Open Cybersecurity Alliance Unveils First Open Source Language to Connect Security Tools

- OpenDXL Ontology enables automatic integration and communication between disparate security technologies via open source standard and code
- Leaders from AT&T, IBM, McAfee, Packet Clearinghouse, Tripwire join OCA?s Technical Steering Committee

February 24, 2020, San Francisco, CA ? The Open Cybersecurity Alliance (OCA) today announced the availability of OpenDXL Ontology, the first open source language for connecting cybersecurity tools through a common messaging framework. With open source code freely available to the security community, OpenDXL Ontology enables any tool to automatically gain the ability to communicate and interoperate with all other technologies using this language. By eliminating the need for custom integrations between individual products, this release marks a major milestone in the OCA?s mission to drive greater interoperability across the security industry.

The newly formed Open Cybersecurity Alliance was launched in October 2019 to connect the fragmented cybersecurity landscape with common, open source code and practices that allow companies to ?integrate once, reuse everywhere.? Governed under the auspices of OASIS [1], the OCA now includes more than 25 member organizations [2] and has brought two major interoperability projects into the open-source realm, with OpenDXL Ontology [3] (contributed by McAfee) and STIX Shifter [4] (contributed by IBM Security) now available for cross-industry collaboration and development on GitHub.

In addition to the availability of OpenDXL Ontology, the OCA is also announcing the formation of its Technical Steering Committee [5], including leaders from AT&T, IBM Security, McAfee, Packet Clearinghouse, and Tripwire, who will drive the technical direction and development of the organization.

?With the adoption of public cloud and explosion of connected devices, the ability for enterprises to quickly respond to threats across ever-changing technologies, and even beyond perimeters, is critical,? says Brian Rexroad, Vice President of Security Platforms at AT&T. ?OCA is driving an industrial shift in interoperability with the OpenDXL Ontology to support security at scale.?

Open Source Language Schema to Connect Security Tools
The Open Data Exchange Layer (OpenDXL) is an open messaging framework that over 4,100 vendors and enterprises already utilize to develop and share integrations with other tools. The release of the OpenDXL Ontology now offers a single, common language for these notifications, information and actions across security products that any vendor can adopt in order to communicate in a standard way with all other tools under this umbrella. This provides companies with a set of tooling that can be applied once and automatically reused everywhere across all product categories, while also eliminating the need to update integrations as product versions and functionalities change.

For example, if a certain tool detects a compromised device, it could automatically notify all other tools and even quarantine that device using a standard message format readable by all. While previously this was only possible with custom integrations between individual products, it will now be automatically enabled between all tools that adopt OpenDXL Ontology. Through continued development by the community, this common language will facilitate a wide variety of interoperability use cases, from sharing threat intelligence to triggering remediation between tools, such as isolating a device or updating a policy.

The adoption of OpenDXL Ontology will help create a stronger, united front to defend and protect across all types of security tools, while reducing the burden of point integrations between individual products.

OCA Momentum: 25+ Organizations Join Forces for Open Security

Since launching five months ago, the OCA has expanded to include more than 25 partner organizations, with the following new members joining: Armis, Center for Internet Security, CyberNB [6], Cydarm [7], Gigamon, Raytheon [8], Recorded Future [9], sFractal Consulting, and Tripwire. The full list of members can be found here [2].

The OCA community is currently collaborating on GitHub and Slack to further new open-source code and use-cases for cybersecurity industry interoperability. In addition to the development of OpenDXL Ontology for a common, open-source language between tools, the OCA is also continuing to build out capabilities for STIX-Shifter [4], a universal, out-of-the-box search capability for security products of all types. Since bringing STIX Shifter to the open-source community, hundreds of visitors have accessed this technology on GitHub, with dozens of users initiating new project forks for development on top of the primary STIX Shifter code.

The OCA will continue development for both STIX Shifter and OpenDXL Ontology, and is actively seeking additional contributors from across the security industry to help guide and drive innovative new use cases for these open source projects.

Visit https://opencybersecurityalliance.org [10] to learn more about the Open Security Alliance and get involved in the projects that are currently underway.

About the Open Cybersecurity Alliance

The Open Cybersecurity Alliance (OCA) brings together vendors and end users to create an open cybersecurity ecosystem where products can freely exchange information, insights, analytics, and orchestrated response. OCA supports commonly developed code and tooling and the use of mutually agreed upon technologies, data standards, and procedures. The OCA is governed under the auspices of OASIS, which offers projects a path to standardization and de jure approval for reference in international policy and procurement.

Media Contact:

Cathy Morley Foster
cathy.morleyfoster@gmail.com [12]
(925) 708-7893

Carol Geyer
Chief Development Officer
Open Source and Standards Communities
OASIS [1]
carol.geyer@oasis-open.org [13]
(941) 284-0403

Links:
[1] https://www.oasis-open.org/
[5] https://opencybersecurityalliance.org/about/
[10] https://opencybersecurityalliance.org
[12] mailto:cathy.morleyfoster@gmail.com
[13] mailto:carol.geyer@oasis-open.org