#	From	To	OCA Activity	Actuator	OC2 Command	OC2 Response	OC2 Notification	Notes
1	SIEM, SOAR	Malware Protect Scanner, Workstation/Endpoint	Quarantine Device	edr	contain device	status		Can isolate device and process, deny (prevent process from executing), allow.
2	SIEM, SOAR	Malware Protect Scanner, Workstation/Endpoint	Block File	av	deny file, deny email_addr	status		No commands defined yet in AV profile, should be called Intrusion Prevention
3	SOAR	PCS	Initiate Posture Collection	pac	query collection parameters	status / results	status / results	Asynchronous option, attributes posted or returned to requestor
4	SOAR	PAS	Initiate Posture Assessment	paa	asses/evaluate? policy and attributes	status / results	status / results	New OpenC2 action needed? Is result a decision or complex value?
5	SIEM, SOAR	Malware Protect Scanner, Workstation/Endpoint	Blacklist URL	pf, firewall?	deny url	status		What mechanisms besides traffic blocking are used by actuator?
6	any	any	Query Device					query what?
7	SIEM, SOAR	PCS	Collect Posture Attributes Action					Same as 3
8	Endpoint, Malware Protect	PCS	Publish Collection Results					Part of 3
9	PCS	Endpoint, Malware Protect	Perform Posture Attribute Collection					Same as 3 - PCS can be an agent on endpoint or a separate endpoint management system?
10	SIEM, SOAR	PAS	Assess Endpoint Posture					Same as 4?
11	SIEM, TIP	SOAR	Open Incident Response Case					Maybe define a ticketing actuator?