Investigative Response Modeling and Predictive Data Collection (RIP)

Dan Moor,
Siva Raj Rajagopalan
HP

Sathya Chandran Sundaramurthy,
Xinming Ou
Kansas State University

Background

- Incident Response is here to stay
- Our security tools do not provide decisive answers
  - Indicators/signatures do not (or rarely) provide enough context to act on the alert alone
  - A cycle of alert/validate/respond consumes analyst time
- Understanding cryptic alerts requires $killed $taff
- Validating alerts requires access, time, skill. Battles must be chosen based on resources

  (another way to look at the High/Med/Low system)

Caveats

- This is not ‘HP’
- My emphasis is IR
  - Scope of impact
  - What happened
  - What was taken
  - Do we have to disclose

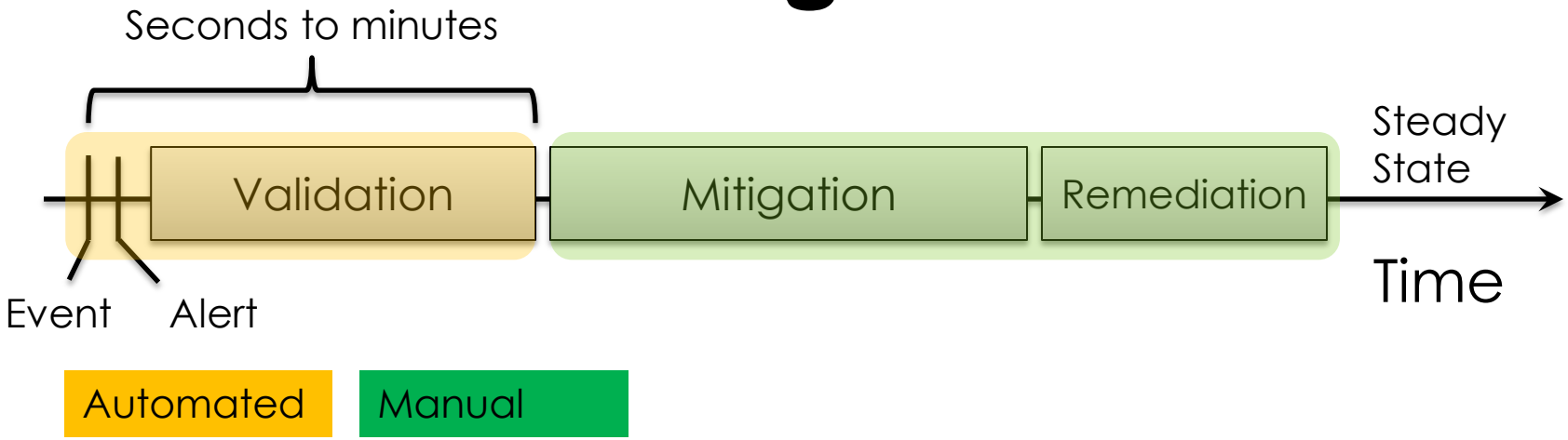
Our goal

- Improve security response efforts through:
  - Increased accuracy of determinations
  - Reduced time spent on investigations
  - Reduction of monitoring staff requirements
  - Improve threat modeling

Background

- Very little automated, investigation and response dictated by skilled human resource availability
- Validation takes minutes to hours if not longer

Background



- Detection and validation are automated. Security resources are utilized to deal with confirmed issues, not double checking the security tools
- Requirements for monitoring staff are significantly reduced

Methodology

Each alert implies that a series of facts be established in order to confirm the event as a threat

- For each threat identify the facts required
- Automate the collection of required data
- Perform automated analysis where possible
- Present the raw data and/or automated analysis to the first level responder for guided evaluation
- Upon the interpretation by the first responder, trigger response as appropriate

Methodology cont.

1. Build a framework of validation steps
2. Build IR/Validation model for a given threat
3. Trigger analysis on alert
4. Collect and present data to users that prompts them to confirm/deny/rank each step
5. Evaluate likelihood of compromise; rank confirmation based on analysis and user input
6. Direct response action (generate ticket, etc.)

Model terminology

Threat: Action or collection of actions that negatively impact your organization

Alert: Event observed via automated means

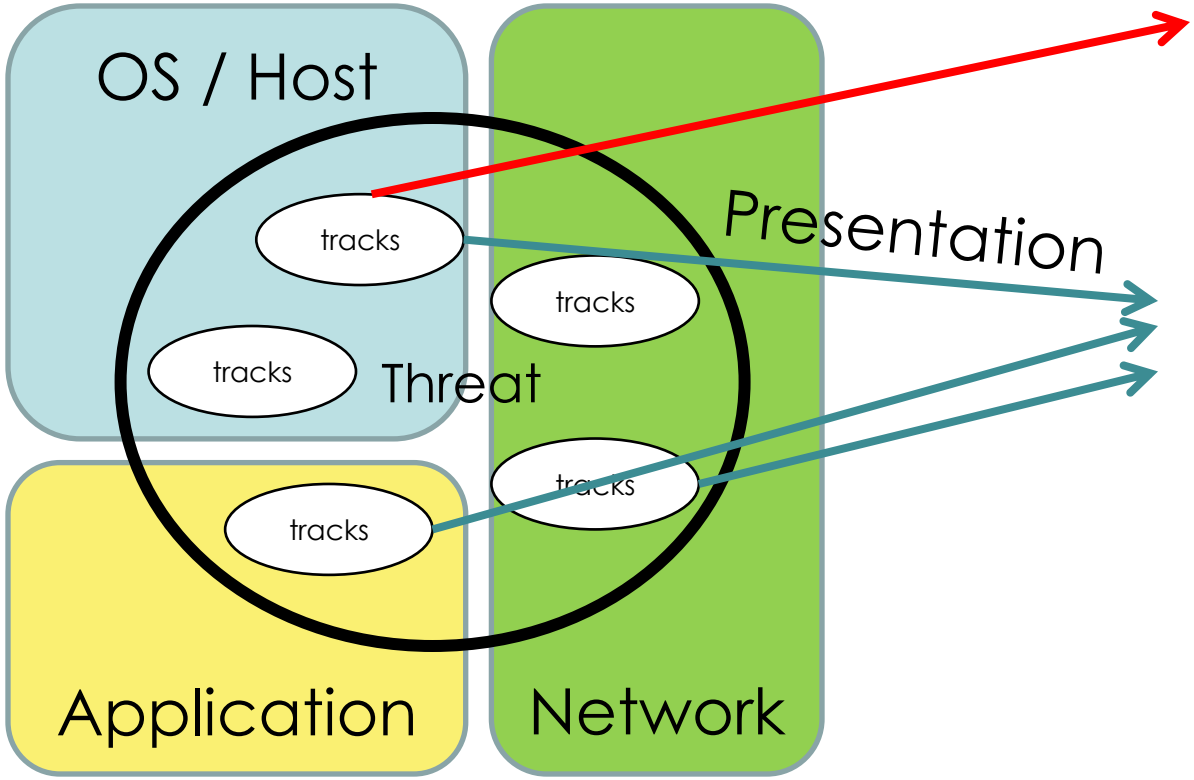
Fact: Expression of a state or value

Data source: System, resource, log, anything 'scriptable'

Analysis: Action of establishing the state of a fact

Weighting: Ranking the likelihood of a threat based on the analysis of a fact or collection of facts

Example model



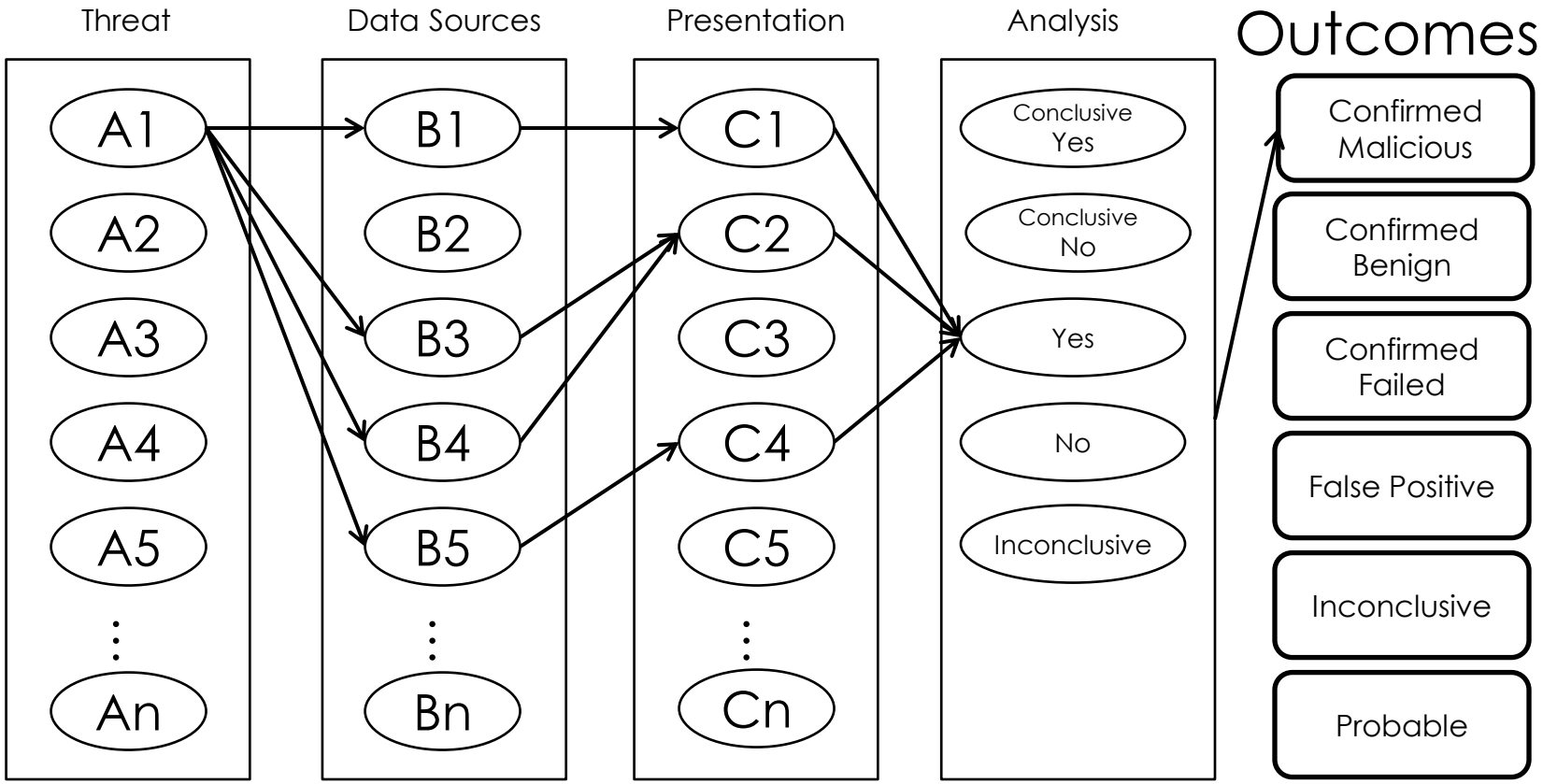
- Alert

Threat confirmation accuracy / confidence low

- Analysis
- Weighting
- Response

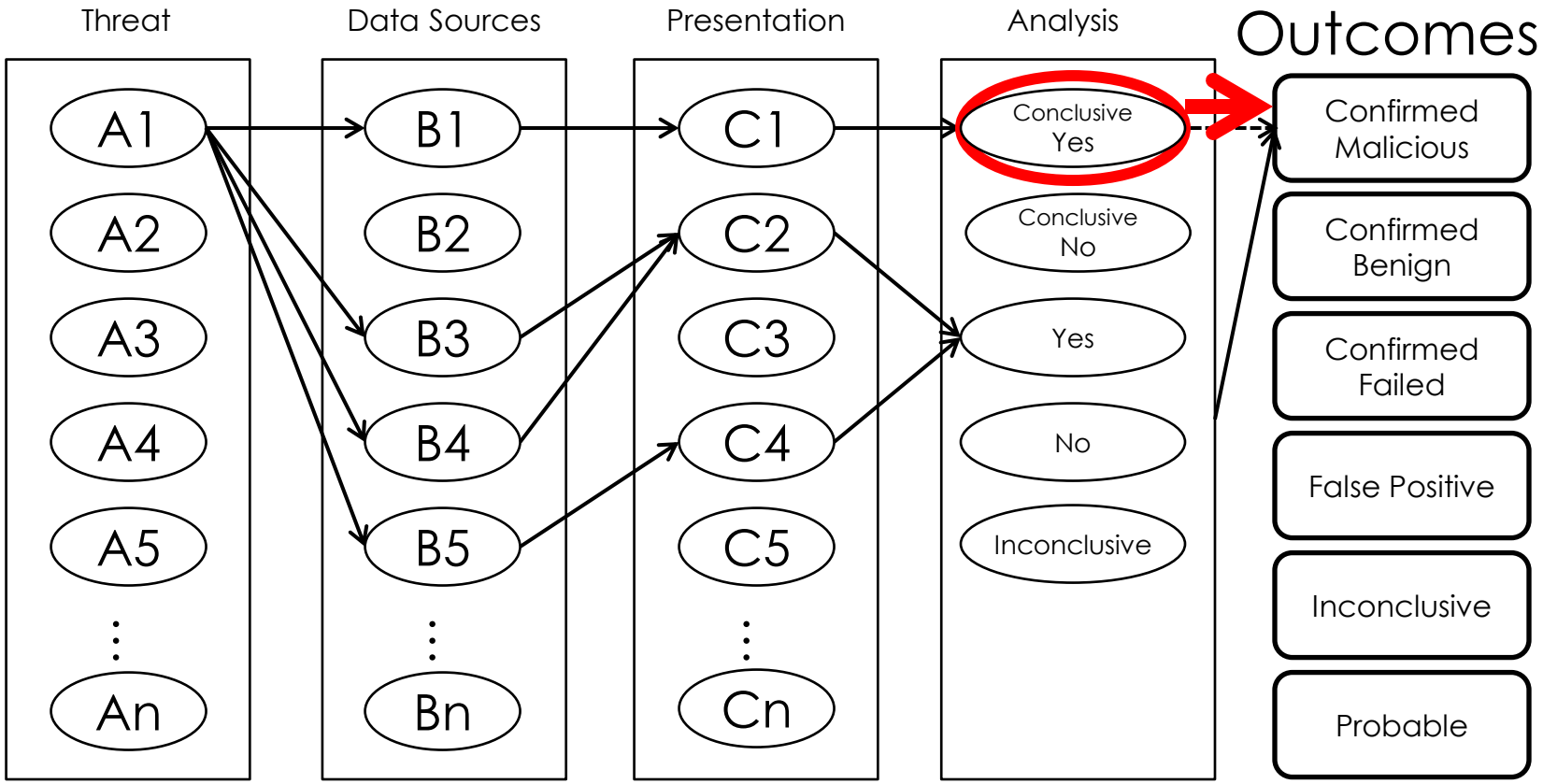
Example scenario

Threat A1 Confirmed as Malicious



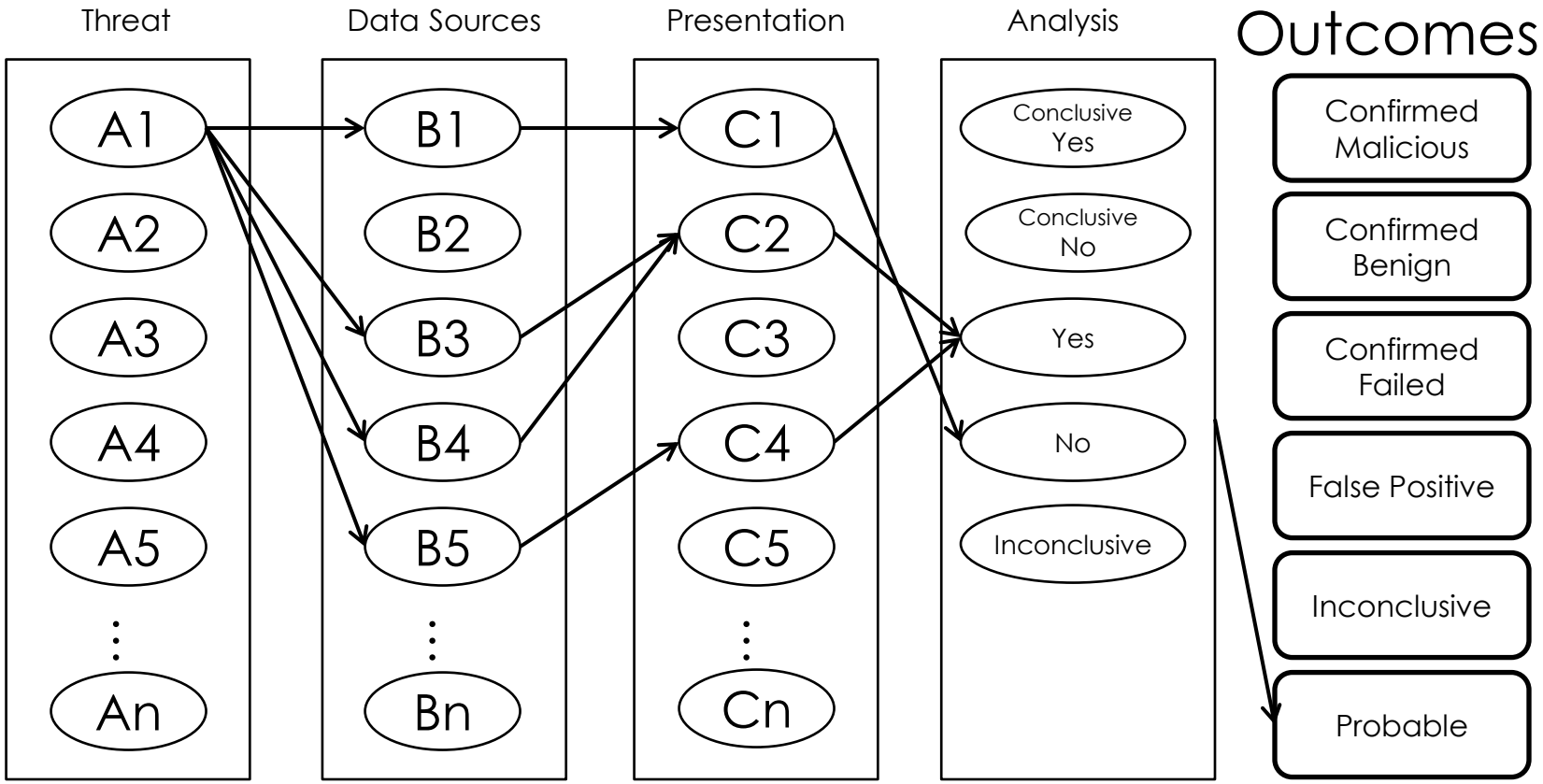
Example scenario

Threat A1 Confirmed as Malicious



Example scenario

Threat A1 Weighted Outcome



Future considerations

- Mine models to identify what should be audited vs. working with what we are given
- Extend framework to non-alert triggered investigations
- Incorporate flexibility in framework for a per-institution flexibility
- Move to an agent based validation engine

Contact information

- Contact presenters at if you are interested in:
  - Asking questions
  - Helping with the project

dan.moor@hp.com

Siva Raj Rajagopalan (Please contact Moor, Ou)

sathya@ksu.edu

xou@ksu.edu