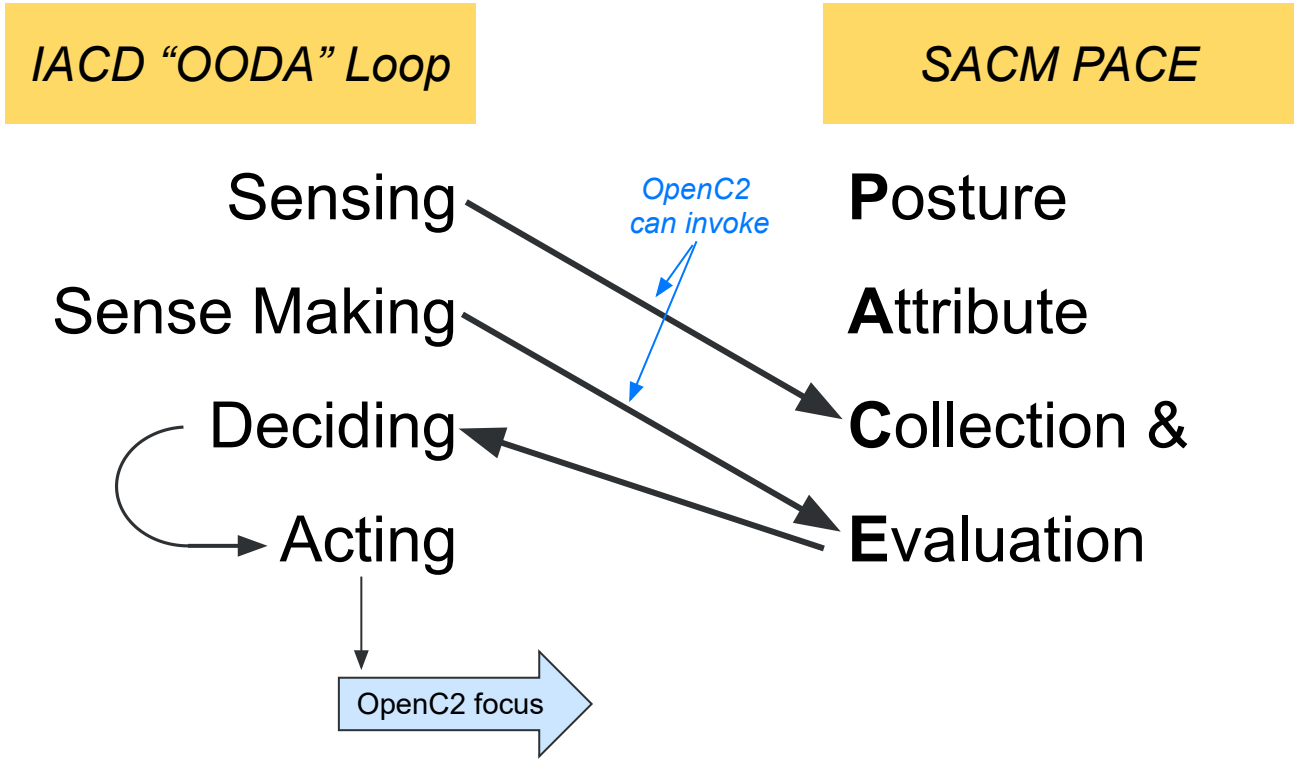
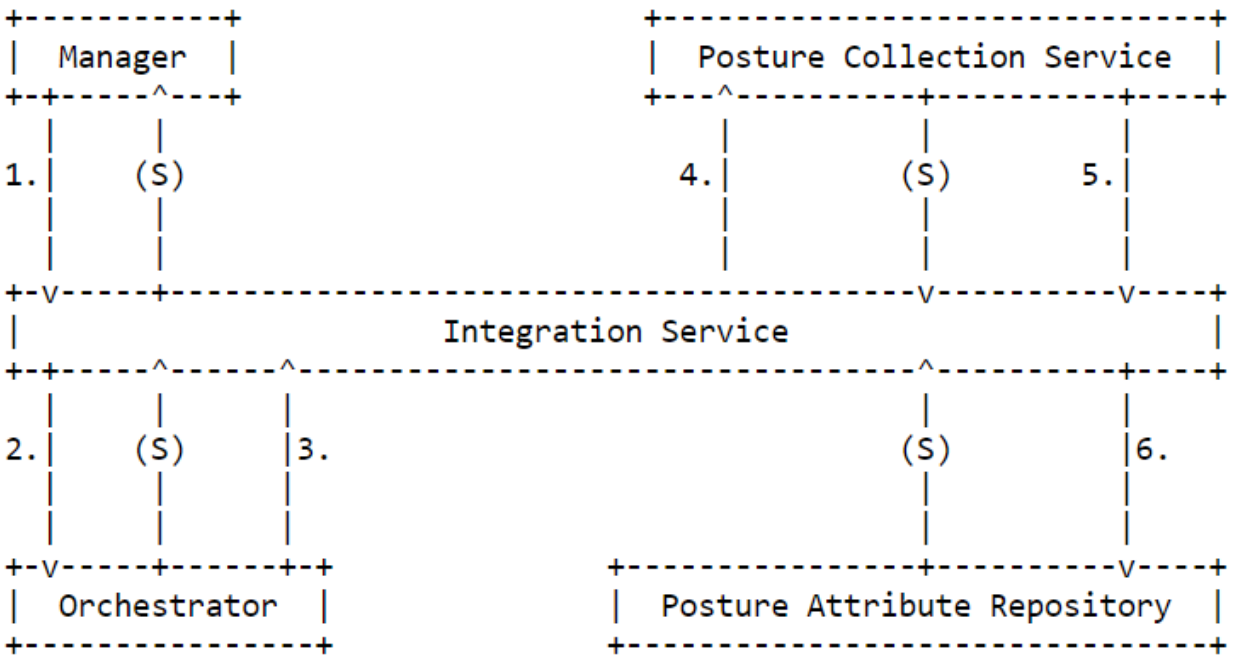
SACM & OpenC2 Prototyping

HII Initial Thoughts

Context (100,000 foot view)

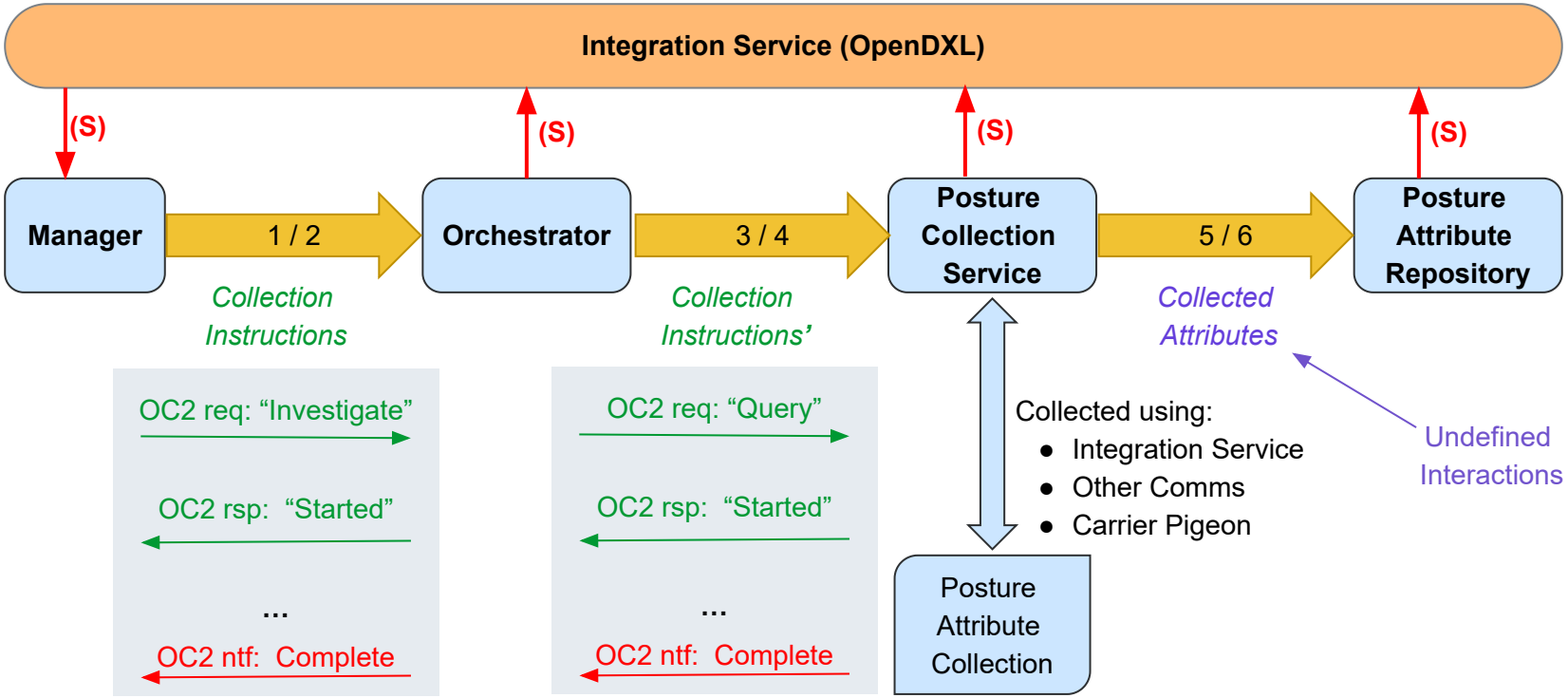


Ad Hoc Collection (ref p35 of SACM Architecture ID)



- Interactions 1 / 2 and 3 / 4 are good fit with OpenC2
- (S)tatus messages could be OpenC2 “notification”
  - *Good use case to define notifications*
- Interactions 5 / 6 are outside usual OpenC2 scope

Ad Hoc Collection Using OpenC2 (ref p35 of SACM Architecture ID)



Component Mapping

- OIF Orchestrator addresses much of
  - SACM Manager
  - SACM Orchestrator
- Posture Collection Service ≅ OpenC2 Actuator
  - Actuator Profile Needed
- Outside OpenC2 Scope
  - Repositories
  - Posture Evaluation Service
  - PCS ⇔ Endpoint interactions

Overall Approach

- Map functions to available HII components (OIF Orchestrator, Device, Yuuki)
- Select OpenC2 *actions* and *targets* to fit SACM process
  - Consider need for new actions or targets
- Develop PCS Actuator Profile
- Define messaging interactions
- Flesh out OpenC2 notification use case, message format for status reporting
- Integrate SACM data model into messages when available
- Other scenarios (*ad hoc* evaluation, periodic collection, etc.) appear to be straightforward extensions

OpenC2 / SACM Conceptual Disconnects

- OpenDXL service handlers vs. OpenC2 Request / Response Model
- Component Registration interactions outside OpenC2 scope
  - thought of ZeroConf
- Administrative Interface
  - Capability Advertisement reverse of OpenC2 “`query features`”
  - Health Check can use OpenC2 “`query`” action
  - Heartbeat has no OpenC2 equivalent

Candidate Technologies to Complement OpenC2

- ELK Stack
  - **E**lasticSearch - Data storage - Posture Attribute Repository
  - **L**ogstash - Data processing pipeline
  - **K**ibana - Data visualization
  - Beats - Data shippers - Piece of Posture Collection Service
- TIG/TICK Stack
  - **T**elegraf - Metric collection - Piece of Posture Collection Service
  - **I**nfluxDB - Time series database - Posture Attribute Repository
  - **G**raphana/**C**hronograf - Data visualization
  - **K**apacitor - Data processing engine

References

- RFC 7632: Endpoint Security Poster Assessment: Enterprise Use Cases (Sept 2015)
- RFC 8248: Security Automation and Continuous Monitoring (SACM) Requirements (Sept 2017)
- draft-ietf-sacm-arch-13: Security Automation and Continuous Monitoring (SACM) Architecture (July 2021)
- draft-ietf-sacm-terminology-16: Security Automation and Continuous Monitoring (SACM) Terminology (Dec 2018, expired)