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

Paul Cichonski

National Institute of Standards and Technology (NIST)

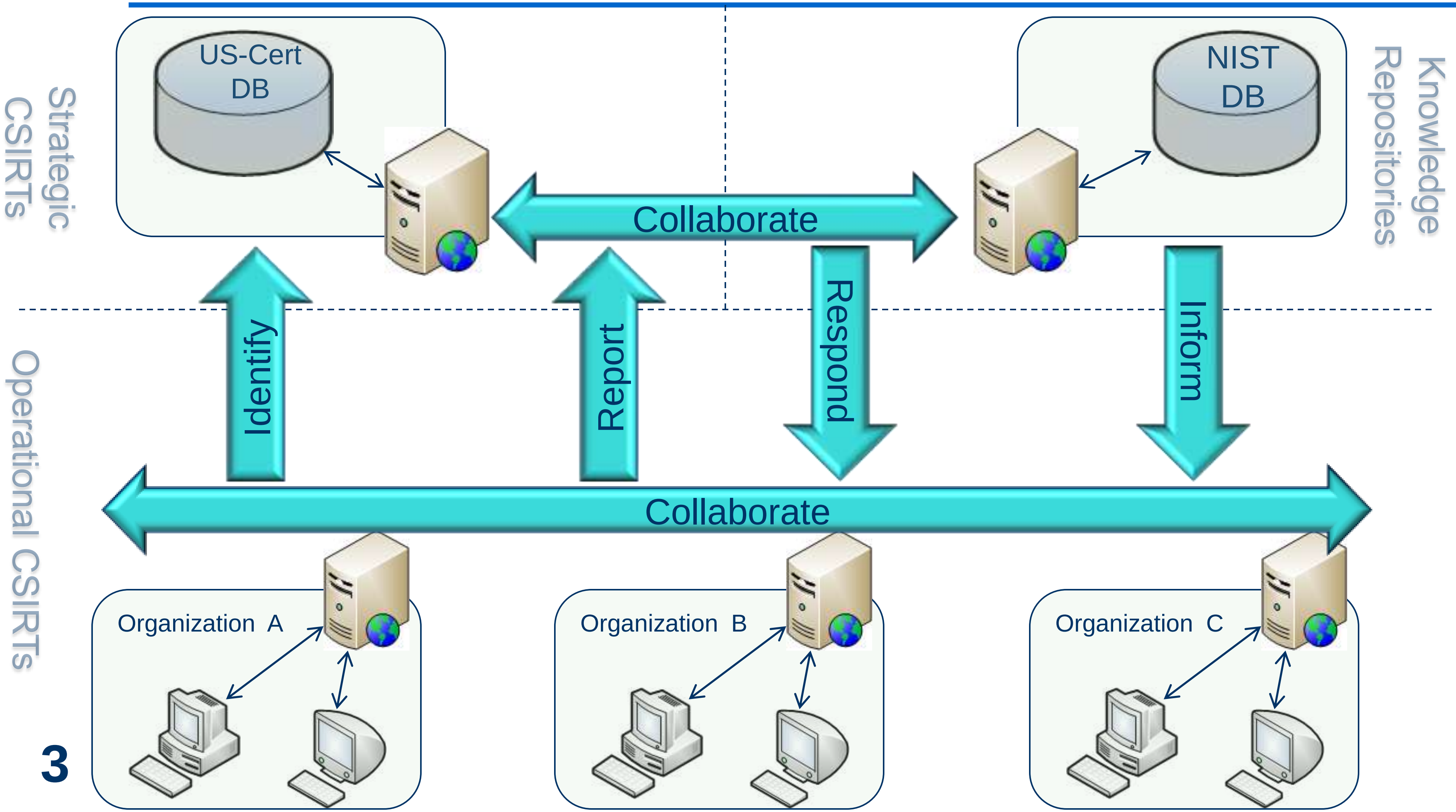
Goals / Design Considerations for Incident Handling Collaboration

- 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

🟦 = Standardized data formats

🖥 = Standardized interfaces



Strategic CSIRTs

US-Cert DB

Collaborate

NIST DB

Knowledge Repositories

Identify

Report

Respond

Inform

Operational CSIRTs

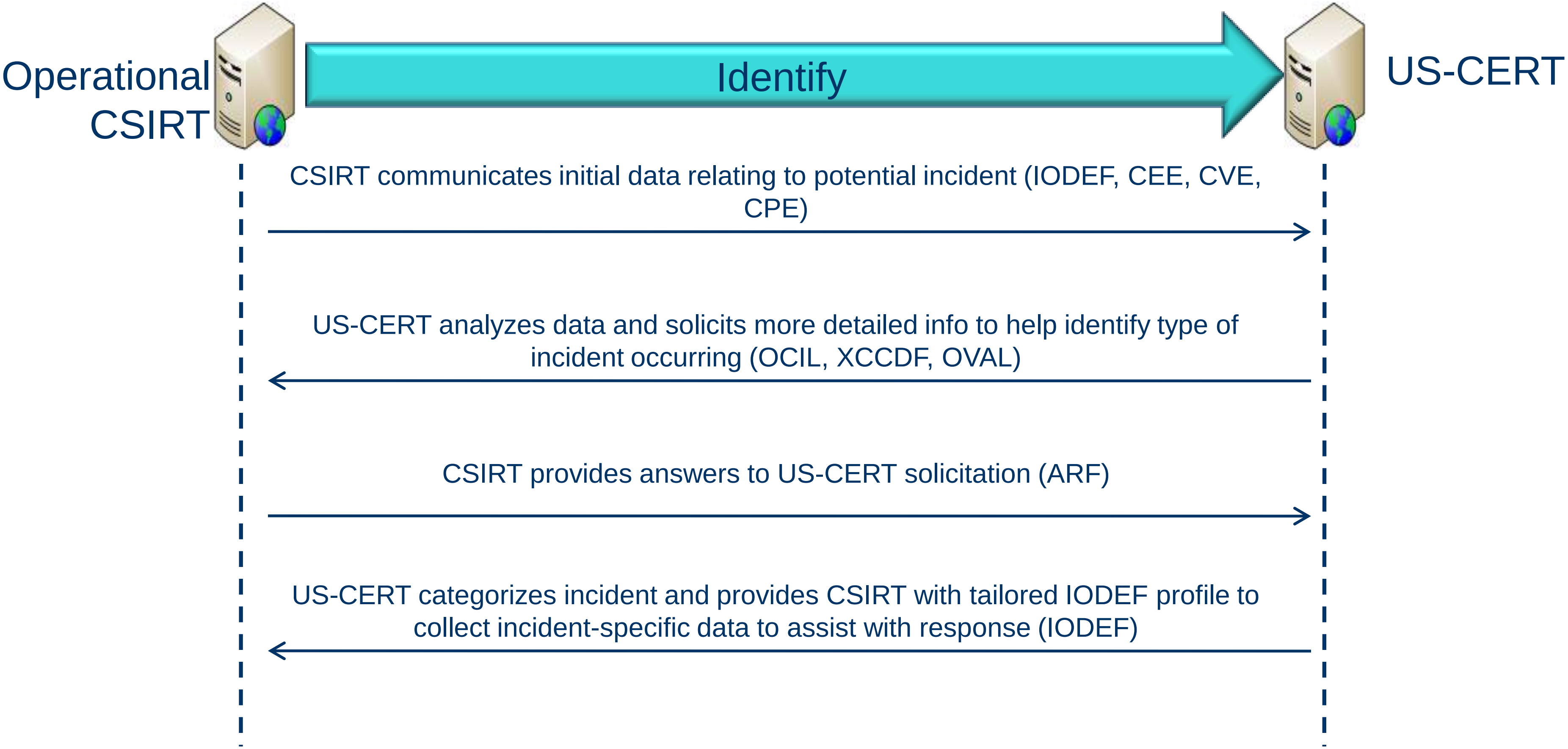
Collaborate

Organization A

Organization B

Organization C

Using standardized data formats to automate incident identification



Operational CSIRT

Identify

US-CERT

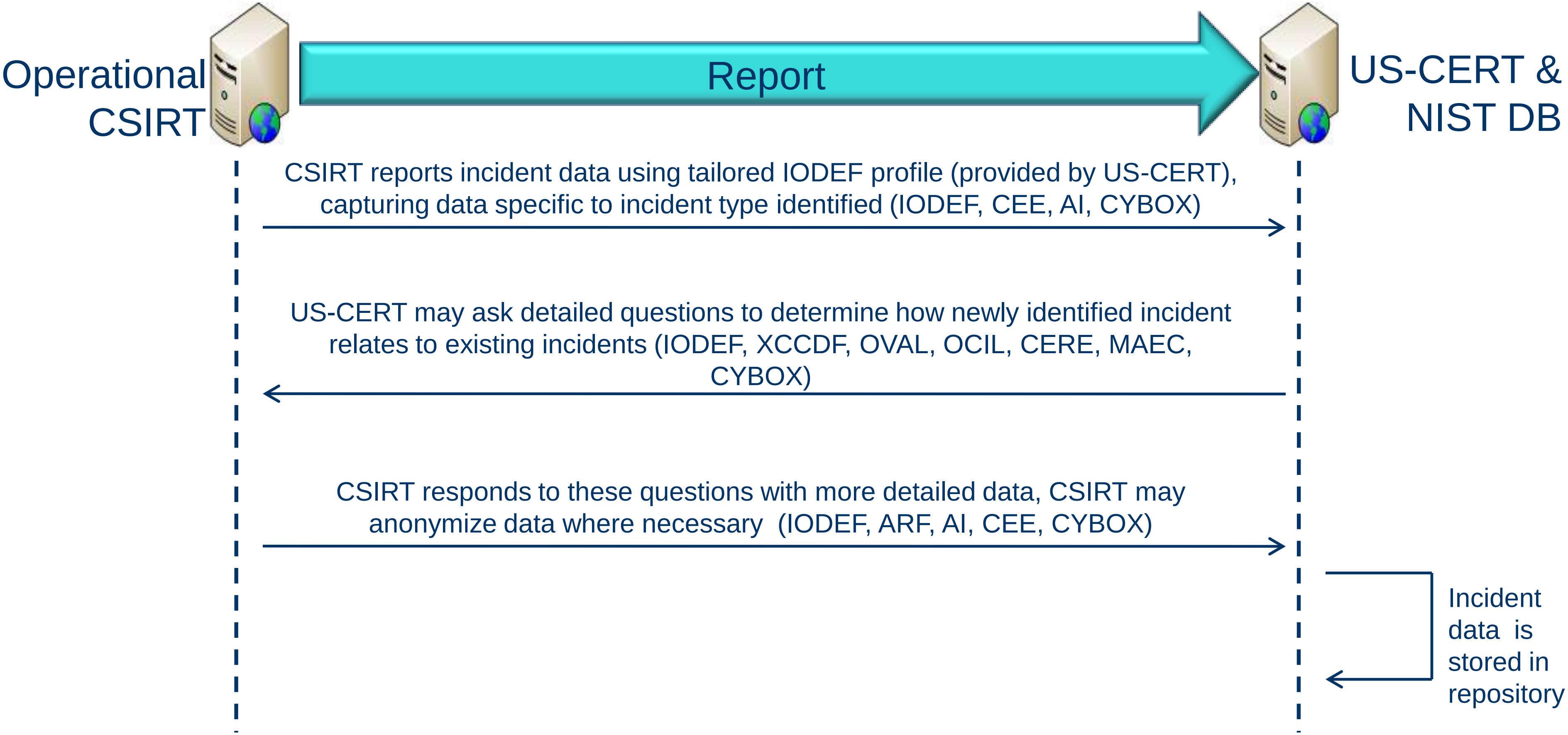
CSIRT communicates initial data relating to potential incident (IODEF, CEE, CVE, CPE)

US-CERT analyzes data and solicits more detailed info to help identify type of incident occurring (OCIL, XCCDF, OVAL)

CSIRT provides answers to US-CERT solicitation (ARF)

US-CERT categorizes incident and provides CSIRT with tailored IODEF profile to collect incident-specific data to assist with response (IODEF)

Using standardized data formats to automate incident reporting



Operational CSIRT

Report

US-CERT & NIST DB

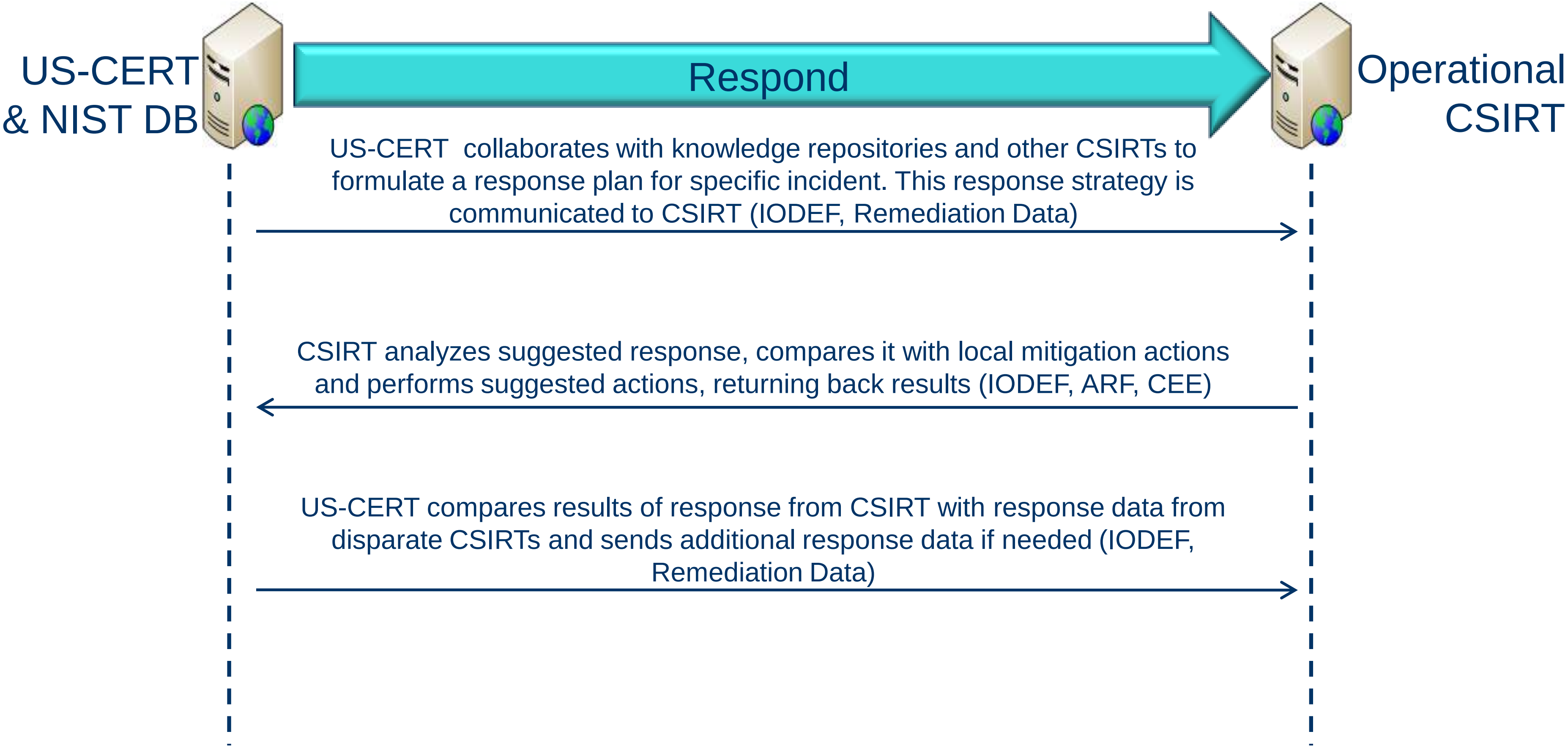
CSIRT reports incident data using tailored IODEF profile (provided by US-CERT), capturing data specific to incident type identified (IODEF, CEE, AI, CYBOX)

US-CERT may ask detailed questions to determine how newly identified incident relates to existing incidents (IODEF, XCCDF, OVAL, OCIL, CERE, MAEC, CYBOX)

CSIRT responds to these questions with more detailed data, CSIRT may anonymize data where necessary (IODEF, ARF, AI, CEE, CYBOX)

Incident data is stored in repository

Using standardized data formats to automate incident response

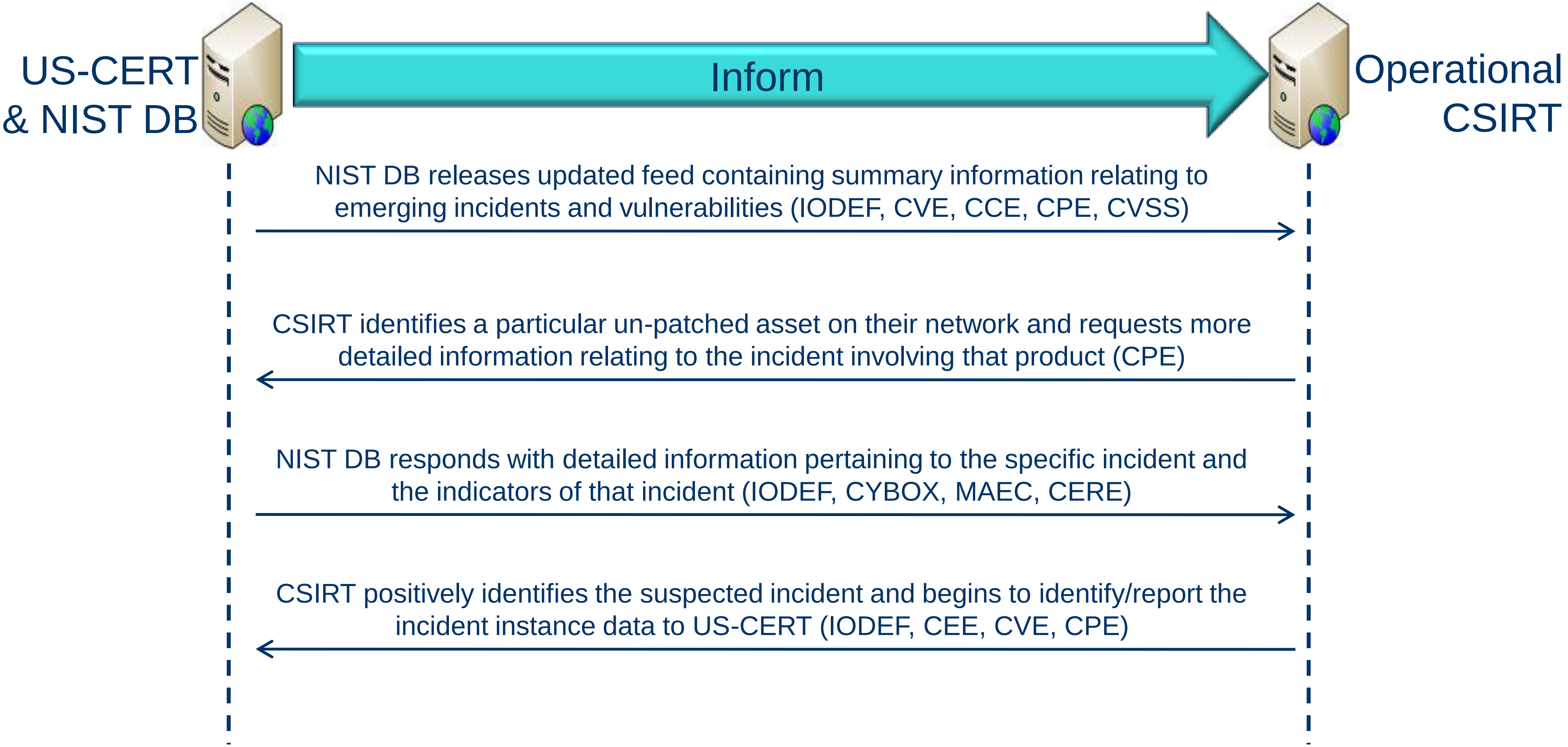


US-CERT collaborates with knowledge repositories and other CSIRTs to formulate a response plan for specific incident. This response strategy is communicated to CSIRT (IODEF, Remediation Data)

CSIRT analyzes suggested response, compares it with local mitigation actions and performs suggested actions, returning back results (IODEF, ARF, CEE)

US-CERT compares results of response from CSIRT with response data from disparate CSIRTs and sends additional response data if needed (IODEF, Remediation Data)

Using standardized data formats to automate information dissemination



US-CERT & NIST DB

Inform

Operational CSIRT

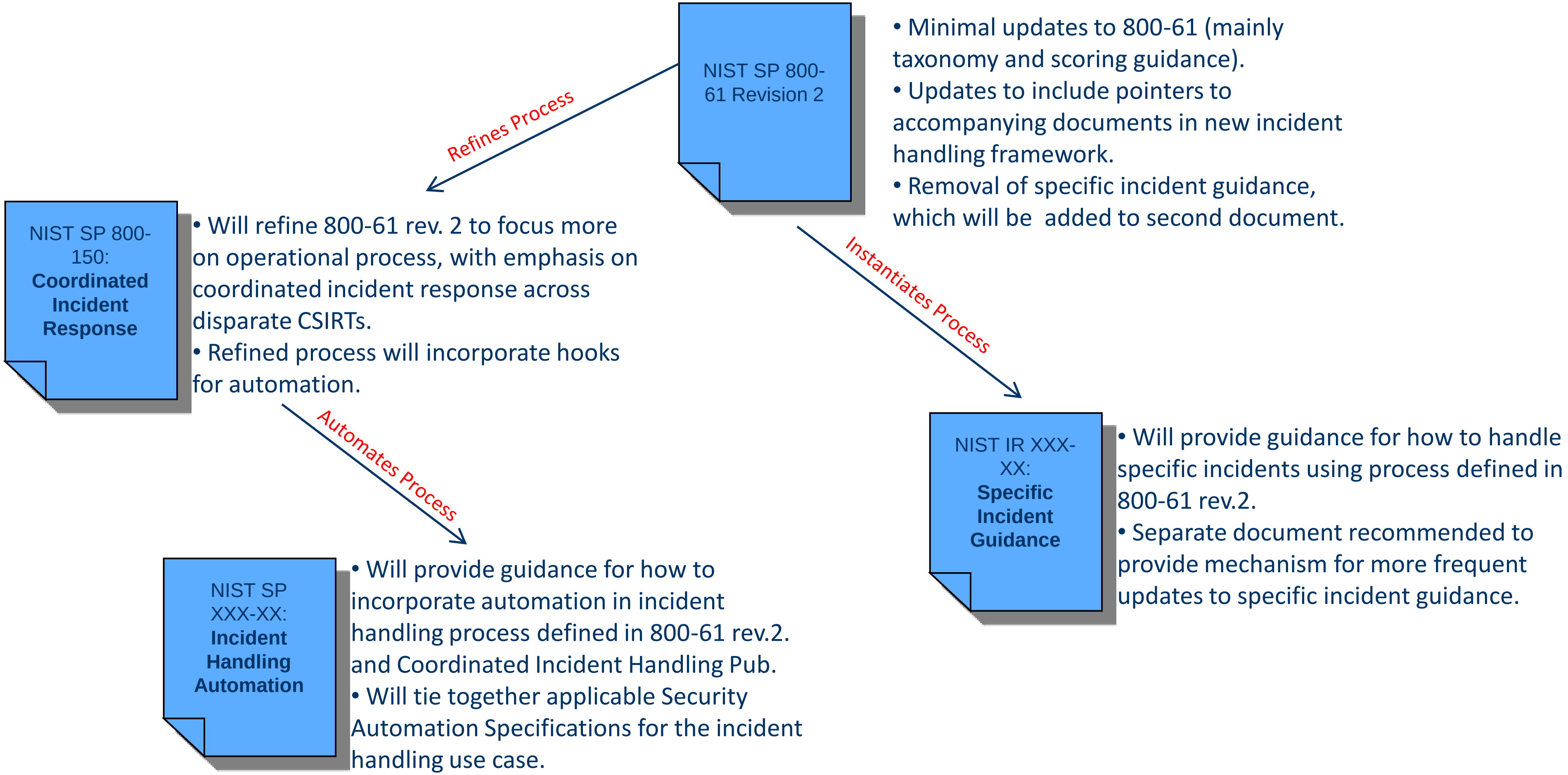
NIST DB releases updated feed containing summary information relating to emerging incidents and vulnerabilities (IODEF, CVE, CCE, CPE, CVSS)

CSIRT identifies a particular un-patched asset on their network and requests more detailed information relating to the incident involving that product (CPE)

NIST DB responds with detailed information pertaining to the specific incident and the indicators of that incident (IODEF, CYBOX, MAEC, CERE)

CSIRT positively identifies the suspected incident and begins to identify/report the incident instance data to US-CERT (IODEF, CEE, CVE, CPE)

Proposed Evolution of NIST SP 800-61 rev.1



NIST SP 800-61 Revision 2

- Minimal updates to 800-61 (mainly taxonomy and scoring guidance).
- Updates to include pointers to accompanying documents in new incident handling framework.
- Removal of specific incident guidance, which will be added to second document.

Refines Process

NIST SP 800-150: **Coordinated Incident Response**

- Will refine 800-61 rev. 2 to focus more on operational process, with emphasis on coordinated incident response across disparate CSIRTs.
- Refined process will incorporate hooks for automation.

Automates Process

NIST SP XXX-XX: **Incident Handling Automation**

- Will provide guidance for how to incorporate automation in incident handling process defined in 800-61 rev.2. and Coordinated Incident Handling Pub.
- Will tie together applicable Security Automation Specifications for the incident handling use case.

Instantiates Process

NIST IR XXX-XX: **Specific Incident Guidance**

- Will provide guidance for how to handle specific incidents using process defined in 800-61 rev.2.
- Separate document recommended to provide mechanism for more frequent updates to specific incident guidance.

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).
  - 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) to be added to list.

Questions & Answers / Discussion

Paul Cichonski

National Institute of Standards and Technology (NIST)

paul.cichonski@nist.gov

(301) 975-5259

EXTRA