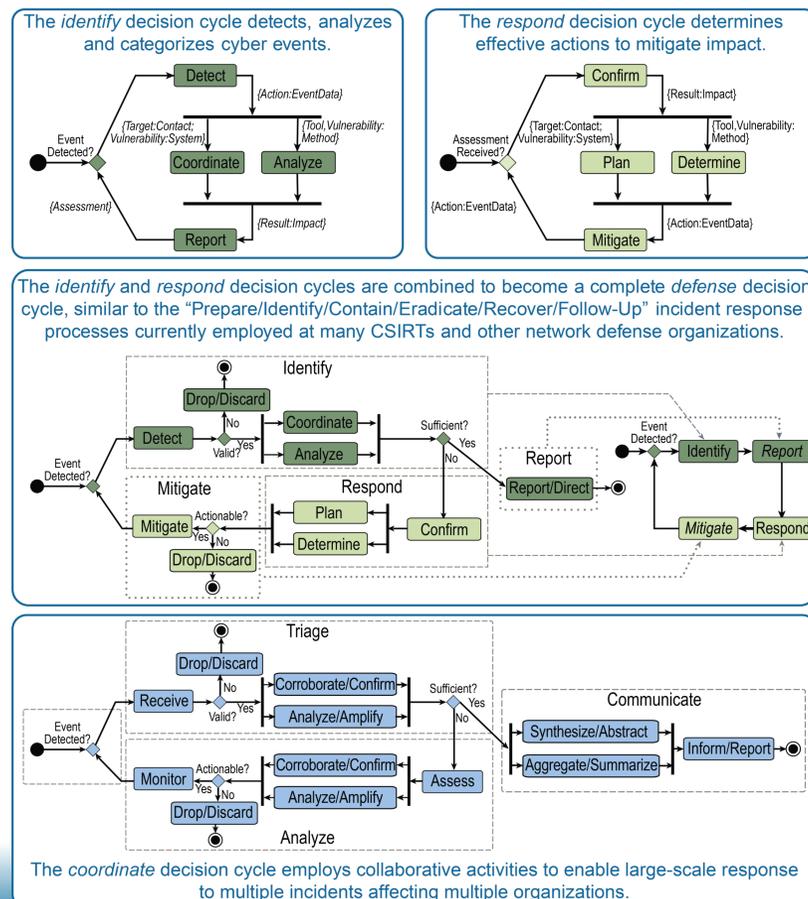
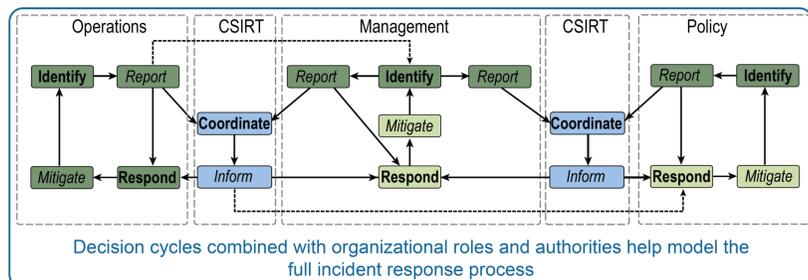


## CSIRT Coordination Model



## Applying process modeling to enable greater collaboration and information exchange in distributed incident response



- Three levels of decision-making:**
- Operations:** immediate activities required to identify incidents and safeguard assets
  - Management:** informed decisions to prioritize activity and allocate additional resources to incident response
  - Policy:** deliberate planning for the establishment of new initiatives, provenance of programs and evolution of organizational practice
- Two modes of communication:**
- Peer-to-peer/Lateral:** operator-to-operator, analyst-to analyst, manager-to-manager and policymaker-to-policymaker collaboration and relay
  - Hierarchical/Vertical:** escalation of incident information and dissemination of directives or plans and the flow of questions and answers between different levels of authority

M. Osorno, T. Millar, D. Rager, "Coordinated Cybersecurity Incident Handling", 16th International Command and Control Research and Technology Symposium (ICCRTS'2011), June 2011, in press.

