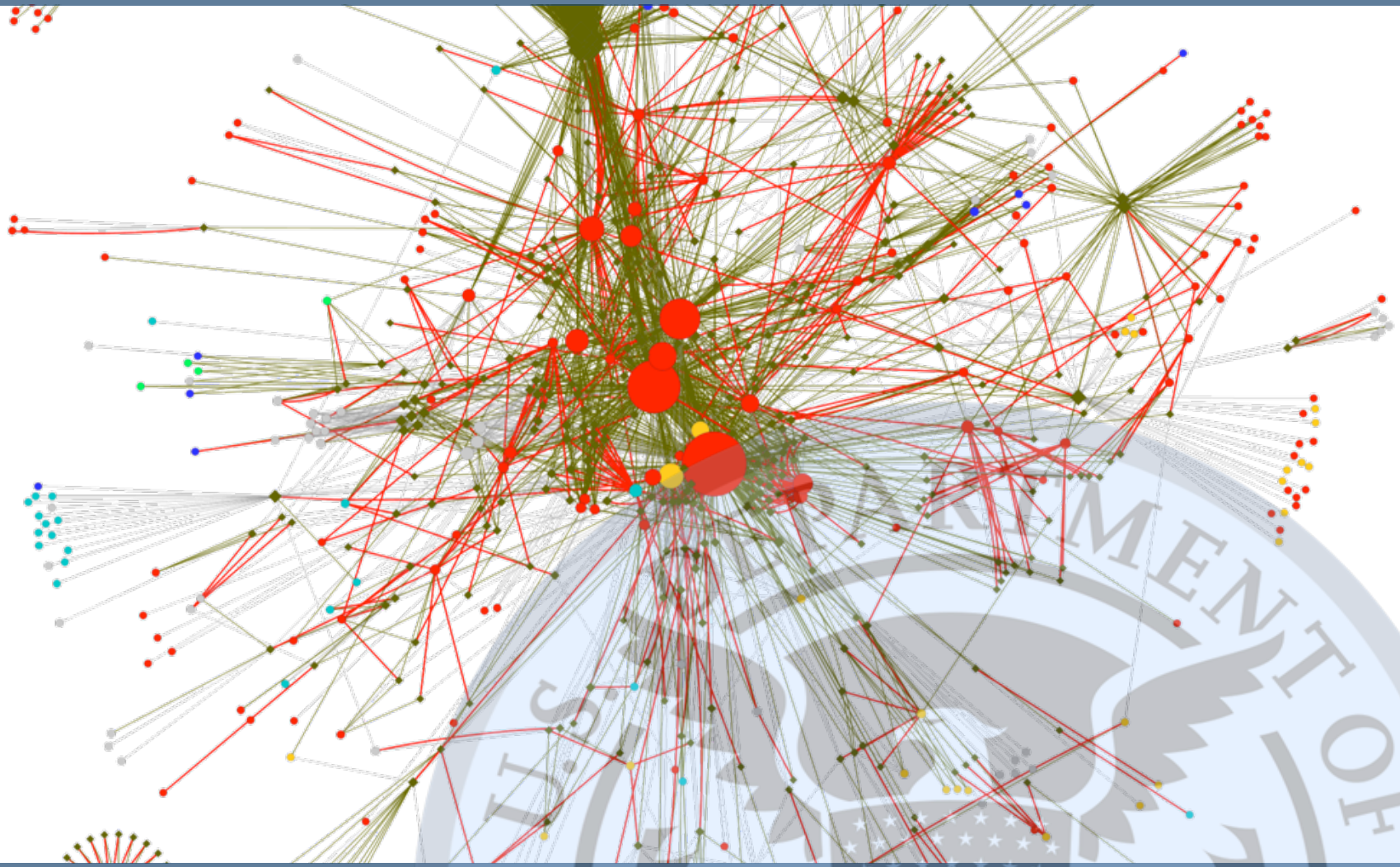




What Difference Will It Make?

- **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

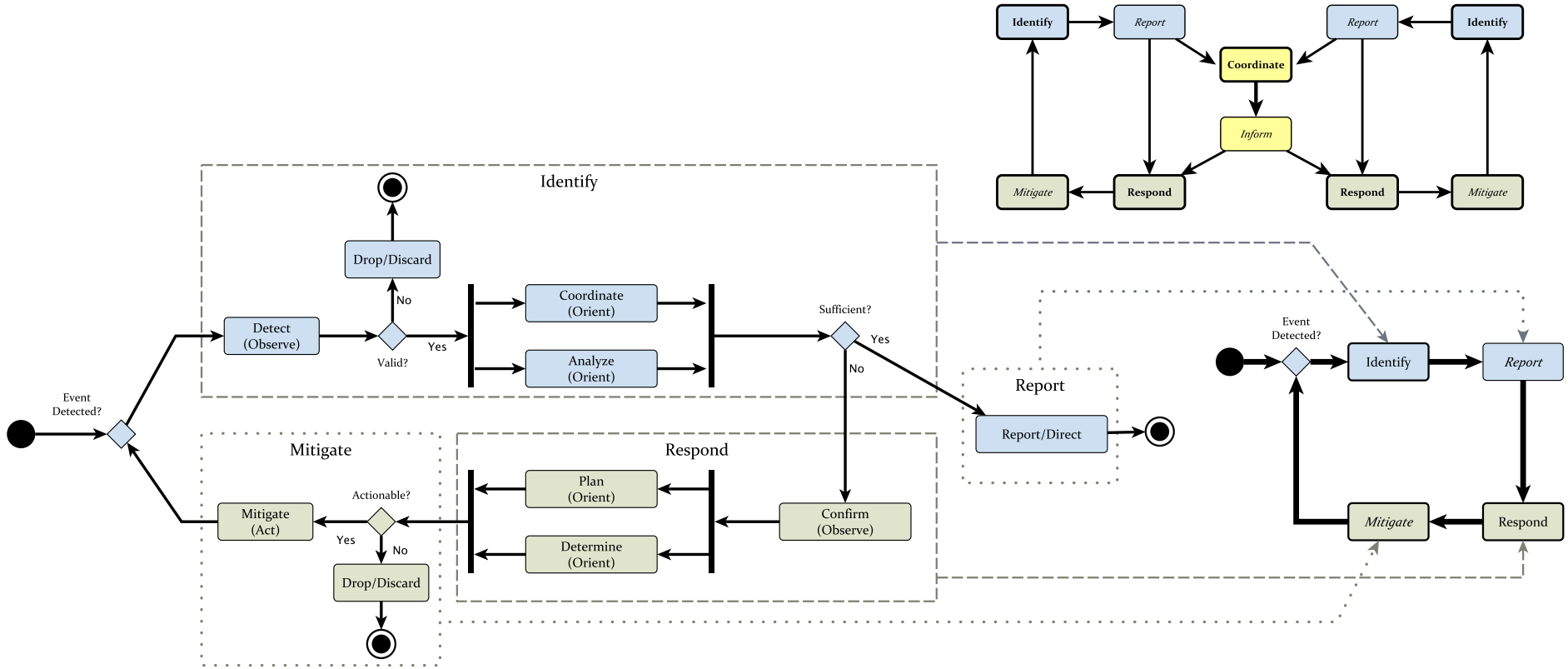
US-CERT
UNITED STATES COMPUTER EMERGENCY READINESS TEAM

APL

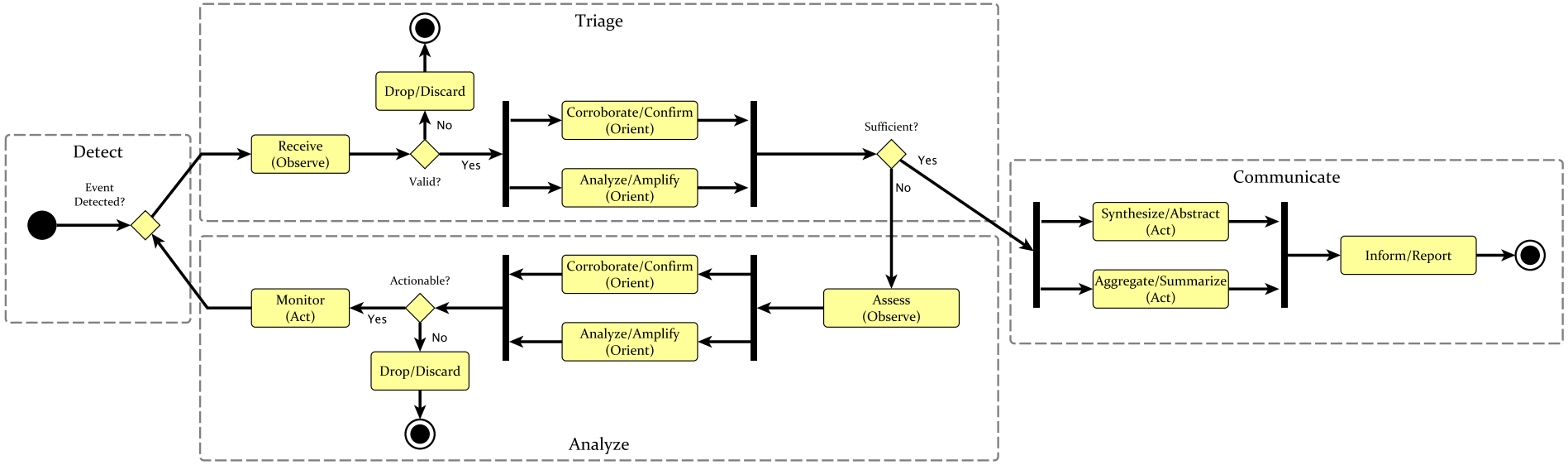
Issues with current approaches

- **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

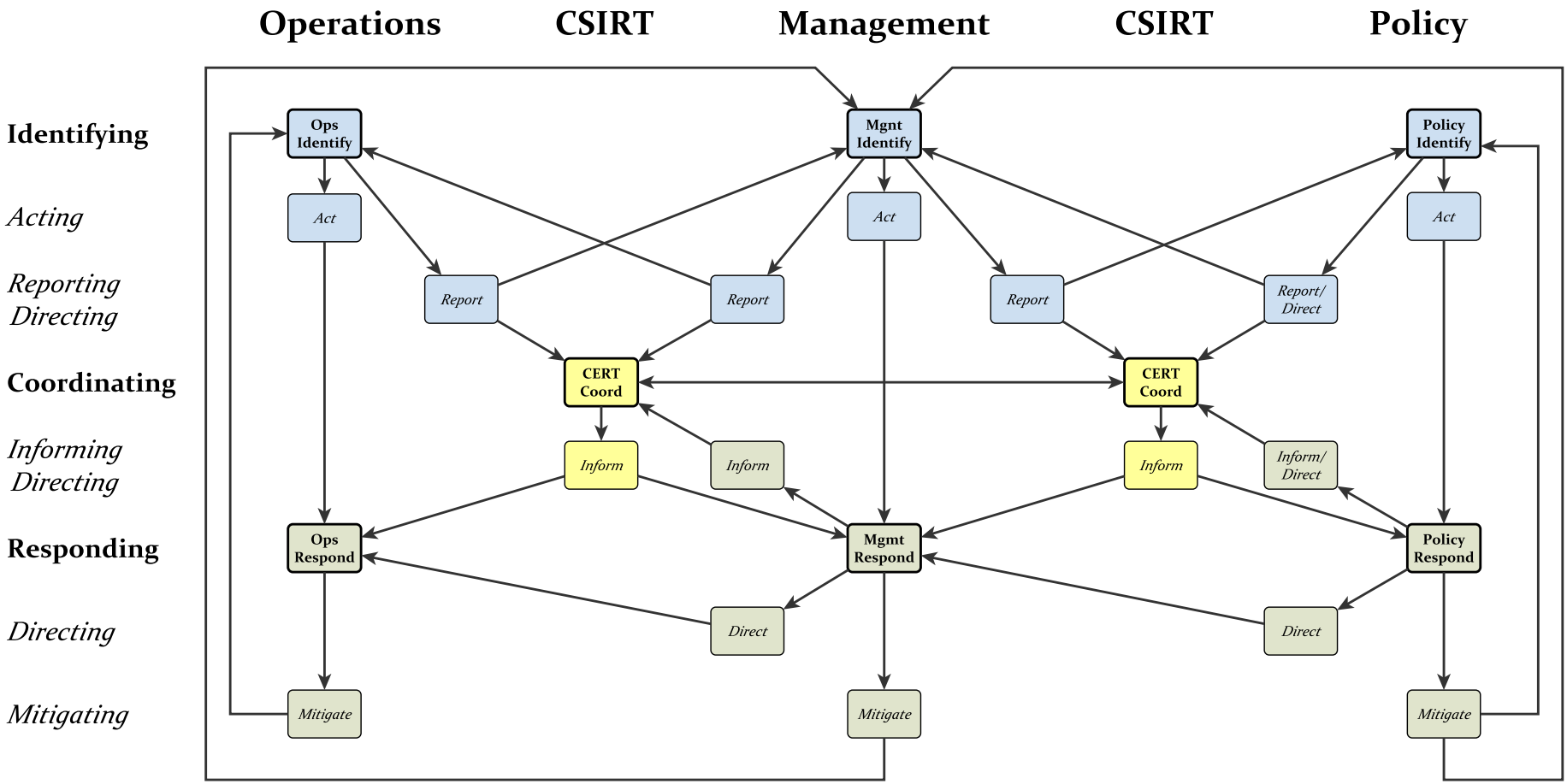
Defend Cycle



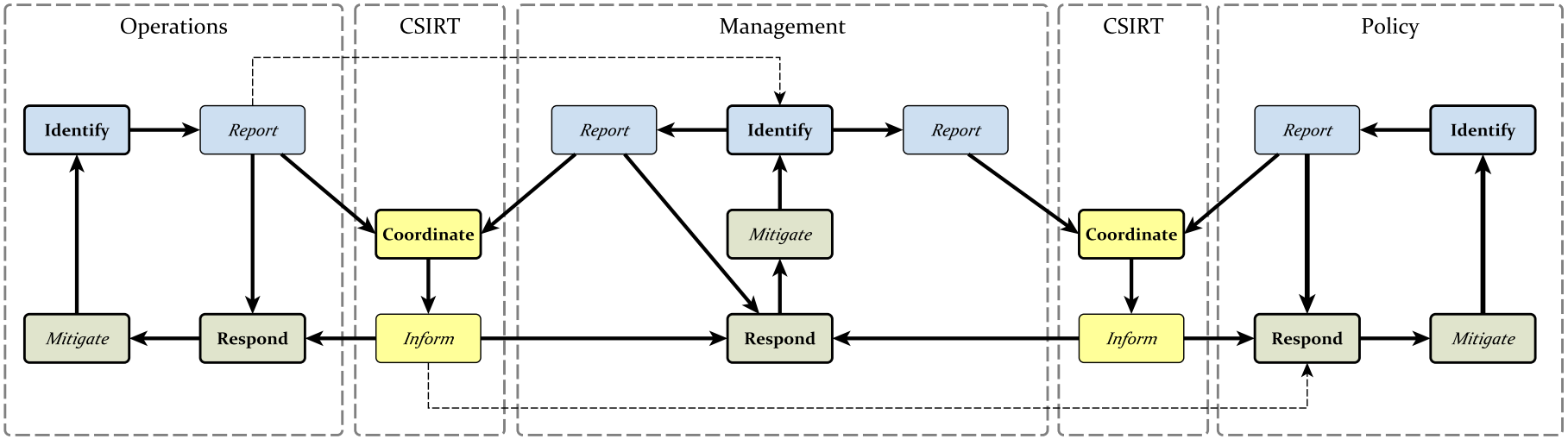
Coordinate Cycle



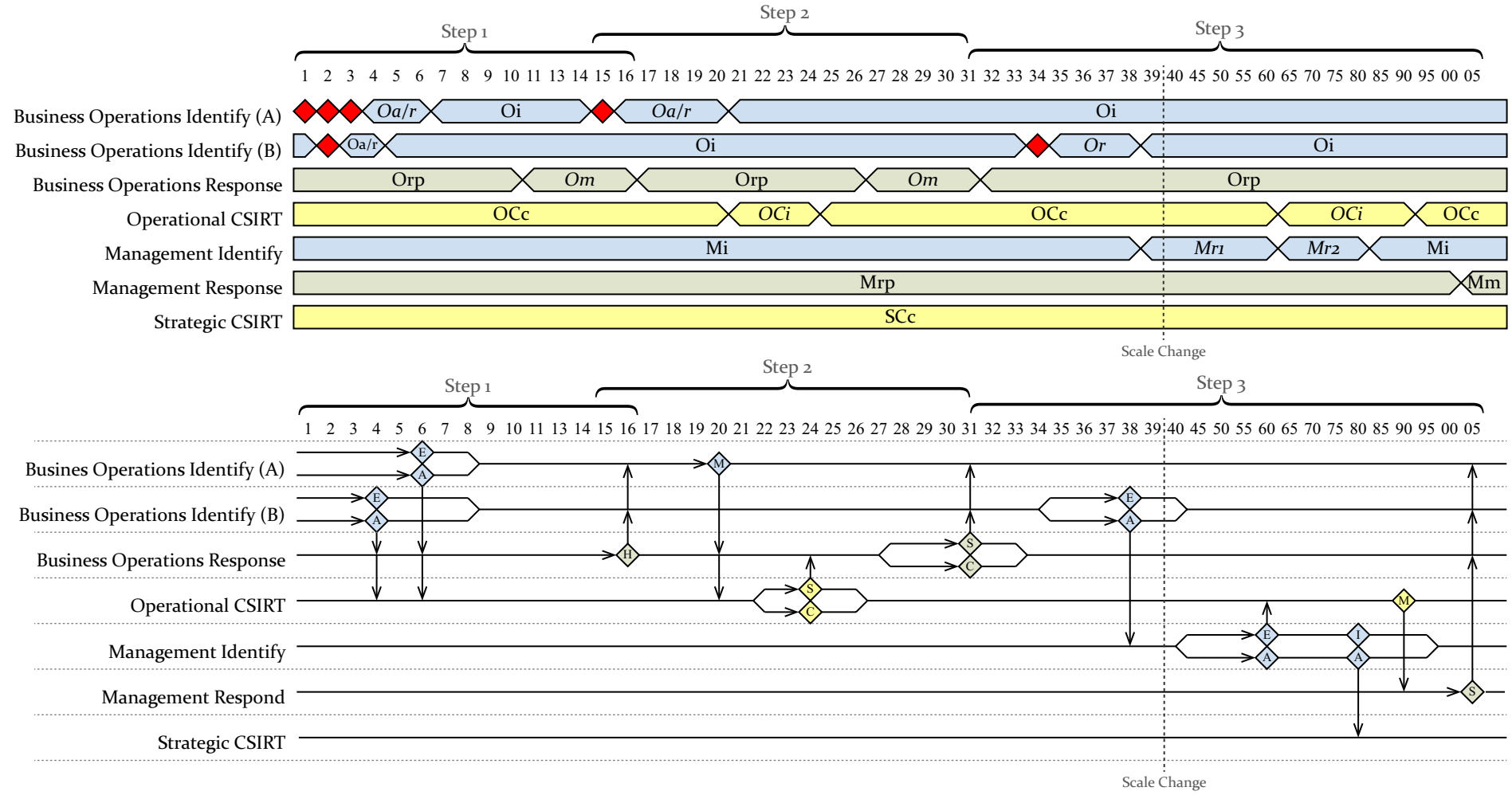
Complete coordination model



Simplified coordination model



Timing and Activity Diagrams



Multi-phase scenario