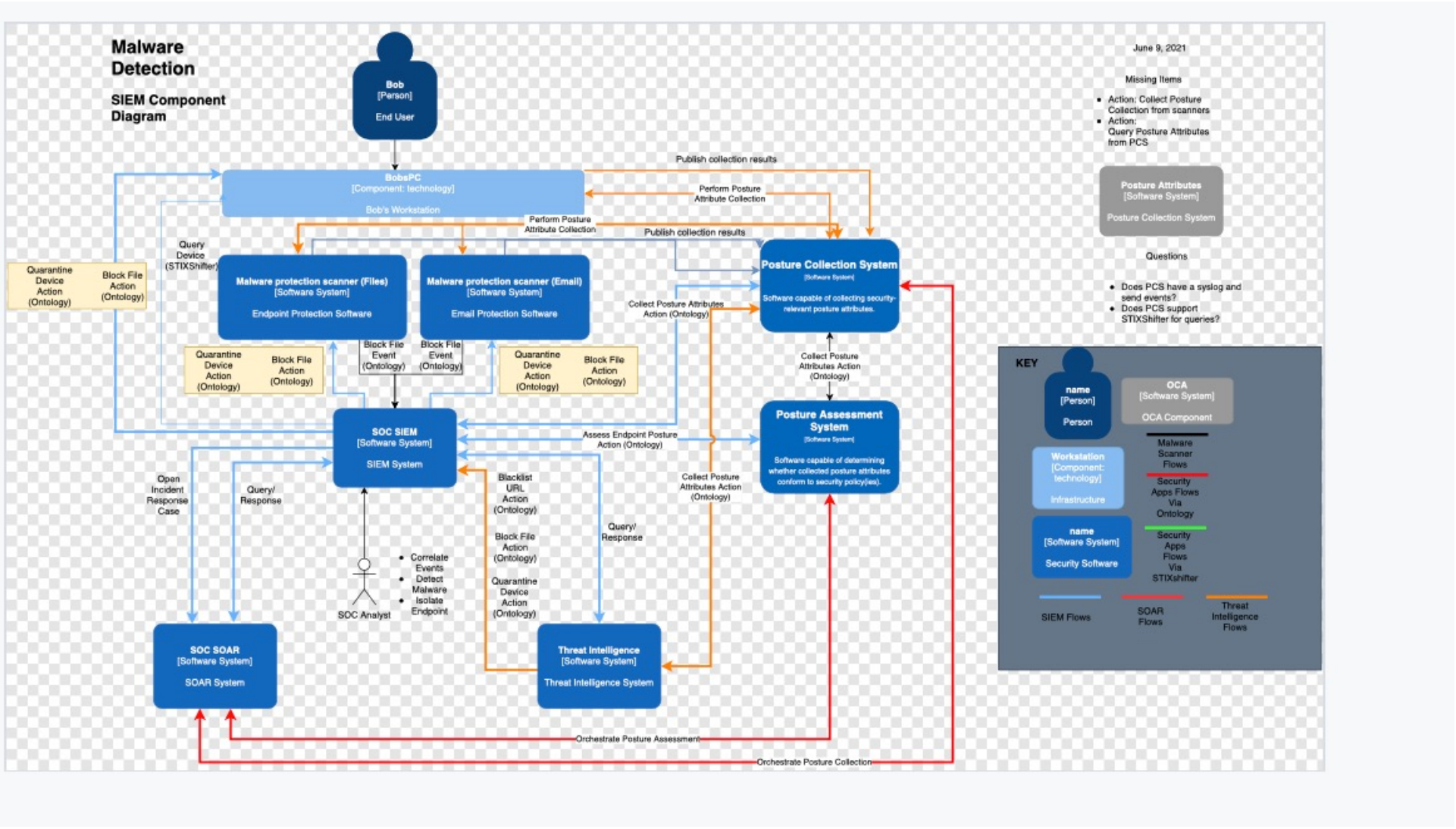
Using OpenC2 in OCA

Current OCA Architecture Diagram
(Malware Use Case)



OpenC2 Actions

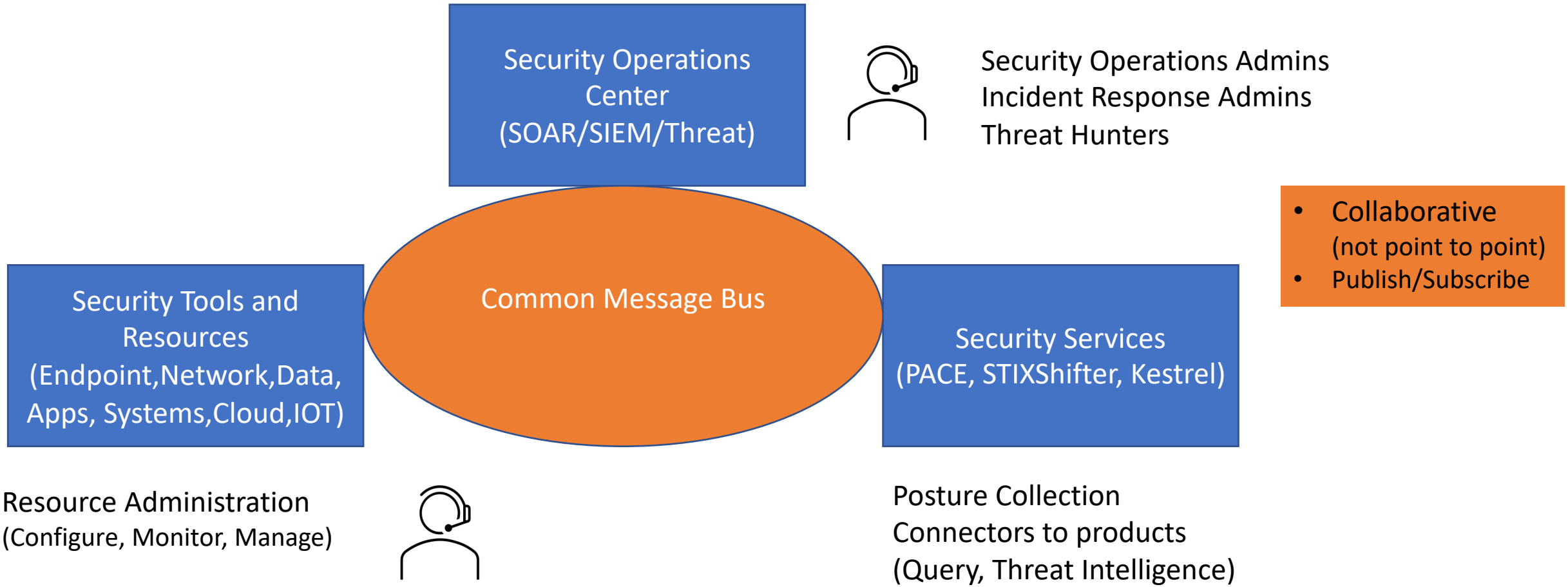
ID	Name	Description
1	**scan**	Systematic examination of some aspect of the entity or its environment.
2	**locate**	Find an object physically, logically, functionally, or by organization.
3	**query**	Initiate a request for information.
6	**deny**	Prevent a certain event or action from completion, such as preventing a flow from reaching a destination or preventing access.
7	**contain**	Isolate a file, process, or entity so that it cannot modify or access assets or processes.
8	**allow**	Permit access to or execution of a Target.
9	**start**	Initiate a process, application, system, or activity.
10	**stop**	Halt a system or end an activity.
11	**restart**	Stop then start a system or an activity.
14	**cancel**	Invalidate a previously issued Action.
15	**set**	Change a value, configuration, or state of a managed entity.
16	**update**	Instruct a component to retrieve, install, process, and operate in accordance with a software update, reconfiguration, or other update.
18	**redirect**	Change the flow of traffic to a destination other than its original destination.
19	**create**	Add a new entity of a known type (e.g., data, files, directories).
20	**delete**	Remove an entity (e.g., data, files, flows).
22	**detonate**	Execute and observe the behavior of a Target (e.g., file, hyperlink) in an isolated environment.
23	**restore**	Return a system to a previously known state.
28	**copy**	Duplicate an object, file, data flow, or artifact.
30	**investigate**	Task the recipient to aggregate and report information as it pertains to a security event or incident.
32	**remediate**	Task the recipient to eliminate a vulnerability or attack point.

Usage Requirements:

Mapping OCA to OpenC2

OpenC2	OCA
Query	Query
Notification?	Response
Deny?	Quarantine, Block File Action
Start?	Open Incident Response
PACE?	Orchestration Process
	Collect Posture
	Assess Endpoint Posture

OCA Architecture - Communications



Next Steps

- Approach for OpenC2
  - Actuator(s)
  - Mapping to command/responses
  - Assess communications layer (pub/sub)
  - Assess responses/event handling

- Sync with PACE
  - Adapting to OpenC2
  - Remap to OCA architecture