In mid-November Russ Warren from the Open Cybersecurity Alliance (OCA) Architecture WG provided several use cases to a small group of OpenC2 TC members, focused on query functions that OCA would like to see supported either in the EDR or another AP. As discussed at today's working meeting, I'm circulating these to the TC mail list for broader visibility. I'm also attaching some slides Russ created highlighting where he saw these use cases extending the functions needed in the EDR AP. At some point this material needs to be capture in the OpenC2 Use Cases GH repo.

The EDR AP editors wish to divide the AP into an Endpoint Response (ER) AP, which is the current content, and a future "Analytics"AP (qualifier in the name to be determined, e.g., "Endpoint Analytics"). These use cases most likely apply to the Analytics AP rather than the current "ER"AP.

Overview: Mapping OpenC2 to leverage STIX and STIXShifter
There are 3 personas mapped in this document. The SOC Administrator, The threat hunter /threat investigator and the SOAR administrator. STIX provides the ability to map to observable objects from security products. STIXShifter maps between STIX and the proprietary product's APIs and data formats and STIX.

Reference: https://docs.oasis-open.org/cti/stix/v2.0/stix-v2.0-part4-cyber-observable-objects.html

What can be done with this technology? You can query ANY of the objects defined in the specification, consistently across the security products. The use cases below are EXAMPLES (any query is possible to these objects) and additional use cases and personas could easily be added. These are examples so we can determine how to best leverage STIX/STIXShifter implementations with OpenC2.

Use Cases via STIXShifter
(1) SOC Administrators wants to (via STIXShifter)
a. execute a federated search (by selecting Scan now/Scan again from the right menu) for all of these IOCs across all data sources defined to gain context on security events received. This results in a query to each data source via STIX.
b. Select an Azure Sentinel Data Source, but it is possible to choose another one and look at the logs. From here he/she can select different filtering criteria, analytics functionality and, eventually, run additional Federated Search using one of the indicators.
c. Do Data investigation to identify actual root cause, user and attackers involved
d. Do the initial triage; Analyst Jeff needs to determine if the incident is an actual event or a false alarm. To analyze the incident in more detail, Jeff reviews the artifacts provided with the case. The Artifacts tab contains the source and destination IP information, provided by a Query.
e. directly perform a deeper analysis by invoking a data query to the data sources
f. Using the data query, Jeff can gain immediate visibility into all connected security tools and possible further insights without having to collect and store the data first.
g. Gain more context of a security incident by a query for the source IP address from the case is based on a search in the open standard STIX and returns results from each data source.
h. Decorated values (IP's, Hashes) can be selected to bring information from threat intelligence and connected asset and risk database
i. Wants to detect suspicious or malicious behavior on endpoints across their environment. This can be done by searching for the hash of a particular file.
j. Want to detect unapproved port activity in their environment. This can help to identify installation of new unapproved software or a successful compromise of a host,

(2) Threat Hunter wants to:(via Kestrel)

a. Query Services running/processes running on an endpoint

b. Query Known TTPs from threat detection systems and threat intelligence feeds

c. Query Connections on the endpoint

d. Query Network traffic (source/dest)

e. You can find connected entities easily in Kestrel, for example, child processes created of processes, network traffic created by processes, files loaded by processes, users who own the processes. To do so, use the FIND command with a previously created Kestrel variable, which stores a list of entities from which to find connected entities.

f. Threat Analysts analyze and prioritize which threats are most urgent to address. The analysts can leverage Federated Search and run a wide search for Indicators of compromise (IOCs) in their environment, and determine which threats might already be present in the environment and need to be handled first"

(3) Incident Responder (SOAR) want to

1. Run a Ransomware"playbook and the related workflow is started if at least one IOC is matched on the Threat Intelligence feeds. Incident responder can Select one of the artifacts in the case (e.g., the hash 834d876b47ae8e595ae417a370cd47cc8e061131), and start a query. Go over the results set of the query. Add the File Name, either ryuk-bin.exe or ruyk.bin depending on which Data source you have selected, as an artifact to the case.

References

OCA home page: https://opencybersecurityalliance.org/

OCA on GitHub: https://github.com/opencybersecurityalliance

STIX-Shifter: an open source library allowing software to connect to data repositories using STIX Patterning, and return results as STIX Observations. (https://github.com/opencybersecurityalliance/stix-shifter)

Kestrel: threat hunting language: building reusable, composable, and shareable huntflows across different data sources and threat intel. (https://github.com/opencybersecurityalliance/kestrel-lang)