OCA to OpenC2 Mapping

OCA to OpenC2 – C4 Diagram

OCA Action	OpenC2 Mapping (Action/Target)
Quarantine	Contain
Block File	Deny
Orchestrate Posture Assessment	
Orchestrate Posture Collection	Query (posture attributes)
Blacklist URL	Deny
Query Device	Query
Collect Posture Attributes Action	Query

OCA to OpenC2 – Use Case Mappings

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

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