SPECIAL THANK YOU TO
OUR BREAKFAST SPONSOR

Open Cybersecurity Alliance

Join Us!

Quick Intro

Mark serves as co-chair of the OCA Project Governing Board.

Mark is co-founder and CPRO of Tenzir, a startup empowering defenders to build sustainable SOC architectures on open core software.

https://www.linkedin.com/in/markmastrangeli/

OPEN CYBERSECURITY ALLIANCE

TENZIR

Our community

Who

Global like-minded cybersecurity vendors, end users, thought leaders & individuals

Vision

An open ecosystem of interoperable security solutions. 1 App, 1 Integration per ”thing”

How

Open-source developed code & tooling
Mutually agreed upon technologies, standards & procedures

Each sponsor gets an equal vote in strategy & direction of the organization

Sponsorship is not required to participate. Anyone can contribute to the projects.

Part of OASIS OPEN PROJECTS


OPEN
CYBERSECURITY
ALLIANCE


CIS
Center for
Internet Security


COPADO


cybereason


CYDARM


CYWARE

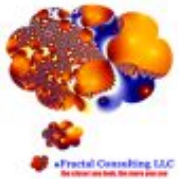

EclecticIQ
Intelligence
at the core


IBM Security


f5


Trellix


Prophecy




SafeBreach


RAPID7


SAIC


tenable


TENZIR


THREATQUOTIENT


VISUA


vmware

Key Initiatives

OPEN CYBERSECURITY ALLIANCE

STIX Shifter

- Cybersecurity toolchain for unified query and response using the STIX 2.x Standards
- Goal: one query language and response data model for all data sources
- 29 Data sources supported (to date)
- Sponsored by IBM

NEW!

Kestrel Threat Hunting Language

- Builds on STIX Shifter to create a unified threat hunting language and tool that works across all supported data sources
- "Out of box" ML & Analytics, integrations with Jupyter Notebooks for GUI
- Sponsored by IBM

NEW!

PACE – Posture Attribute Collection & Enumeration

- Bring posture collection standards up to date with the cloud era
- Instantiation of the IETF SACM working group's architecture w/SCAPv2
- Sponsored by CIS, NSA

Indicators of Behavior Sharing (Workgroup)

- Focused on the challenge of moving detections to Indicators of Behavior
- How to collaborate on, share IoB based detections between products and tools
- Chaired by Cybereason, JHU-APL, IBM

OCA Ontology (Workgroup)

- Creating a unified ontology for cybersecurity information in order to have standard ways of encoding information on data fabrics, APIs, etc
- Originally "Open DXL Ontology", evolved to be fabric agnostic
- Chaired by SAIC, NIST, Tenzir

NEW!

Zero Trust Architecture (Workgroup)

Working to create and further refine OCA technologies to enable a Zero Trust architecture

Continues work which sought to create a unified reference architecture for all aspects of enterprise cybersecurity operations

Chaired by IBM, NIST, VMWare, others

Recent Momentum

OPEN CYBERSECURITY ALLIANCE

- 5 new sponsors join (VMWare, Tenable, Prophecy, VISUA, Tenzir)
- 17 different media publications
- 23 YouTube videos
- 186 Forks of “stix-shifter” project, from at least 6 organizations
- 30+ unique connectors in stix-shifter
- 2 new major projects (Kestrel, PACE) and a new working group (Zero Trust)
- Washington DC Automation Workshop – 70+ attendees focused on Kestrel, PACE, SBOM

Get Involved!

Everyone is welcome to participate.

- Individuals can make technical contributions to OCA Repositories via **GitHub**.
- Organizations can become sponsors, which includes a seat on the **Project Governance Board**.

Contact **communications@oasis-open.org** for more information
Join our **Slack Channel** to track ongoing discussions
Visit the website **Opencybersecurityalliance.org**

Thank you! Questions?

Join our communities and engage with us!

OCA Slack

http://slack.tenzir.com

Thank you for joining us today and thank you to CIS for hosting our breakfast!