OCA White Paper (Proposed Outline)

Objectives of the OCA

Develop and promote sets of common code, tooling, patterns and practices for sharing data among cybersecurity tools

Vendors who make use of these artifacts will be able to seamlessly interoperate with other vendors

Our approach for collaboration – Overview

OCA focus is on data interchange over a common standardized message bus (commands, responses, data exchange)

Leverage existing open projects and standards (ex STIX, OpenC2)

Develop and initiate OCA projects to develop working code and prototypes to demonstrate interoperability across security technologies

Discuss emerging security topics and issues (ex. Indicators of Behavior, Zero Trust)

Overview of OCA projects

STIXShifter – normalizes data across security tools

Kestrel – threat hunting

PACE – posture attribute collection and evaluation – automate collection and evaluation of security posture attributes from computing resources

OCA Ontology – create a unified ontology for cybersecurity information; enables automation

Overview of the OCA workgroups

Architecture – enable a collaborative approach across security products and tools

Indicators of Behavior – focused on how to collaborate across products that provide behavioral analysis

Zero Trust – enable a Zero Trust architecture

Where you can learn more

OCA Web Site

OCA project GitHubs

OCA Your tube channel

How to get involved

OCA mailing lists

OCA SLACK channels

Applicable audiences

Developers – use and extend OCA common code, tools and practices; participate In OCA projects and/or workgroups

Technology companies – join OCA and promote and extend OCA approach to open collaborative security, provide OCA directions and approaches via seat at our Program Governance Board

Integrators – ensure OCA benefits are realized (simplification, more effective security via collaborative solutions, reduced costs) by active participation in OCA projects and workgroups.

End users (technical, business, Cxo) – drive requirements to OCA and validate OCA project via participation in OCA projects and workgroups