DoD Cyber Crime Center

A Federal Cyber Center

STIX Incident Working Group Kickoff

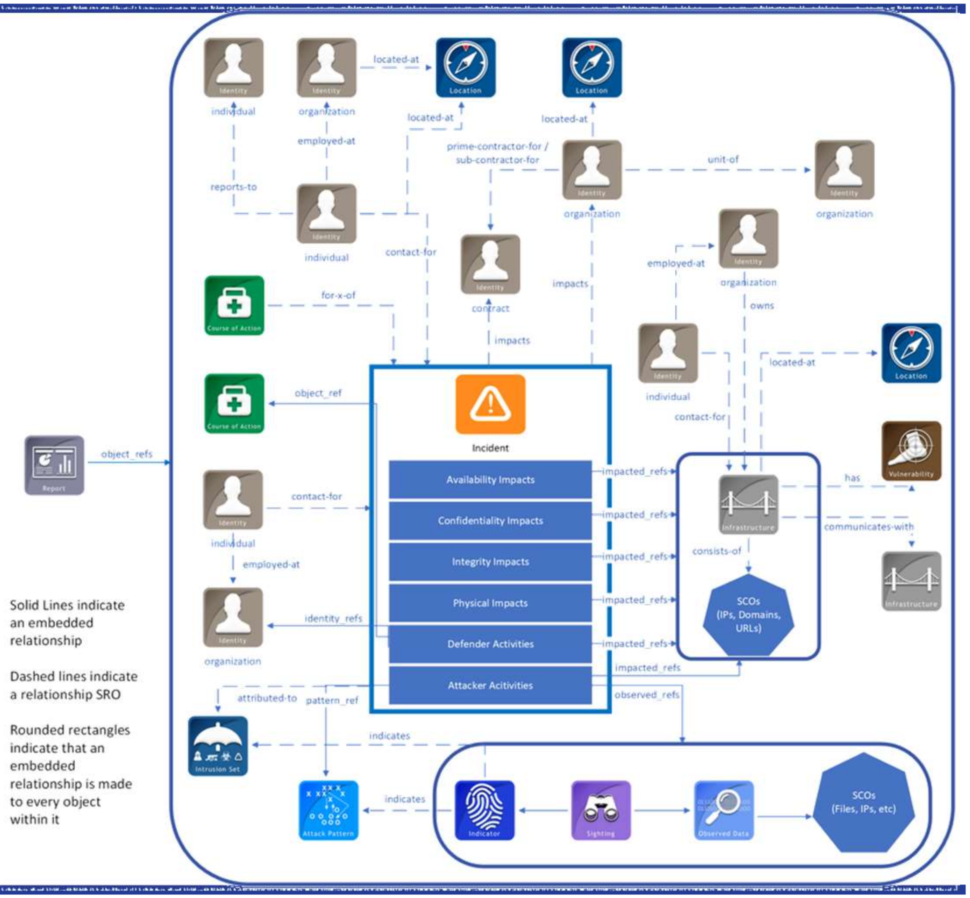
Jeffrey Mates
Computer Scientist
7 April 2023

Where We Are

- **Core Incident Extension 1.0 work has been completed**
  - Works well in a lot of cases
  - Allows for relatively easy expression
- **During Implementation Weaknesses were Found**
  - No way to tie an impact and an activity
  - Some activity types are fuzzy and not necessarily attacker or defender
  - Why can't I say I found an observable as a defender?
  - Hard to say how multiple parties are involved in activities
  - Limited ability to express sub-activities
  - Additional overhead for SEIM workflows that focuses on suspicious activities prior to incidents
  - TAXII level classification filtering means we need to fully re-author incidents to share further

Current STIX 2.1 Incident Report

- **Lots of incident data is stored in other STIX objects**
  - Attack Patterns
  - Courses of Action
  - Identities
  - Indicators / Observations / Sightings
  - Infrastructure
  - Intrusion Sets
  - Locations
  - Report
  - SCOs *(Domains, Files, IPv4, etc.)*
  - Vulnerabilities



Solid Lines indicate an embedded relationship

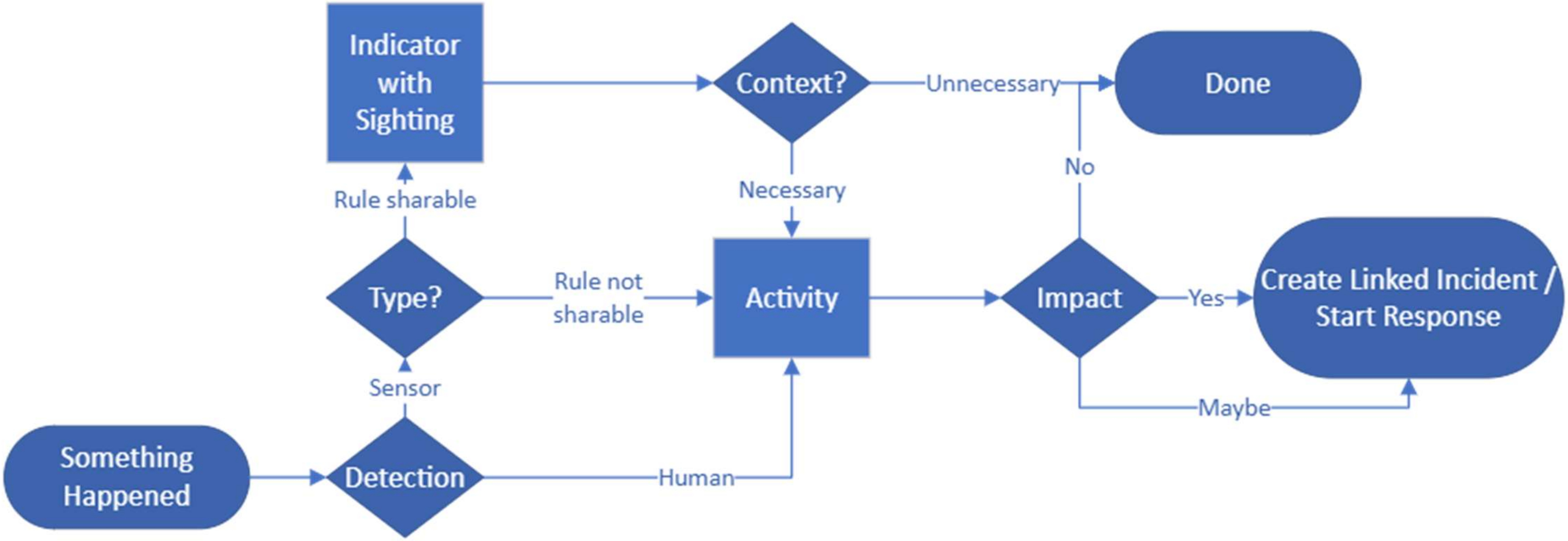
Dashed lines indicate a relationship SRO

Rounded rectangles indicate that an embedded relationship is made to every object within it

Breaking the Incident Extension Up

- 2 SDOs
  - Incident
  - Activity
- 9 SDOs
  - Incident
  - Activity
  - Impact (7): CIA, External, Monetary, Physical, Traceability
- 3 SDOs
  - Incident
  - Activity
  - Impact (1): Use named extensions to record domain specific details for each impact

Malicious Activity Flow



How to Relate the Split Activities

	Relationships	**Embedded:** Incident -> Activity	**Embedded:** Activity -> Incident
Pros	• Allows greatest possible automated redaction • No new parsing concepts	• Only the Incident author can assert these • Pushes vendors to put the details directly in the objects instead of in relationships • Allows activity sequencing	• Allows activity sequencing • Allows full redaction of activities without duplicating incidents
Cons	• Hardest to read / process • Conflicts between vendor tools and GUIs likely • Non-duplicate incidents can share the same activities • No relative sequences • Activities with more than one parent?	• Non-duplicate incidents can share the same activities • Requires making an optionally sequenced list type to avoid losing relative sequence data • Fully redacting activity requires making duplicate incidents	• Third parties can attach activities to an incident • Harder to read / process than using the Incident as the root • Activities must be updated when associated with an Incident

Common Properties for Impacts

Common

- criticality
- description
- labels
- impacted_refs

Partially Shared Properties

- Recoverability
  - Availability
  - Integrity
  - Physical
  - Traceability
- Information Type / Record Count / Record Size
  - Confidentiality
  - Integrity

Unique Properties on Impacts

- Availability: 1
- Confidentiality: 1
- External: 1
- Integrity: 1
- Monetary: 4
- Physical: 2
- Traceability: 1

Splitting Impacts

	Embedded	Split
Pros	• The creating organization defines their own impacts • Easier to parse and understand • Fewer SDOs	• Allows redaction of sensitive impacts • When submitting to external groups this might make it possible to add impacts the original organization was unaware of **IF** the linking pattern allows for it
Cons	• Need to duplicate incidents to define new impacts • Need to duplicate incidents to redact sensitive information about impacts	• Harder to process • We would need to determine how to link these (see the questions on how to split activities) • It could result in a lot of additional SDO types

Additional Questions

- **Should we call it Activities, Incident Activities or something else?**
- **Should we align Activities to Actions in UCO?**
- **What relationships should activities embed and what should be through SROs?**
  - **If I perform a defender activity because of a Sighting of an Indicator how should I link these?**
- **Is fuzzy ordering necessary?**
- **Should impacted_entity_counts be moved under impacts?**
  - **Remaining properties:** criticality, detection_methods, determination, incident_types, investigation_status, recoverability, and scores

DoD Cyber Crime Center

A Federal Cyber Center

Questions?

Jeffrey Mates
Computer Scientist
410-694-4335
jeffrey.mates@us.af.mil
www.dc3.mil