BIWEEKLY FORUM MEETING

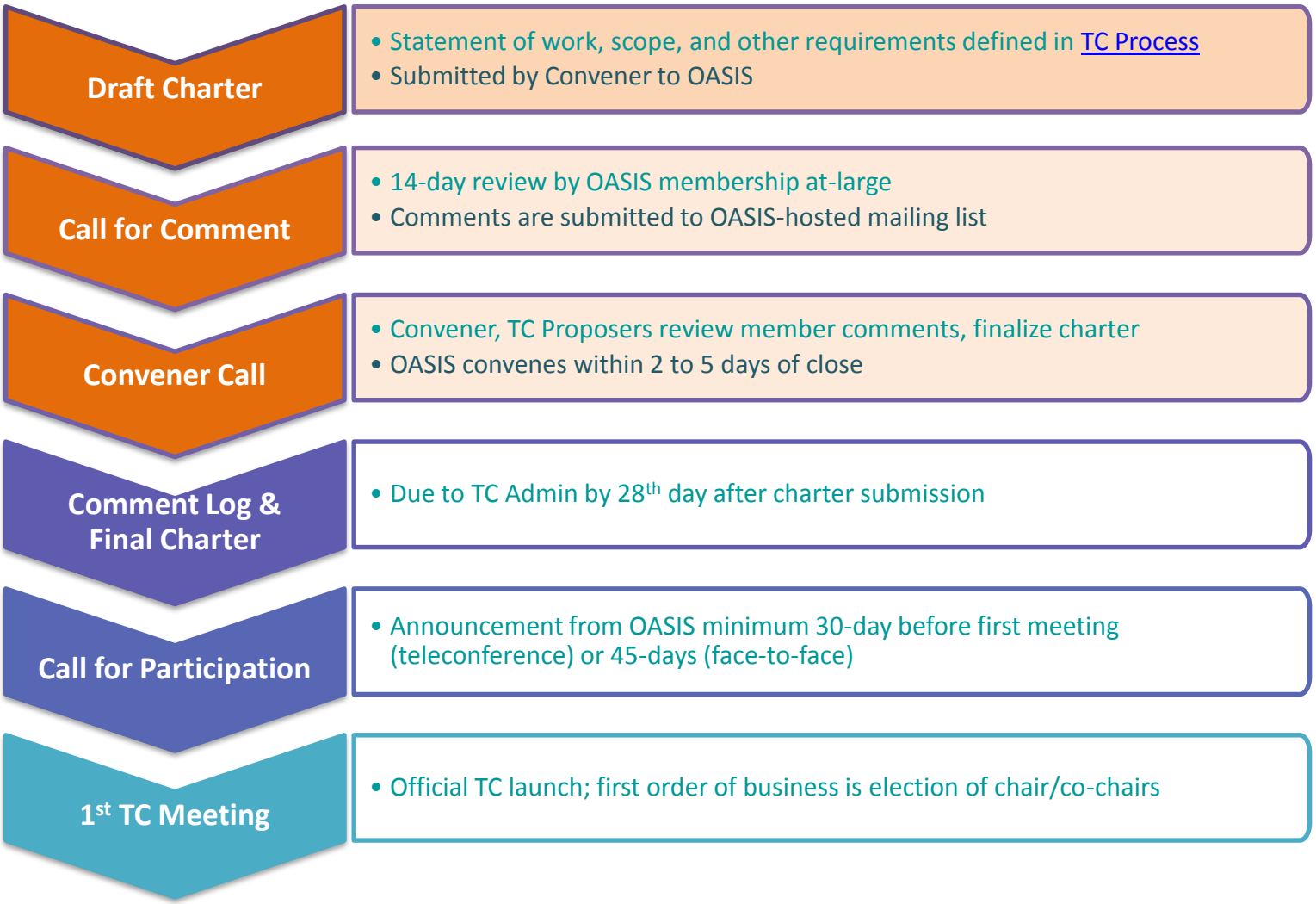
02 Mar 2017

Agenda

- RSA Debrief (Brule)
- OASIS Transition (Ensign)
- LDD Updates (Romano)
- Actuator Profile Subgroup Report (Romano)
- STIX/OpenC2 Subgroup Report (Verma)

RSA Debrief

TC Launch Timeline



TC Launch Timeline

- Timeline for OASIS actions:
  - Call for participation sent
  - Reminder of deadline to join with voting rights (approx. 10 days before first mtg)
  - Call for nominations for chair (approx. 8 days before)
  - Last day to join with voting rights (7 days before 1st meeting)
  - List of eligible voters to mailing list
  - Inaugural meeting

TC Resources when C4P is sent

- Members-only TC web site / collaboration tools (“Kavi”)
  - Only OASIS members may view
- Public TC web site (subset of Members-only)
- TC mailing list
  - Publicly archived
  - Only TC Members may post
  - Only TC Members and Observers are subscribed (automatically)
- TC comment list (non-member feedback to TC)
- TC wiki*
- JIRA issue tracking system*
- Version control system (SVN or GitHub)*

**Created upon request*

Language Description Document

- Updated the Target Data Model
- Removed and updated Actions (33)
- Incorporated many suggested changes
- Reorganized Section 3: OpenC2 Language
  - OpenC2 Command
  - OpenC2 Response
  - OpenC2 Alert

RESPONSE Format


```
(
    RESPONSE (
        SOURCE (
            type = <data-model>:<ACTUATOR_TYPE>,
            <actuator-specifier>
        ),
        [CMDREF = <COMMAND_REFERENCE>,]
        STATUS = <STATUS_CODE>,
        [STATUS_TEXT = <STATUS_TEXT>,]
        RESULTS (
            <DEFINED_VALUE>
        )
    )
)
```

Actuator Profile Subgroup Report

STIX/OpenC2 Subgroup Report

Attendees

- General Dynamics – Jason Romano, Joyce Fai
- NSA – Joeph Brule, Dave Kemp, Kevin Miller, Joan Peterson
- Cisco – Jyoti Verma
- Symantec – Bret Jordan
- Looking Glass – Allan Thomson, Todd Beine
- Cyber Phantom – Sourabh
- sFractal – Duncan Sparrel
- DHS - Juan Gonzales
- JHAPL – Mark Moss
- Mitre – Sean Barnum, Applebaum
- Soltra – Aharon Chernin
- …

History

- Formed a couple of months ago to develop reference implementations for OpenC2 in STIX
- Started off with XML - developed STIX COA in XML for 1.2
- Moved to JSON following STIX 2.0

What we have achieved

- Influenced OpenC2 with decisions from CTI-TC
  - JSON MTI, Cyber Observables etc.
- Socialized and influenced CTI-TC about using OpenC2

Next Steps

- Short term - Complete STIX COA representation for STIX 2.1
  - Ongoing work here - to be done before OpenC2 becomes a TC
- Longer term - Interoperability topics between STIX and OpenC2 – example Playbook

Takeaways from CTI-TC F2F

- Playbook
  - A Playbook represents a workflow for incident response. Following are the characteristics of a playbook:
    - Each step of the playbook can either be manual or automated.
    - Playbook has synchronous or asynchronous steps
    - Every step in the playbook may depend on the response of the earlier step - for sequential steps
    - Playbooks can be very long lived
    - The steps of a playbook could be related to each other out of order

Playbook definitions

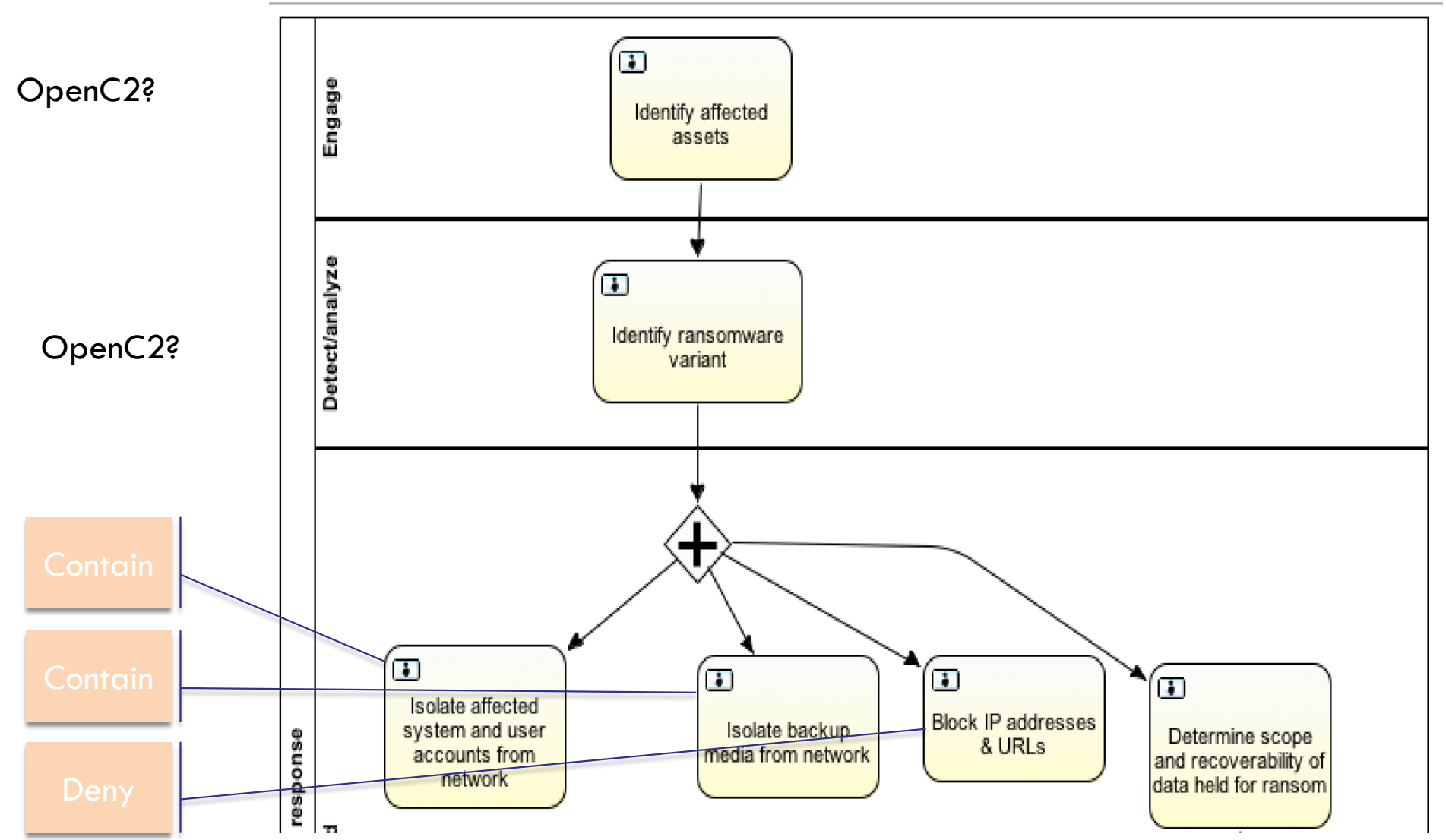
- "Playbook is a named sequence of coa that can be referred to by one or more SDOs (campaign, sighting, ...etc) where the playbook is a top-level SDO that has its own object lifecyle like other objects"
- "Playbooks will contain a series of COAs (manual, process, automated) that have conditional logic and temporal logical associated with each one. Do X then if result Y do Z followed by A and B within 1 day"

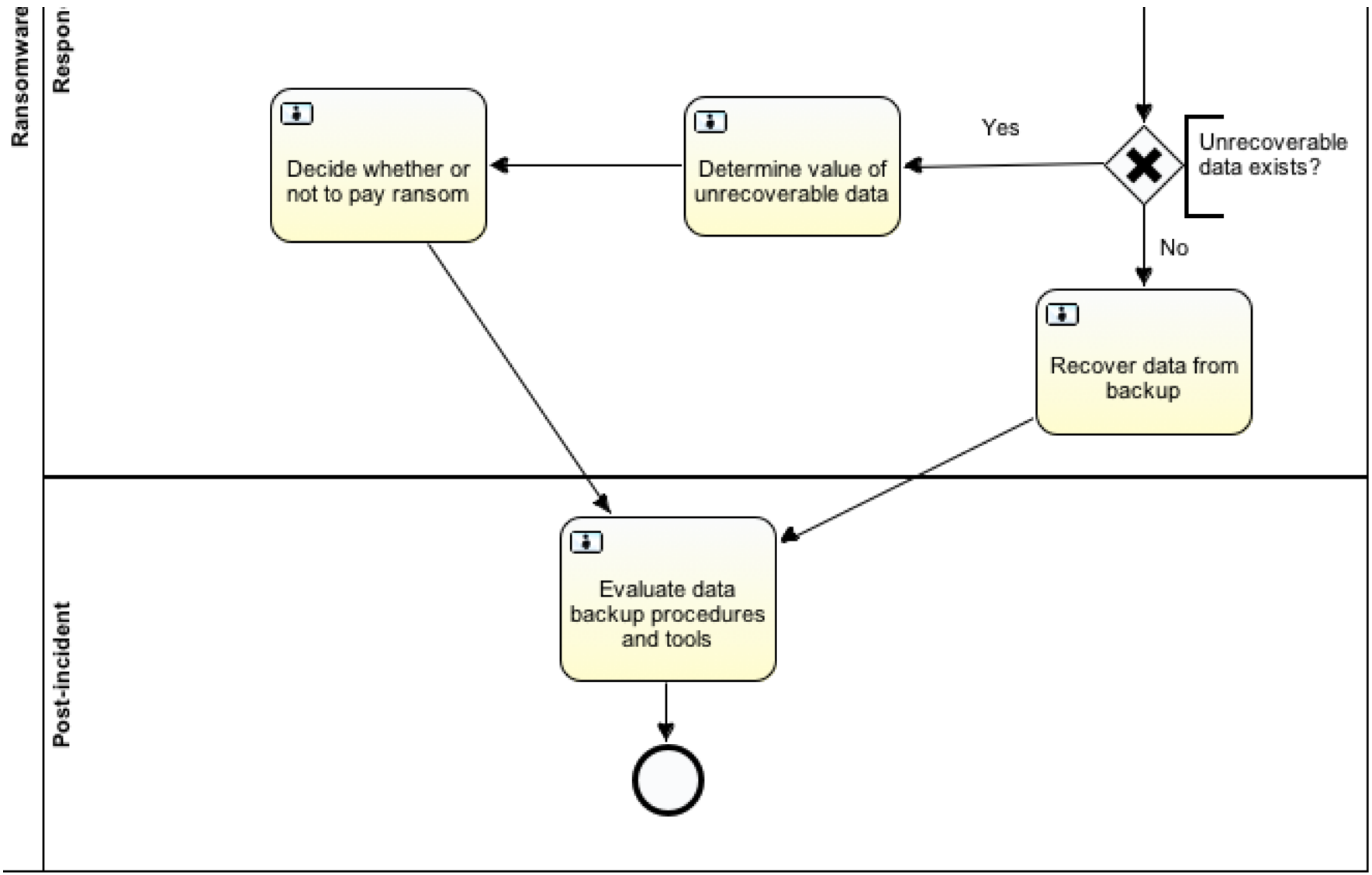
Examples

- Ransomware

OpenC2?

OpenC2?




Ransomware
Respon
Post-incident
Decide whether or not to pay ransom
Determine value of unrecoverable data
Yes
Unrecoverable data exists?
No
Recover data from backup
Evaluate data backup procedures and tools

Open Questions

- How to handle interoperability
  - Participate in mini groups of CTI-TC – Example Playbook
  - Handled by CTI-TC interoperability sub-committee – headed by Allan
  - As part of OpenC2 TC?
  - Liaison group in OASIS?