Cybersecurity Leaders Launch Initiative for Interoperable Security Technologies to Thwart Attacks

Open Cybersecurity Alliance to connect the fragmented cybersecurity landscape with common, open source code and practices. IBM Security and McAfee join with Advanced Cyber Security Corp, Corsa, CrowdStrike, CyberArk, Cybereason, DFLabs, EclecticIQ, Electric Power Research Institute, Fortinet, Indegy, New Context, ReversingLabs, SafeBreach, Syncurity, ThreatQuotient, and Tufin to collaborate on new initiative at OASIS

Borderless Cyber, WASHINGTON, D.C., October 8, 2019. Today, the OASIS international consortium announced an industry initiative to bring interoperability and data sharing across cybersecurity products. With initial open source content and code contributed by IBM Security and McAfee, and formed under the auspices of OASIS, the Open Cybersecurity Alliance [1] (OCA) brings together organizations and individuals from around the world to develop open source security technologies which can freely exchange information, insights, analytics, and orchestrated responses.

According to industry analyst firm, Enterprise Strategy Group, organizations use 25 to 49 different security tools from up to 10 vendors on average, each of which generates siloed data. (Cybersecurity Landscape: The Evolution of Enterprise-class Vendors [2]).

Connecting these tools and data requires complex integrations, taking away from time that could be spent hunting and responding to threats. To accelerate and optimize security for enterprise users, the OCA will develop protocols and standards which enable tools to work together and share information across vendors. The aim is to simplify the integration of security technologies across the threat lifecycle – from threat hunting and detection, to analytics, operations and response -- so that products can work together out of the box.

The purpose of the OCA is to develop and promote sets of open source common content, code, tooling, patterns, and practices for interoperability and sharing data among cybersecurity tools. For enterprise users, this means:

- Improving security visibility and ability to discover new insights and findings that might otherwise have been missed;
- Extracting more value from existing products and reducing vendor lock-in;
- Connecting data and sharing insights across products.

Founders of the Alliance, IBM Security and McAfee, are joined in the initiative by Advanced Cyber Security Corp, Corsa, CrowdStrike, CyberArk, Cybereason, DFLabs, EclecticIQ, Electric Power Research Institute, Fortinet, Indegy, New Context, ReversingLabs, SafeBreach, Syncurity, ThreatQuotient, and Tufin. The OCA welcomes participation from additional organizations and individual contributors.

"Today, organizations struggle without a standard language when sharing data between products and tools," said
Carol Geyer, chief development officer of OASIS. "We have seen efforts emerge to foster data exchange, but what has been missing is the ability for each tool to transmit and receive these messages in a standardized format, resulting in more expensive and time-consuming integration costs. The aim of the OCA is to accelerate the open sharing concept making it easier for enterprises to manage and operate."

"When security teams are constantly spending their time manually integrating tools and maintaining those integrations, it’s not helping anyone other than the attackers," said Jason Keirstead, chief architect, IBM Security Threat Management. "The mission of the OCA is to create a unified security ecosystem, where businesses no longer have to build one-off manual integrations between every product, but instead can build one integration to work across all, based on a commonly accepted set of standards and code."

"Attackers maximize damage by sharing data with one another. Our best defense strategy is to share data too," said D.J. Long, vice president business development, McAfee. "The OCA creed is 'Integrate once, reuse everywhere' which builds upon McAfee’s open philosophy that led to the OpenDXL project in 2016. Organizations will be able to seamlessly exchange data between products and tools from any provider that adopts the OCA project deliverables. We’re looking at the potential for unprecedented real-time security intelligence."

Initial technology contributions to the open project are as follows, with additions expected as part of ongoing work:

**STIX-Shifter** [3] (from IBM Security): This project aims to create a universal, out-of-the-box search capability for security products of all types, by providing a way to connect security products to other security, cloud, and software data repositories via a standardized cybersecurity data model (STIX 2). STIX-Shifter is an open source library which can identify information about potential threats within a wide variety of data repositories and translate it into a format that can be digested and analyzed by any security tool that has this standard enabled.

**OpenDXL Standard Ontology** [4] (from McAfee) focused on the development of an open and interoperable cybersecurity messaging format for use with the OpenDXL messaging bus. The OpenDXL Standard Ontology will be offered under the Apache 2.0 license.

**Open Cybersecurity Alliance Sponsors**

"Every digital device is a potential vulnerability point. Advanced Cyber Security Corp. is proud to be an initial sponsor of the OCA and is committed to this collaborative effort to promote the use of common code, tooling, and standards for endpoint security and to help industry professionals and government agencies advance in cyber security awareness and preparedness."

*C.J. Brunet, president and COO - Advanced Cyber Security Corp.*

"Cybersecurity systems will be strongest and most able to effectively adapt and respond to changing threats when communication and connectivity within the ecosystem is open. Corsa Security is part of OCA to create such an open environment and build towards highly effective cyber systems."

*Carolyn Raab, chief product officer - Corsa Security*

?At CrowdStrike, the power of crowdsourced data critically informs our customers with actionable insights to help defeat sophisticated adversaries, ensuring organizations stay ahead of future threats. Our participation in the OCA will facilitate strategic information sharing for more visibility into cybercriminal patterns, motivations, and behaviors. Aligning with our partners like IBM to foster better integration and alert exchange will help stop breaches before they occur."

*Mathew Polly, vice president of worldwide alliances, channels and business development - CrowdStrike*

"CyberArk strongly believes in the power of vendor collaboration to strengthen the enterprise security fabric. We continue to support open source initiatives that elevate that level of collaboration, and being part of the
Vendor community actively engaged in the Open Cybersecurity Alliance (OCA) is another important step forward. By creating a framework to share data that improves communication and effectiveness among an ecosystem of software solutions, OCA is helping to enrich and improve the effectiveness of security solutions, while enabling organizations to increase adoption to better defend against cyberattacks.

Adam Bosnian, executive vice president, global business development - CyberArk

"Focus on tools detracts from the task at hand: doing security. It's our job to make our tools and the seams among them more and more transparent. Going deeper than check box integration and finding ways to move up the stack is the goal of the OCA. We have to develop a new generation of protocols and interoperability that put the end user and the process of security front and center. If we do that, we'll not only remove waste but can provide every advantage to defender in cyber conflict."

Sam Curry, chief security officer - Cybereason

"As an automation and orchestration vendor, DFLabs is keenly aware of the importance of open standards in efficiently and effectively sharing information and working collaboratively with different technologies throughout the security stack. DFLabs is proud to be a part of shaping the standards which will move the security industry towards enhanced information sharing and interoperability through the OCA."

Michele Zambelli, CTO - DFLabs

"Fortinet is focused on integrating and collaborating with industry?s top technology vendors to provide end-to-end security through our Fabric-Ready Partner Program. We?re pleased to advance this commitment by joining the OCA?s industry-wide initiative focused on data sharing and interoperability across cybersecurity products. Alongside our Fabric-Ready Partners IBM Security and McAfee, as well as other vendors, we look forward to developing open code, standards and tooling that can help solve some of the industry?s biggest challenges."

John Maddison, executive vice president of products and CMO - Fortinet

"With IT (information technology) and OT (operational technology) systems converging, sharing security information is essential for detecting and remediating threats. As a global leader in Industrial Cybersecurity and a member of the OCA, we are all working together to ensure customers can seamlessly integrate intelligence from OT and IT to protect their industrial operations. We?re proud to extend full visibility, security and control of OT environments to this important partnership."

Mille Gandelsman, CTO and co-founder - Indegy

"New Context is proud to be a founding member of the Open Cybersecurity Alliance. We look forward to working with our fellow OCA members to develop and promote open source resources and best practices to support the cybersecurity community."

Patrick Duggan, chief of staff - New Context

"At ReversingLabs, we are committed to providing complete visibility and insight into every destructive object?unwanted, vulnerable and malware-infected destructive files, emails, attachments, binaries, and third-party and open source code?by integrating and optimizing existing enterprise security investments. With the establishment of the Open Cybersecurity Alliance (OCA) we can now more easily extend those integrations through open source content and code to amplify line of sight into hidden objects and deliver the breadth and depth of visibility enterprise organizations need to seek out and remediate the most dangerous and complex threats."

Mario Vuksan, CEO and co-founder - ReversingLabs
"SafeBreach, a leader in breach and attack simulation, was built on the mission to extend cybersecurity awareness and measure cybersecurity controls throughout every organization. To join this consortium of like-minded vendors is a testament to the commitment and innovation that we all see necessary to drive cybersecurity excellence in the community through information sharing and intelligence."

Itzik Kotler, CTO and co-founder - SafeBreach

"At ThreatQuotient we are interested in fostering an open cybersecurity ecosystem where products can freely exchange information to help defenders protect their environments. We are also proud to support protocols and standards to simplify the exchange of information from several different vendors and technologies. With this in mind, we are happy to be a part of the OCA to support the initiative and work with other stakeholders."

Haig Colter, director, Alliances - ThreatQuotient

"Fostering an open exchange of information among vendors, end users, thought leaders, and individuals is more crucial than ever in today’s cybersecurity ecosystem. We are excited to be part of the important work that the OCA is doing to bring our community together to help drive mutually agreed upon technologies, procedures, and security standards."

Pamela Cyr, senior vice president business development - Tufin Technologies

To learn more visit www.opencybersecurityalliance.org.

About OASIS

One of the most respected, member-driven standards bodies in the world, OASIS offers projects ? including open source projects ? a path to standardization and de jure approval for reference in international policy and procurement. OASIS has a broad technical agenda encompassing cybersecurity, privacy, cryptography, cloud computing and IoT ? any initiative for developing code, APIs, specifications or reference implementations can find a home at OASIS. # # #

Links:
[1] https://opencybersecurityalliance.org/
[3] https://urldefense.proofpoint.com/v2/url?u=https-3A__github.com_IBM_stix-2Dshifter&amp;d=DwMFJg&amp;c=jf_iaSHvJObTbx-siAlZOg&amp;r=_VmY0y9Vkrneh0mnRQsG1E2Qp3y-vg_X0oKDYy32a3Y&amp;m=uVKwwV7ODq1AVdrFlCvT8KL2H7BgGnq1_k5U5h5ZIUApaveIQhKf0.png&amp;s=QIqp5yLBKCEu