OpenC2

STATUS AND WAY FORWARD

Joe Brule

Executive Director

17 FEB 2017

Agenda

- Background
  - Motivation
  - Status
- Way Forward
  - Implementation Considerations
  - Reference Implementations
  - Actuator Profiles
  - Path to Standardization
- Future of the OpenC2 Forum

The Motivation and Vision

- Future Cyber Defense Tactics:
  - Sharing of indicators
  - Coordination of response actions
  - Automated, multi-part actions at machine speed
- OpenC2 Forum
  - Identify and fill gaps as they pertain to command and control for the provision or support of cyberdefense
  - Create a diverse and collaborative environment.
- Standardization is a Key Enabler for Unambiguous C2

OpenC2 ‘Philosophy’

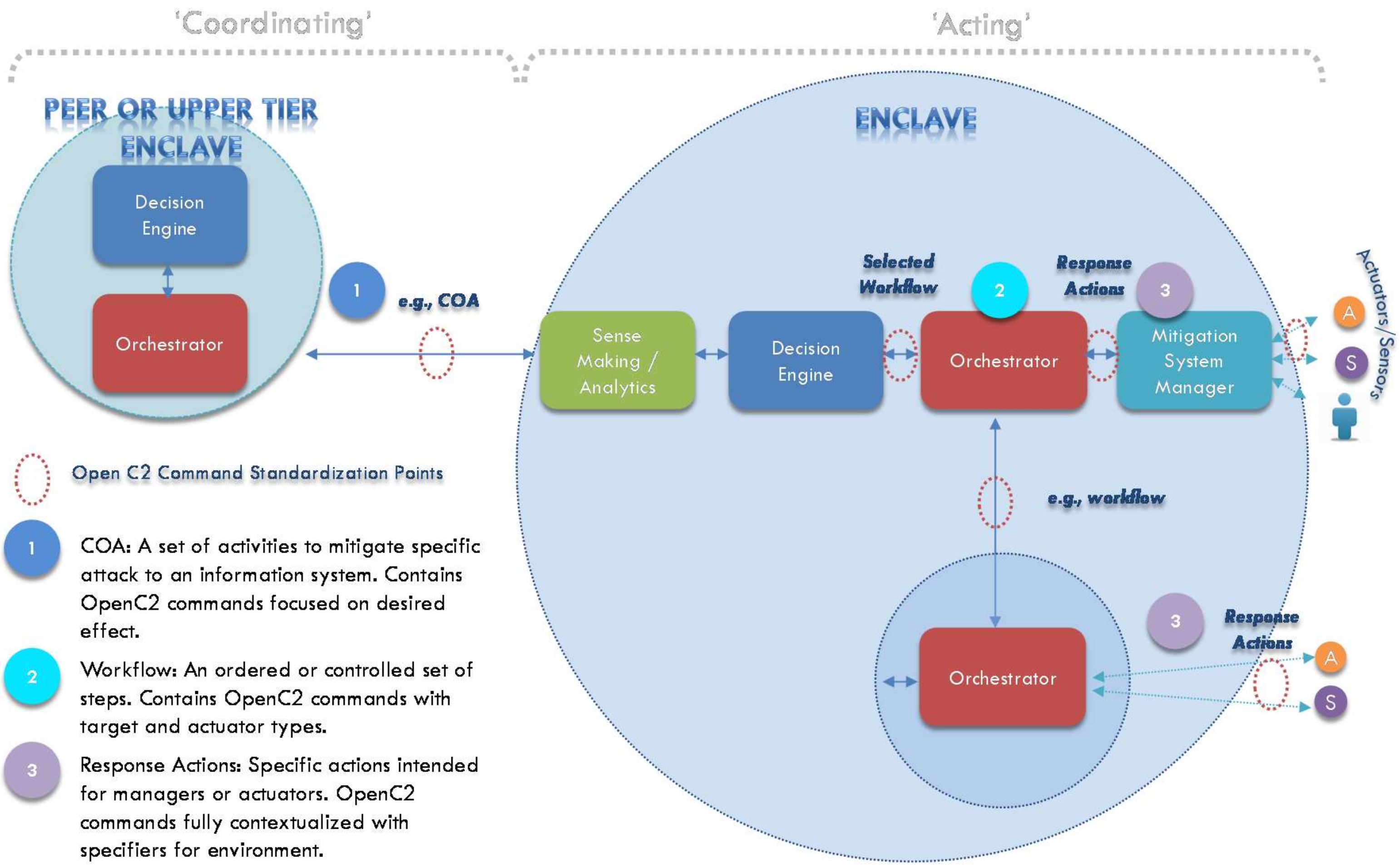
- Pre-existing standards will be leveraged to the greatest extent practical
- Minimize Complexity of Command
  - Minimize Overhead on Sensor/Actuator
  - Facilitate Adoption
- Infrastructure, architecture, and vendor agnostic
- Extensible to support different levels of detail and future technologies

OpenC2 Design Principles

- Lightweight Efficient Machine-to-Machine communications
- Abstract
  - Focuses on 'What' to do vice 'Device Specific'
  - Permits different levels of commanding
- Extensible
  - Enables additional precision and flexibility
- Flexible to facilitate implementation
  - Agnostic of Transport, Information Assurance and Message Fabric
  - Importable data modeling to accommodate new technologies

Enable Unambiguous Machine-to-Machine
Command and Control Messages

OpenC2 Deployment Environments



Open C2 Command Standardization Points

1 COA: A set of activities to mitigate specific attack to an information system. Contains OpenC2 commands focused on desired effect.

2 Workflow: An ordered or controlled set of steps. Contains OpenC2 commands with target and actuator types.

3 Response Actions: Specific actions intended for managers or actuators. OpenC2 commands fully contextualized with specifiers for environment.

Status: Recently Posted

- Language Description Document (Release Candidate)
  - Focus on Semantics
  - Define Lexicon for Actions, Syntax
- Version 1.0 of the IA Considerations Document
- Draft JSON Abstract Encoding Notation
- STIX sub-working group
  - OpenC2 to be included in STIX 2.1
- Draft SDN Profile posted
- Web Presence
  - Documentation (OpenC2.org, Wiki)
  - Collaborative (Github, slack, googledocs)
- Libraries
  - Validation code
  - Sample commands and test suite

Prototypes Posted on Github

- Yuuki
  - University of Maryland
  - Implements OpenC2 as multiple dispatch on type
  - Actuators are dynamically created and hot swappable
- OrchID
  - Zepko
  - OpenC2 proxy built in Django
- OCAS
  - S-fractal
  - OpenC2 API Proxy written in ERLANG
- G-2
  - G-2
  - Implementation of OpenC2 on open source firewall written in C

Additional Prototype Efforts

- Perimeter Firewall
  - Joint NSA, Phantom Cyber
  - DENY, ALLOW issued to Palo Alto Firewall
- Cisco ASA Prototype Implementation
  - Cisco
  - Orchestrator issues DENY and ALLOW to Cisco ASA based on CTIA update
- Implement Distributed Policy Convergence with OpenC2
  - Cisco
  - Use of Pub-Sub Architecture to Reduce Convergence time
- IACD Course of Action Implementation
  - JHU/APL on behalf of NSA
  - 15 OpenC2 Actions issued to Nine actuators
  - Implemented in Java

Next Steps

- Actuator Profiles
  - Produce Guide for Creation of Profiles
  - Define applicable Actions and actuator specific Modifiers and Specifiers
  - Firewall Profile Underway
  - Router Profile Pending
- Document Implementation Considerations
  - Address issues to build interoperable implementations
  - External dependencies such as IA, Transport etc.
- OpenC2 Data Model for Target Space
- Polyglot Implementation
- OpenC2 Tutorial
- Negotiation Protocol
- Transition to OASIS

Transition of Forum

- OASIS
  - Draft Charter for OASIS Technical Committee
  - Identify Chair, Secretary, Tempo
  - OASIS Kickoff
- External Engagements
  - RSA Presentation
    - STIX, TAXII and OpenC2
  - DHS IACD Effort
  - Information Assurance Symposium

Questions?

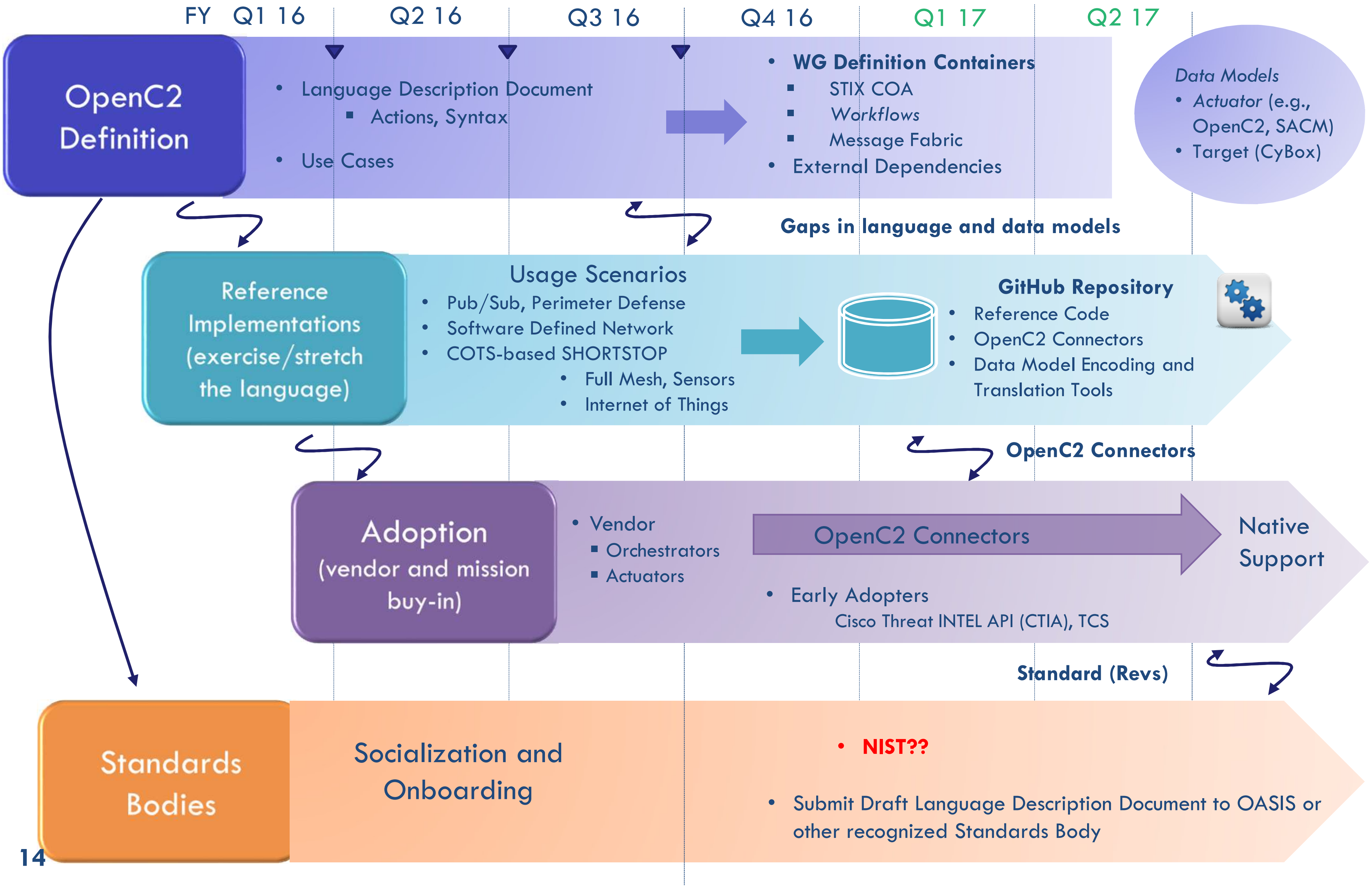
Before I Leave…

Kickoff July 29, 2015	**20 individuals representing 8 organizations**
March 2016	**Public Facing Website & Collaboration site**
April 2016	**First Profile (SDN)**
August 2016	**Release Candidate of Language Description Document**
August 2016	**Five Prototype Implementations Posted on GitHub**
September 2016	**Formalized Charter, By-Laws, and Membership Agreement**
~ April 2017	**OASIS Kickoff Meeting (Planned)**

Membership and Tempo

- Participation includes 33 Member Organizations
- Two Sub-committees
- Biweekly Telecons & Quarterly Face-to-Face Meetings

OpenC2 Standardization Timeline



FY Q1 16 | Q2 16 | Q3 16 | Q4 16 | Q1 17 | Q2 17

OpenC2 Definition

- Language Description Document
  - Actions, Syntax
- Use Cases

- **WG Definition Containers**
  - STIX COA
  - *Workflows*
  - Message Fabric
- External Dependencies

Data Models

- *Actuator* (e.g., OpenC2, SACM)
- Target (CyBox)

Gaps in language and data models

Reference Implementations (exercise/stretch the language)

Usage Scenarios

- Pub/Sub, Perimeter Defense
- Software Defined Network
- COTS-based SHORTSTOP
  - Full Mesh, Sensors
  - Internet of Things

GitHub Repository

- Reference Code
- OpenC2 Connectors
- Data Model Encoding and Translation Tools

OpenC2 Connectors

Adoption (vendor and mission buy-in)

- Vendor
  - Orchestrators
  - Actuators

OpenC2 Connectors

Native Support

- Early Adopters

  Cisco Threat INTEL API (CTIA), TCS

Standard (Revs)

Standards Bodies

Socialization and Onboarding

- **NIST??**
- Submit Draft Language Description Document to OASIS or other recognized Standards Body