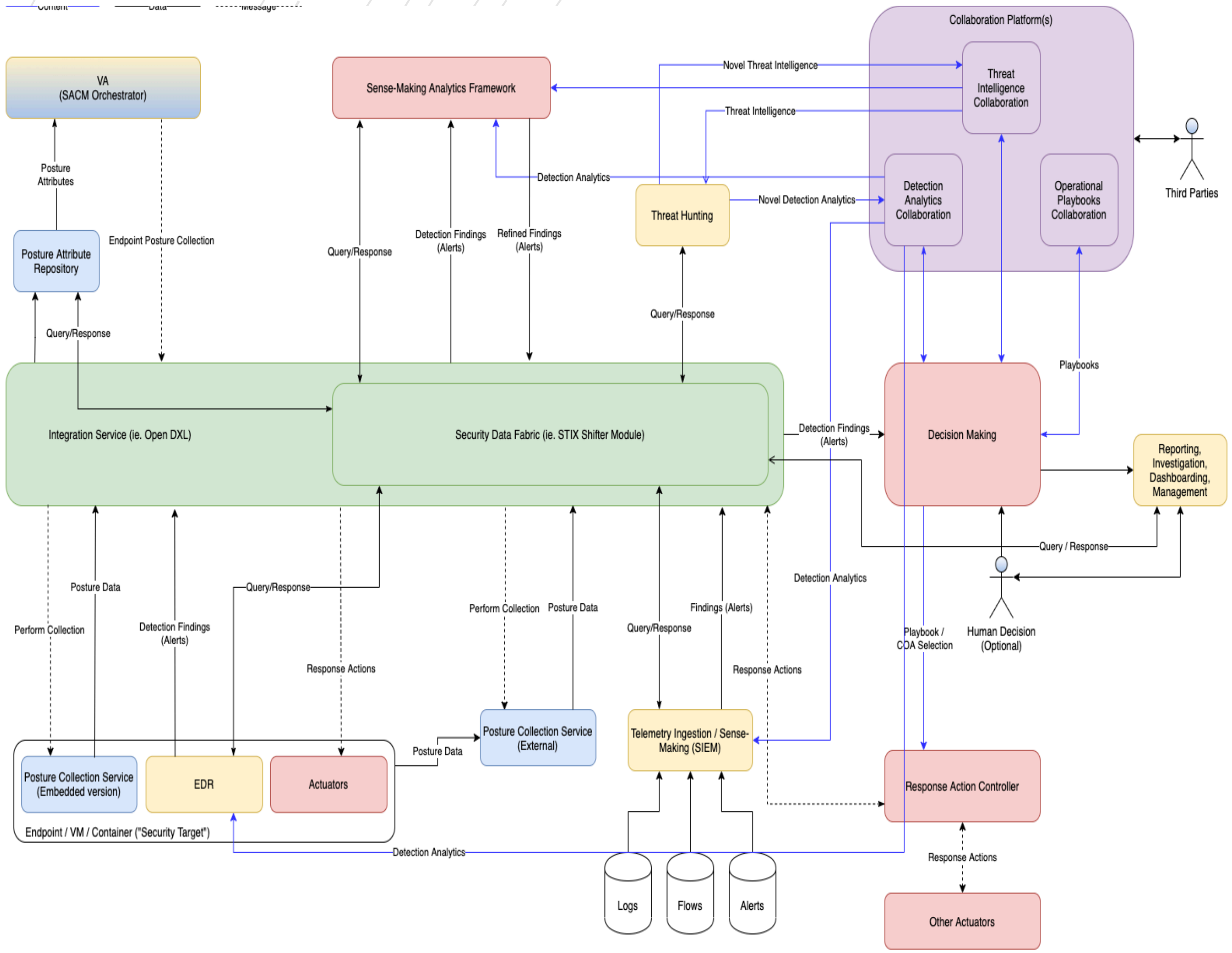
OASIS OPEN PROJECTS

OPEN CYBERSECURITY ALLIANCE

Workgroup Objectives

- Based on the terrific work that the Architecture Working Group have created, with an initial offering of the reference architecture here (https://github.com/opencybersecurityalliance/documentation/blob/master/SACM_OCA_IACD.png) we want to turn this into practical implementations.
- **The rough expectation is to allocate an hour per week of a technical resource within your organization** to deliver on Phase 1 and Phase 2 over the next 9 weeks. 9 weeks of minor work per organization will really see this project take off.
  - *Phase 1* - Over next 4 weeks we ask that work with your peers in your category and define some Actions and Notifications for your category, leveraging the outline/samples here https://opencybersecurityalliance.github.io/opendxl-ontology/ . The project management working group, led by Russ Warren & Adam Montville, will be working to help get these calls organized and track the work.
  - *Phase 2* – Over subsequent 4 weeks, we ask that create Actions and Notification code for your category, again leveraging the outline/samples here https://opencybersecurityalliance.github.io/opendxl-ontology/

Bring It Together
Reference Architecture (Draft)



Aligned with applicable existing open projects and standards

- **SCAP**
- **IACD**
- **OpenDXL**
- **STIXShifter**

Positioned Industry Function and Information Sharing Capabilities

Enable architecture to define interoperation points (Actions, Data) to enable collaboration

OpenDXL Ontology

Open, interoperable cybersecurity messaging format

Categorized set of messages used to perform actions and/or notify

Other common open standards for message content (OpenC2, STIX, etc.)

Sample code on how to integrate the ontology into existing security products and related solutions

Workstream Initiative

Vulnerability
Compliance
Policy
Endpoint

SOAR

OT Embedded
Security

Threat
Intelligence

Overlay
Consolidators
Consultancy

Infrastructure

SIEM

Thank You.

opencybersecurityalliance.org