

OCA to OpenC2 Mapping

OCA to OpenC2 – C4 Diagram

OCA Action	OpenC2 Mapping (Action/Target)
Quarantine	Contain File, Contain device
Block File	Deny Process, Deny File
Block URL	Deny URL
Query Device	Query Device
Open Incident Response Case	SIEM or Threat Intelligence to SOAR

OCA to OpenC2 – Use Case Mappings

OCA Action	OpenC2 Mapping
Endpoint Protection Software (EPSW) – update signatures	Update File
EPSW checks for new network blocks	Query Files
EPSW scans file	Scan Files
EPSW sends alert to logging tools	
EPSW receives Quarantine file request	Contain File
EPSW polls TIP for updated malicious hash list	Update File

OpenC2 EDR Actuator Profile

Type: Action (Enumerated)

ID	Name	Description
3	query	Query the EDR actuator for a list of available features.
6	deny	Deny a process or service from being executed on the endpoint.
7	contain	Isolate a device from communicating with other devices on a network, quarantine a file.
8	allow	Un-isolate a previously isolated device.
9	start	Initiate a process, application, system, or activity.
10	stop	Halt a system or end an activity.
11	restart	Restart a device, system, or process.
15	set	Change a value, configuration, or state of a managed entity (e.g., registry value, account).
16	update	Instructs the Actuator to retrieve, install, process, and operate in accordance with a software update, reconfiguration, or other update.
19	create	Add a new entity of a known type (e.g., registry entry, file).
20	delete	Remove an entity (e.g., registry entry, file).

EDR Command/Target Matrix

OCA

Table 2.3-1. Command Matrix

	query	deny	contain	allow	start	stop	restart	set	update	create	delete
device			valid	valid		valid	valid				
features	valid										
file		valid	valid	valid	valid				valid		valid
ipv4_net		valid		valid				valid			
ipv6_net		valid		valid				valid			
process					valid	valid	valid				
registry_entry								valid		valid	valid
account								valid			
service						valid					valid

Missing:

- Query Device
- Block URL
- Scan Files

OCA to OpenC2 – Use Case Mappings

OCA Action	OpenC2 Mapping
TIP gathers updates (threats)	QUERY or REST API
Email filtering deny list update (threats)	DENY
New blocking policy pushed out by operations	Update
Security operations invokes new server scan	SCAN
Vulnerability service scans new server VM	SCAN

OCA to OpenC2 – C4 Diagram - PACE

OCA Action	OpenC2 Mapping (Action/Target)
Publish Collection Results	(Endpoint, Malware protect for Email, Malware protect for Endpoint to Posture Collection)
Perform Posture Attribute Collection	Query (Posture Collection System to Endpoint, Malware protect for Email, Malware protect for Endpoint)
Orchestrate Posture Assessment	SOAR to Posture Collection System
Orchestrate Posture Collection	Query (posture attributes) SOAR to Posture Assessment System
Assess Endpoint Posture	Query (SIEM or SOAR to Posture Collection System)
Collect Posture Attributes Action	Query (SIEM or SOAR to Posture Collection System)

SACM Architecture

