Published on *OASIS* (https://www.oasis-open.org)

Call for Participation: Open Cybersecurity Alliance

Submitted by censign on Tue, 2019-10-08 15:42
Type:
Call for Participation

A new OASIS Open Project is launching. The Open Cybersecurity Alliance [1] has been organized by the Sponsors listed in the charter below, which also explains its planned purpose, intended benefits, and scope of activity. This is an open invitation to take part in this initiative.

Anyone, whether OASIS member or not, is welcome to contribute to the work of the OCA. Comments, bug reports, or suggestions can be made by opening a GitHub issue or submitting email to the project's general mailing list [2]. Contributions of substantive material such as code or documentation will require signing of the project's Contributor License Agreement before pull requests can be approved.

If you wish to be actively involved in supporting and governing the direction of the project, you may join it as a Sponsor. To become a Sponsor, you pay the sponsor fee applicable for your organization [3] and, optionally, nominate the person to be your representative on the Project Governing Board (PGB).

For more information on the Open Cybersecurity Alliance, see the project website [4] and its GitHub organization [5]. For more information on OASIS Open Projects, see the website [6].

----?
[1] https://opencybersecurityalliance.org/ [1]

[2] https://lists.oasis-open-projects.org/g/oca [2]
To subscribe to this mailing list, send an empty email message to oca+subscribe@lists.oasis-open-projects.org.

[3] http://oasis-open-projects.org/sponsorship/ [3]

[4] https://opencybersecurityalliance.org/ [1]

[5] https://github.com/opencybersecurityalliance/ [4]

[6] http://oasis-open-projects.org/ [5]

Open Cybersecurity Alliance Project Charter

_____

1. Project Name

1.1 Full Name

Open Cybersecurity Alliance (OCA) Open Project

1.2 Familiar Name

opencybersecurityalliance

2. Abstract

The Open Cybersecurity Alliance Project is comprised of global like-minded cybersecurity vendors, end users, thought leaders and individuals who are interested in fostering an open cybersecurity ecosystem, where products from all vendors and software publishers can freely exchange information, insights, analytics, and orchestrated response, via commonly developed code and tooling, using mutually agreed upon technologies, data standards, and procedures.

3. Purpose and Scope

The cybersecurity industry has an ever-growing number of vendors and products, resulting in the fact that enterprise cybersecurity teams are on average using 25 to 49 different security tools from up to 10 different vendors, each of which generate an explosion of data & insights. (ESG 2019) The value of integrating security tools cannot be disputed with the top five benefits being streamlined security management, consolidated vendors & policy management, data exchange, and workflow automation (IDC 2019.) While these tools routinely have integrations amongst one another, there is a lack of industry-wide vendor cooperation on protocols and standards surrounding sharing cybersecurity insight and findings data. As a result, these integrations are often one-off, vendor-specific, expensive to maintain and often lacking the ability to share all available data related to the findings, insights, or incidents. Users of these security products are therefore often unable to break down their data silos and extract peak value from their investments. Vendors find themselves torn on where to invest their finite resources when it comes to integrating with partners. The result is incomplete options for end users regarding which technologies can interoperate within their environment.

The purpose of the OCA project is to develop and promote sets of common code, tooling, patterns, and practices for sharing data among cybersecurity tools. Vendors who make use of these code, tooling, and patterns, will be able to seamlessly interoperate with any other vendors who are making use of OCA project deliverables. Integrate once, reuse everywhere.

The focus of the OCA project is data interchange over a common, standardized messaging bus within cybersecurity operations over the threat management lifecycle, including threat hunting and detection, analytics, operations, and response. Projects will often utilize and/or interoperate with complementary standards such as STIX and OpenC2. OpenDXL will be utilized to facilitate data interchange and STIX Shifter will be used to federate data. Formats enabled via OCA project deliverables, may evolve into OASIS Standards, depending on the wishes of the OCA community.

The OCA project considers out of scope at this time the initial creation and curation of threat intelligence for sharing purposes (for example, threat intelligence platforms), as projects in these domains are more aligned with other initiatives at OASIS.

4. Business Benefits

End user organizations have consistently wanted to be able to integrate ?best-of-breed? products and solutions

into their operational environments with minimal effort and time. However, they have been unable to because of the lack of real interoperability at the communications and data levels. For end users, the inability to properly optimize and extract value from existing toolchains, often leads to attempts to re-solve problems that have been already solved in other cyber domains - simply because clients do not realize a solution already exists due to failure to interoperate and extract that value.

This can lead to the unnecessary procurement of new tools to replace functions that already exist in current tools but are being under-utilized ? exponentially exasperating the problem of too many non-integrated tools in their environments. Further, poor integration can also lead to missing critical insights and findings that would have otherwise been detected if the tools were more well-integrated. A second benefit to end users is reduction of vendor lock-in, as more tools in the cybersecurity operations ecosystem implement their integrations using OCA tooling and standards. The choice of which tools to integrate can now be placed in the hands of the end user rather than waiting for vendors to strike agreements with one another.

For vendors, the ability to integrate cybersecurity products with multiple vendors using one common set of communication capabilities and tooling will greatly reduce the expense of engineering resources spent on integration. Easy integration also mitigates the problem of having to be too selective and narrow in focus when it comes to choosing which vendor technologies to integrate with. Resources previously spent on integrations can then be re-deployed to other parts of the product pipeline, enabling higher value functionality to be developed in the products.

5. Relationship to Other Projects

This project is related to the following other efforts:

* OpenDXL ? OCA will make use of OpenDXL as the foundational transport layer that allows message interchange using its standard messaging bus, working with formatted messages from the OCA project (this document). OpenDXL is the layer that will be used to share these messages between participating technologies. OpenDXL is an open source project created to allow adaptive systems of interconnected services to communicate and share information for real-time, accurate security decisions and actions. More information is available at opendxl.com

* OpenC2 - The OCA project may make use of the OpenC2 standard, to communicate with endpoint devices for automated remediation activities. More information is available at openc2.org

* STIX - The OCA project will make usage of the STIX 2 Cyber Observable model as a representation of cybersecurity data. It will also use STIX 2 format for any consumption or federation of cyber threat intelligence for operations purposes. Other use cases involving STIX 2 and TAXII 2 may also be implemented in projects in the future. More information is available at oasis-open.github.io/cti-documentation/

6. Repositories and Licenses

The initial contributions to this open project will be as follows:

* STIX Shifter is a project centered on open and interoperable threat hunting and analytics, using the STIX 2 Cyber Observable Model as a base. takes in STIX 2 Patterns as input, and "finds" data that matches the patterns inside various products that house repositories of cybersecurity data. Examples of such products include SIEM systems, endpoint management systems, threat intelligence platforms, orchestration platforms, network control points, data lakes, and more. In addition to "finding" the data by using these patterns, STIX-Shifter uniquely also transforms the output into STIX 2 Observations so that all of the security data, regardless of the source, mostly looks and behaves the same. This is critical because the cleansing and normalizing of the data across

domains is one of the largest hurdles to overcome with attempting to build cross-platform security analytics. STIX Shifter is offered under an Apache 2.0 License.

* OpenDXL Standard Ontology is a project focused on the development of an open and interoperable cybersecurity messaging format for use with the OpenDXL messaging bus. The ontology consists of a categorized set of messages that are used to perform actions on one or more cybersecurity products as well as notifications used to signal when significant security-related events occur. The ontology attempts to incorporate other common and open standards for message content (OpenC2, STIX, etc.). In addition to the ontology (messaging catalog), this project also includes sample code that demonstrates how to integrate the ontology into existing security products and related solutions. The OpenDXL Standard Ontology will be offered under the Apache 2.0 license.

7. Initial Contributions from Existing Work

https://github.com/IBM/stix-shifter [6]

8. Project Leadership

8.1 Project Governing Board

* Jason Keirstead (IBM) - Jason.Keirstead@ca.ibm.com [7]
* Darren Thomas (McAfee) - Darren_Thomas@McAfee.com [8]
* Carolyn Raab (Corsa Security) - carolyn.raab@corsa.com [9]
* John Moran (DFLabs) - john.moran@dflabs.com [10]
* Patrick Duggan (New Context) - patrick.duggan@newcontext.com [11]
* Adam Bosnian (CyberArk) - Adam.Bosnian@cyberark.com [12]
* JP Bourget (Syncurity) - jp@syncurity.net [13]

Pending members proposed by project sponsor companies

* Yariv Lenchner (Indegy) - yariv@indegy.com [14]
* Jon Warren (ThreatQuotient) - Jon.Warren@threatq.com [15]
* Craig ?CJ? Brunet (Advanced Cyber Security Corp) - cjb@advancedcybersecurity.com [16]
* Yotam Ezra (SafeBreach) - yotam.benezra@safebreach.com [17]
* Reuven Harrison (Tufin) - reuven.harrison@tufin.com [18]
* Hugh Pyle (ReversingLabs) - hugh.pyle@reversinglabs.com [19]
* Marko Dragoljevic (EclecticIQ) - marko@eclecticiq.com [20]

8.2 Sponsors

The following organizations sponsor the Open Cybersecurity Alliance.

* Advanced Cyber Security Corp - https://www.advancedcybersecurity.com/ [21]
* Corsa Security - https://www.corsa.com/ [22]
* CrowdStrike - https://www.crowdstrike.com/ [23]
* CyberArk - https://www.cyberark.com/ [24]
* Cybereason - https://www.cybereason.com/ [25]
* DFLabs - https://www.dflabs.com/ [26]
* EclecticIQ - https://www.eclecticiq.com/ [27]
* Electric Power Research Institute (EPRI) - https://www.epri.com/ [28]
* Fortinet - https://www.fortinet.com/ [29]

* IBM Security - www.ibm.com/ [30]
* Indegy - https://www.indegy.com/ [31]
* McAfee - www.mcafee.com/ [32]
* New Context - https://www.newcontext.com/ [33]
* ReversingLabs - https://www.reversinglabs.com/ [34]
* SafeBreach - https://safebreach.com/ [35]
* Syncurity - https://www.syncurity.net/ [36]
* ThreatQuotient - https://www.threatq.com/ [37]
* Tufin - www.tufin.com/ [38]

8.3 Other Contributors (Optional)

The following participants have indicated their intention to be active contributors to the project:

* Chris Smith (McAfee) - Christopher_Smith@McAfee.com
* Don Hanson (McAfee) - Don_Hanson@McAfee.com [39]
* Thierry Supplisson (IBM) - thierry.supplisson@ie.ibm.com [40]
* Ian Murphy (IBM) - Ian.Murphy@ibm.com [41] +
* Kent Landfield (McAfee) - kent_landfield@mcafee.com [42]
* Bill Woodcock (Packet Clearing House) - woody@pch.net [43]
* John Todd (Quad9) - jtodd@quad9.net [44]

Deadline:
Tue, 2019-10-08 - Fri, 2019-11-08

Links:
[1] https://opencybersecurityalliance.org/
[2] https://lists.oasis-open-projects.org/g/oca
[3] http://oasis-open-projects.org/sponsorship/
[4] https://github.com/opencybersecurityalliance/
[5] http://oasis-open-projects.org/
[6] https://github.com/IBM/stix-shifter
[7] mailto:Jason.Keirstead@ca.ibm.com
[8] mailto:Darren_Thomas@McAfee.com
[9] mailto:carolyn.raab@corsa.com
[10] mailto:john.moran@dflabs.com
[11] mailto:patrick.duggan@newcontext.com
[12] mailto:Adam.Bosnian@cyberark.com
[13] mailto:jp@syncurity.net
[14] mailto:yariv@indegy.com
[15] mailto:Jon.Warren@threatq.com
[16] mailto:cjb@advancedcybersecurity.com
[17] mailto:yotam.benezra@safebreach.com
[18] mailto:reuven.harrison@tufin.com
[19] mailto:hugh.pyle@reversinglabs.com
[20] mailto:marko@eclecticiq.com
[21] https://www.advancedcybersecurity.com/
[22] https://www.corsa.com/
[23] https://www.crowdstrike.com/

[24] https://www.cyberark.com/
[25] https://www.cybereason.com/
[26] https://www.dflabs.com/
[27] https://www.eclecticiq.com/
[28] https://www.epri.com/
[29] https://www.fortinet.com/
[30] http://www.ibm.com/
[31] https://www.indegy.com/
[32] http://www.mcafee.com/
[33] https://www.newcontext.com/
[34] https://www.reversinglabs.com/
[35] https://safebreach.com/
[36] https://www.syncurity.net/
[37] https://www.threatq.com/
[38] http://www.tufin.com/
[39] mailto:Don_Hanson@McAfee.com
[40] mailto:thierry.supplisson@ie.ibm.com
[41] mailto:Ian.Murphy@ibm.com
[42] mailto:kent_landfield@mcafee.com
[43] mailto:woody@pch.net
[44] mailto:jtodd@quad9.net