

# Enabling Distributed Incident Management: Identifying, Responding, Reporting and Coordinating at Scale and Speed



Paul Cichonski

National Institute of Standards and  
Technology (NIST)

---





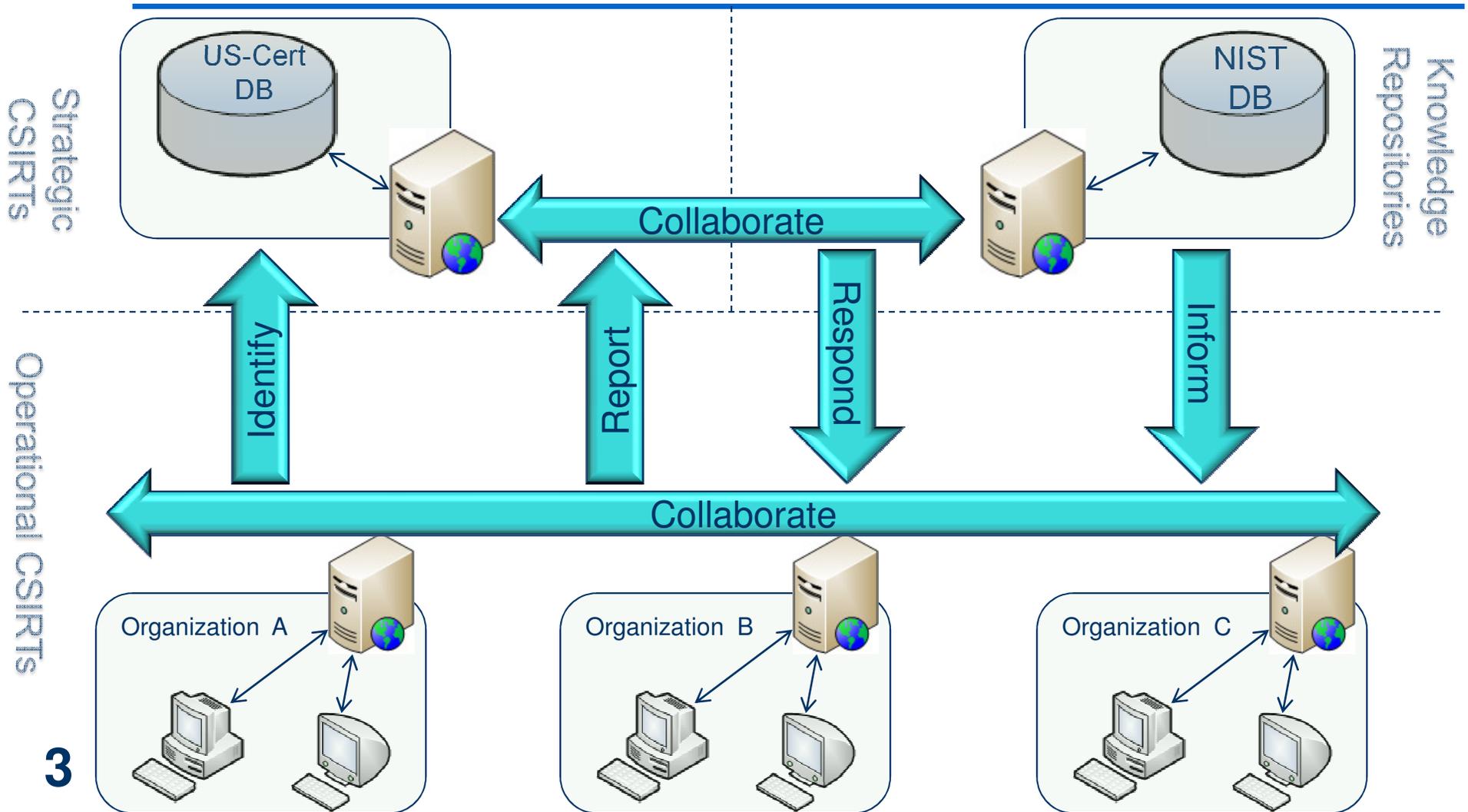
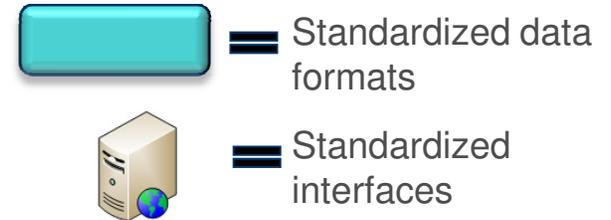
# Goals / Design Considerations for Incident Handling Collaboration

---

- Adaptive Data Models
  - Incidents change rapidly, so should the data models.
  - Encode stabilized semantics, but leave room for extension.
- Customized Reporting Techniques
  - Allow CSIRTs to customize how they report depending on incident type.
  - Only need the data to make sense of the incident, no more.
- Re-use and Composability
  - No need to re-invent data models, use what exists.
  - Combine multiple data models to paint the larger picture.

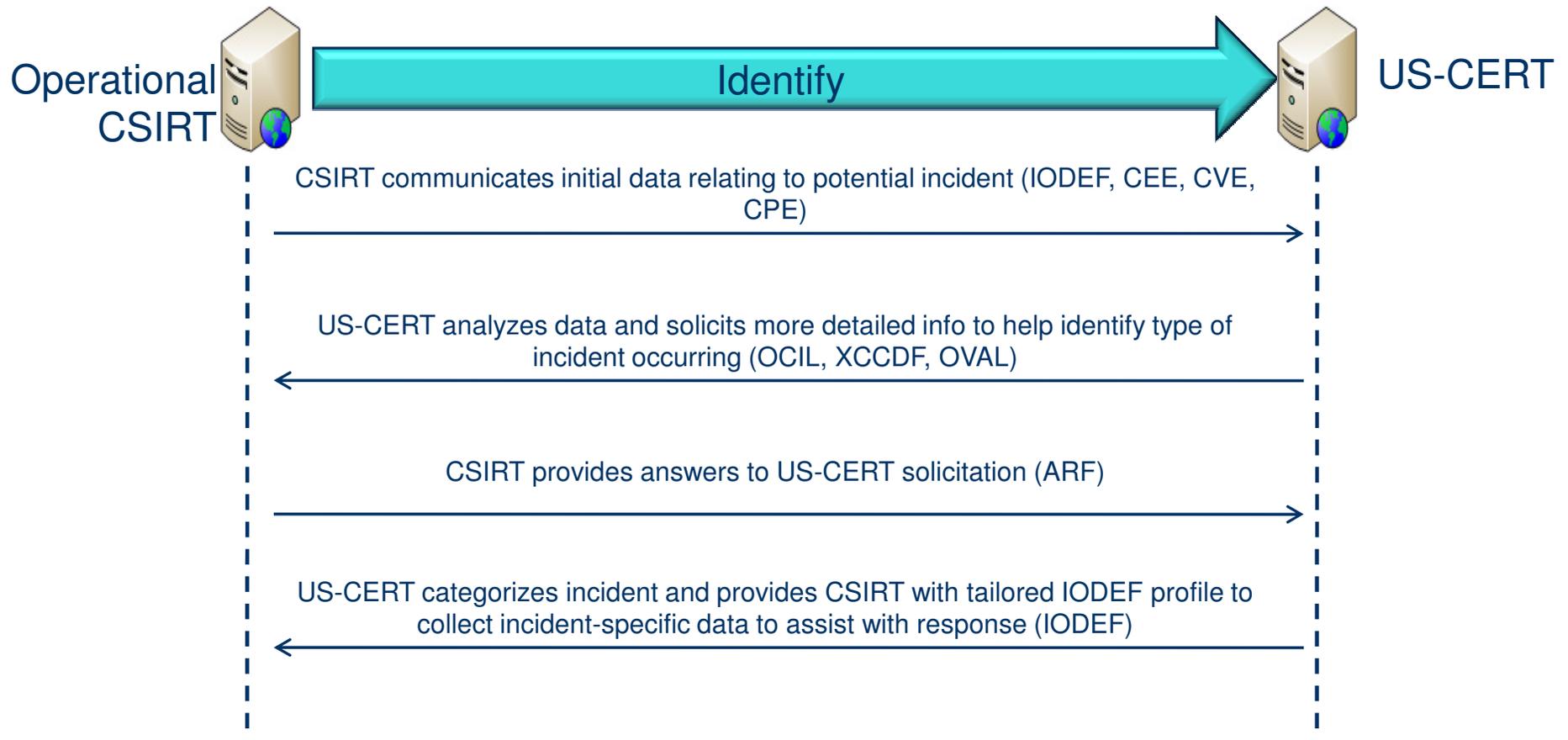


# Potential Collaboration Architecture



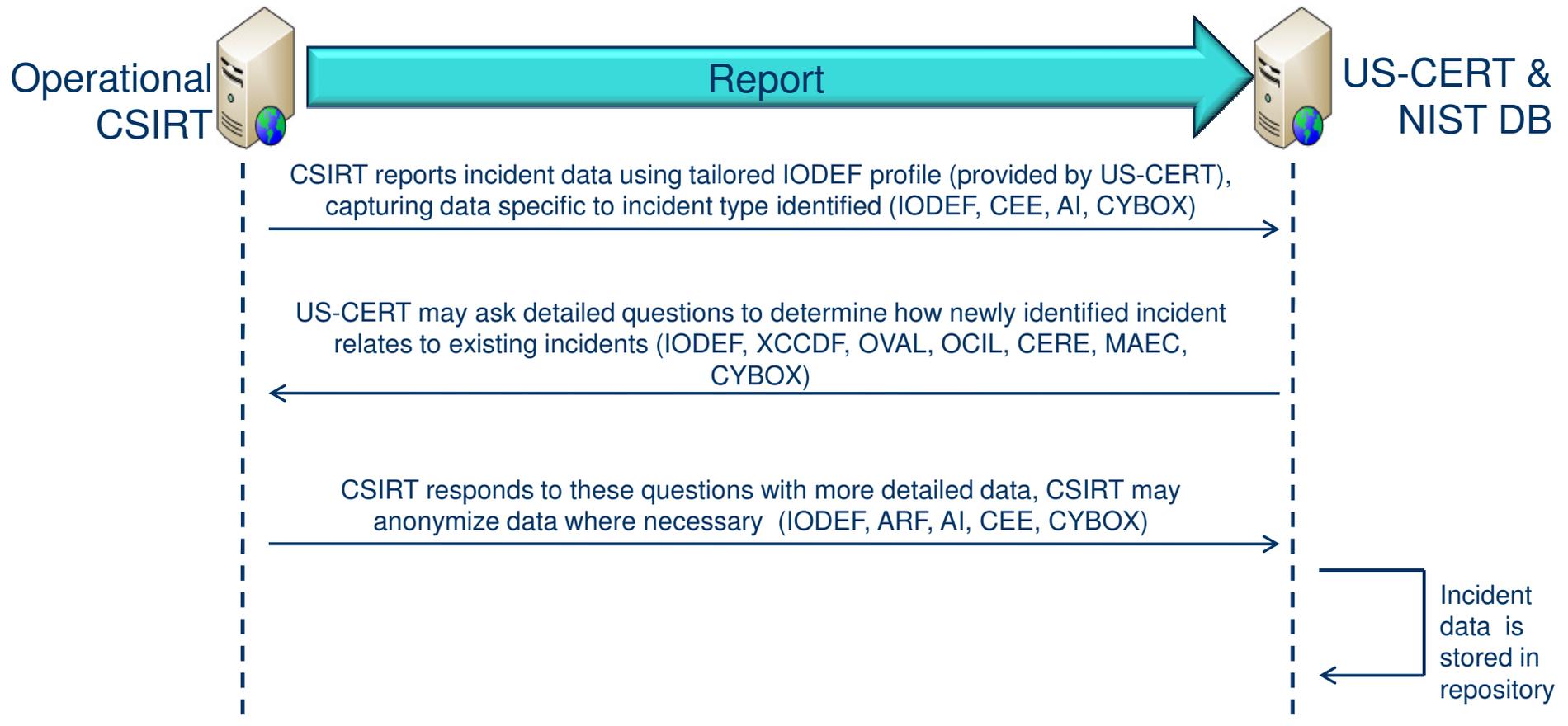


# Using standardized data formats to automate incident identification



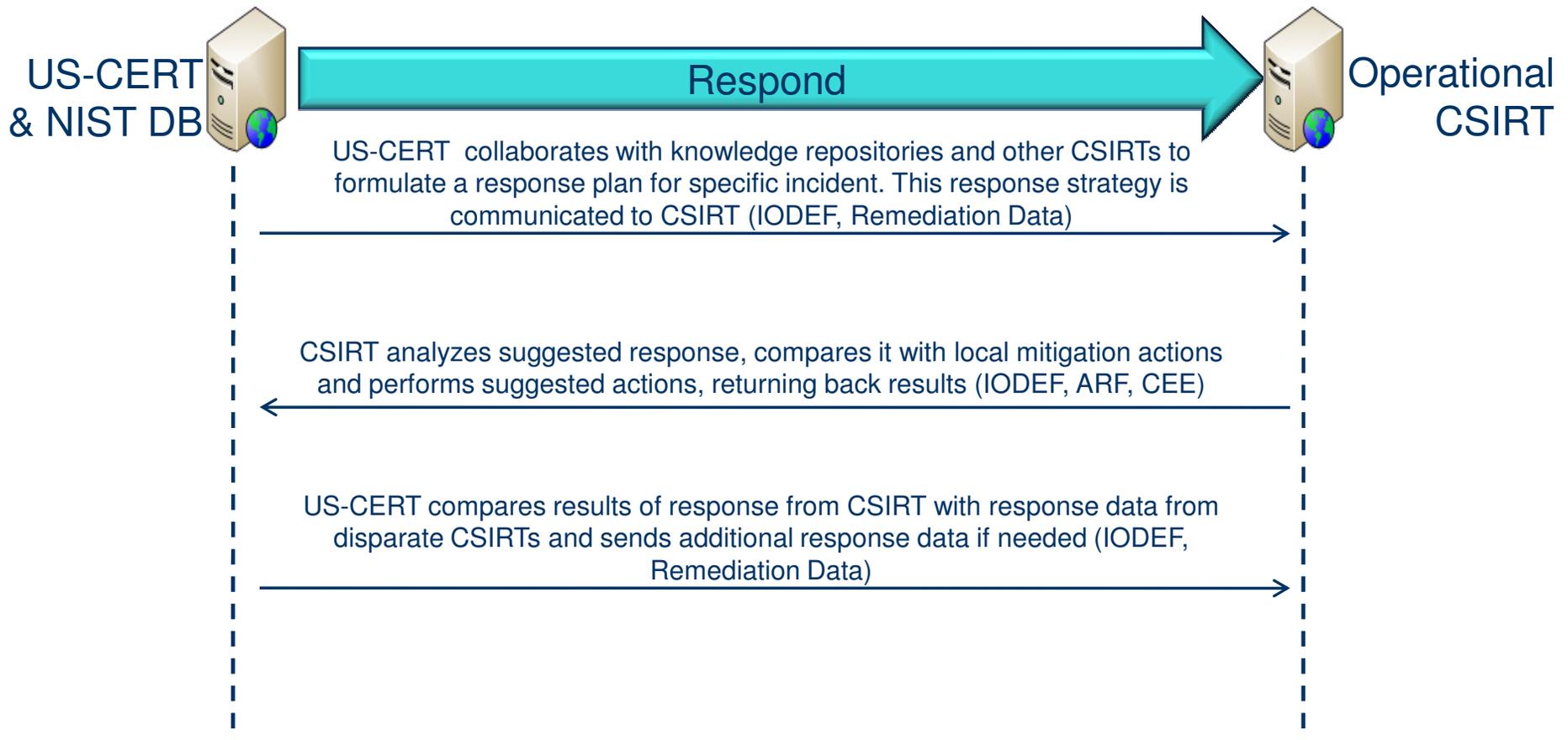


# Using standardized data formats to automate incident reporting



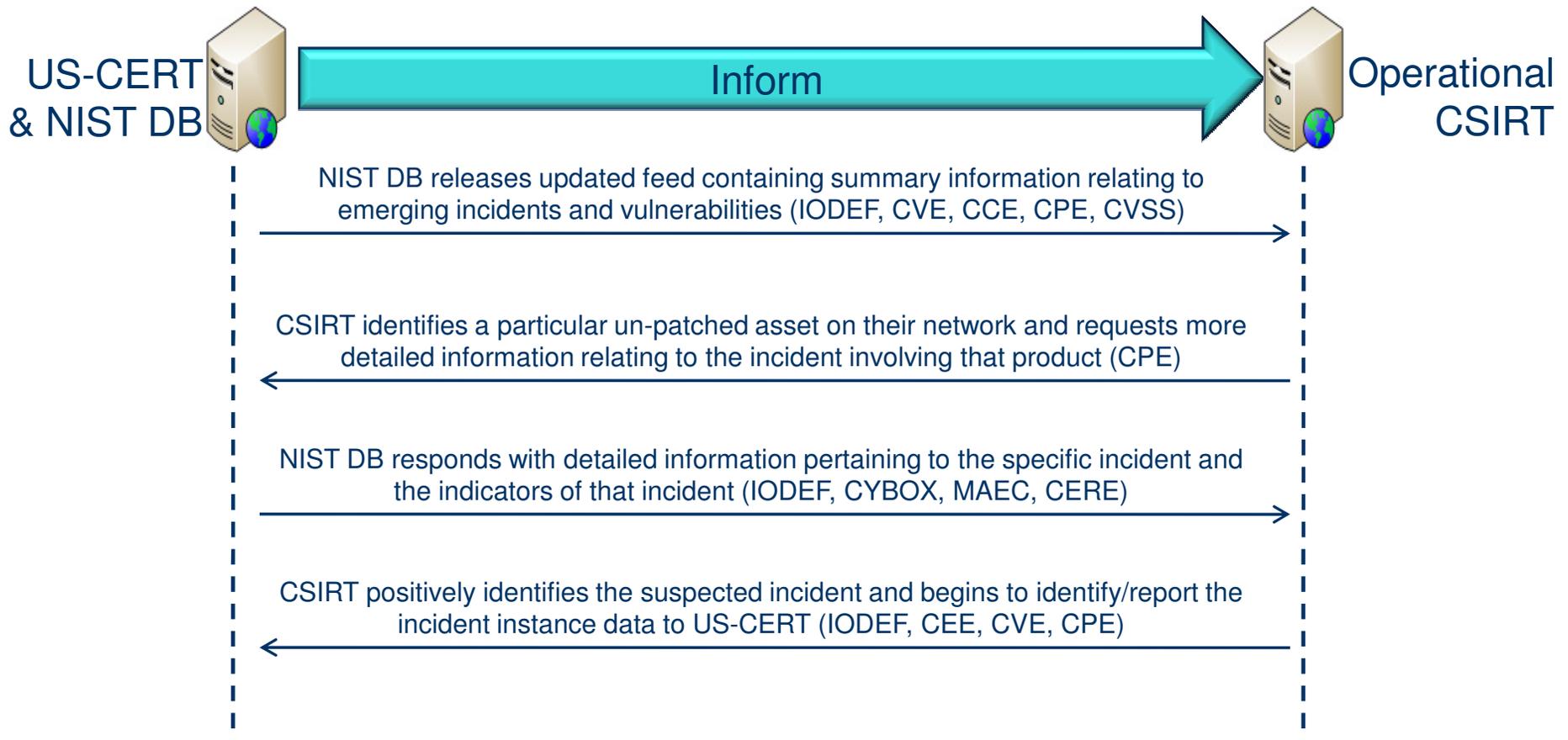


# Using standardized data formats to automate incident response



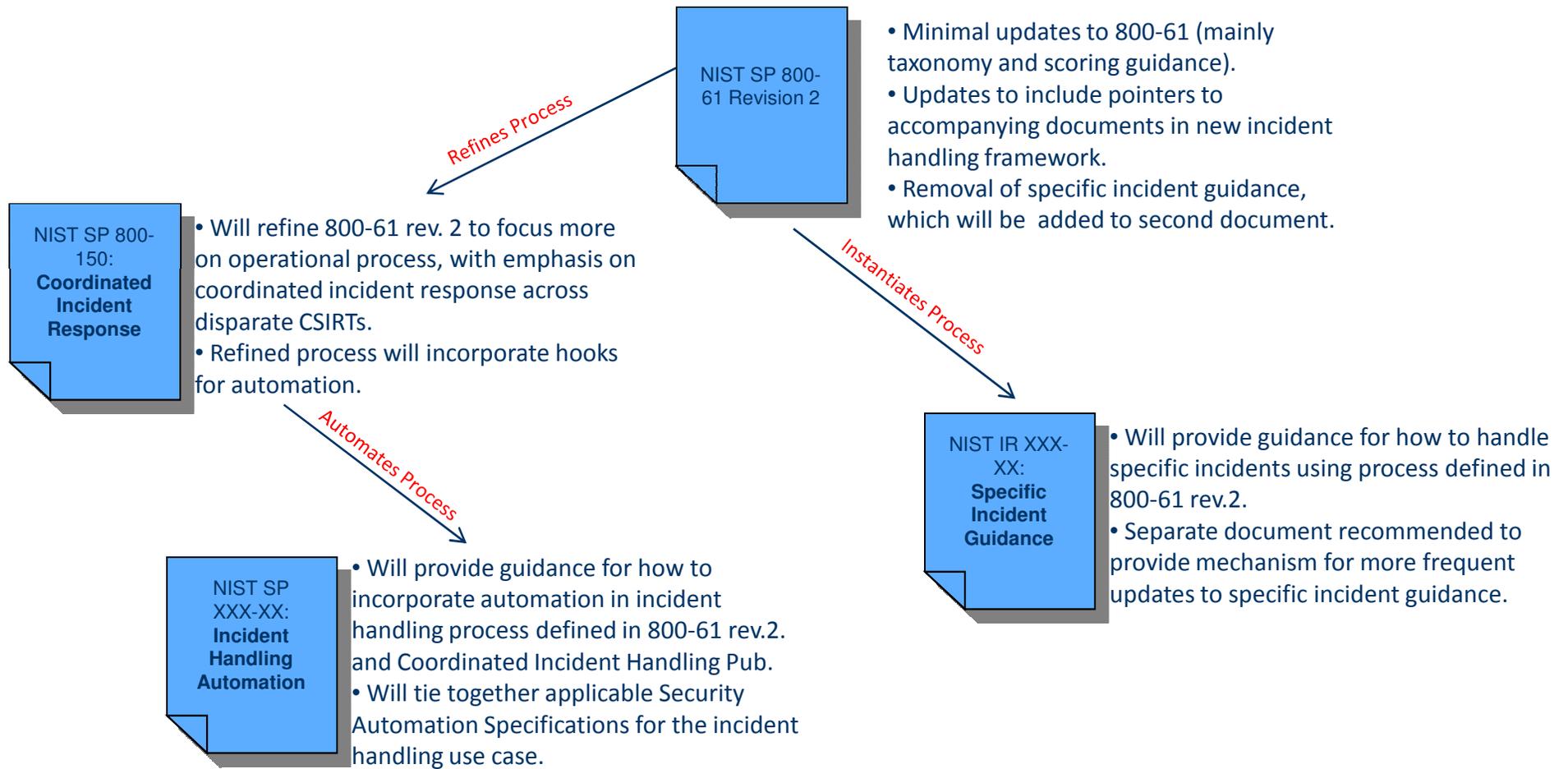


# Using standardized data formats to automate information dissemination





# Proposed Evolution of NIST SP 800-61 rev.1





# Community Involvement

---

- Community feedback will drive the future direction of this work.
- The primary mechanism for community involvement will be the Incident Data Exchange Working Group mailing list ([idxwg@nicwg.org](mailto:idxwg@nicwg.org)).
  - Engineering discussions relating to the technical aspects of this work.
  - Announcements relating to release of publications, data models, and reference implementations.
  - Contact Tom Millar ([Thomas.Millar@us-cert.gov](mailto:Thomas.Millar@us-cert.gov)) to be added to list.



## Questions & Answers / Discussion

---



Paul Cichonski

National Institute of Standards and  
Technology (NIST)

[paul.cichonski@nist.gov](mailto:paul.cichonski@nist.gov)

(301) 975-5259



# EXTRA