Open Cybersecurity Alliance Adds Indicators of Behavior (IoB) Sub-Project

Security Practitioners to Create Standardized Approach for Representing Cyber Threat Actor Behaviors in a Sharable Format

BOSTON, MA, USA, January 17, 2023 /EINPresswire.com/ -- The Open Cybersecurity Alliance (OCA), a global, standards-based initiative to simplify integration across the threat lifecycle, announced today that it has accepted the Indicators of Behavior (IoB) Working Group (WG) as a sub-project. The OCA IoB brings together like-minded stakeholders in the cyber threat intelligence community to collectively focus on patterns of behavior associated with malicious cyber activity. By understanding the behavior patterns, innovative solutions can be developed to enable shared behavior sets, leading to more proactive detection, effective mitigations, and, through timely and actionable sharing, more prevention.

OCA IoB will work to improve detection and response to cyber threats in a broader capacity than what is currently possible with the primary actionable shared data, typically Common Vulnerability Enumerations (CVEs) and Indicators of Compromise (IoCs). While it is critical to ensure CVEs are mitigated and active IoCs are blocked, these actions by their very nature force a reactive posture to an ever-increasing cyber threat. OCA IoB aims to create a standardized approach for representing cyber threat actor behaviors in a shareable format.

“The overarching theme with OCA IoB is to foster collaboration across and between organizations. Machine-readable IoB objects and reference implementation code that can easily integrate representations of adversary behaviors provide rapid detection and response capabilities that can be readily accessible to all organizations,” said Charles Frick, OCA IoB Chair, of the Johns Hopkins Applied Physics Laboratory. “The OCA IoB provides standardization amongst the vendor community who can, in turn, help provide this capability to smaller organizations that may not have the resources for advanced threat hunting teams.”

The OCA IoB will make use of the OASIS STIX™ Version 2.1 standard for representation of IoB

data in machine readable format. It will also use the STIX™ 2.0 format for any consumption or federation of cyber threat intelligence for operations purposes. For objects that may help organizations respond to threat behaviors via automated workflows, the OCA IoB will ensure that shared workflows are compliant with the OASIS Collaborative Automated Course of Action Operations (CACAO) standard as it is developed.

IoB aligns with the project's mission of integrating tools and solutions across security teams. IoB will directly enable vendors and end users to advance OCA's mission of building an open ecosystem where cybersecurity products interoperate without the need for customized integrations. IoB joins the growing body of OCA work including: the Kestrel threat hunting tool, the STIX Shifter patterning library, and the Posture Attribute Collection and Evaluation (PACE) for cybersecurity readiness.

Support for IoB

Canadian Institute for Cybersecurity
"Monitoring Indicators of Behaviors (IoB) presents the best opportunity for organizations to hunt for advanced threats and attacks at an early stage. Automated learning from unexpected and unauthorized modifications to normal operating baseline will empower and shift the focus of an organization from reactive to preventive cybersecurity. The Canadian Institute for Cybersecurity (CIC) is a leader in leveraging AI and contextual data to identify and detect IoB with a low false positive rate."
–Haruna Isah, Research Associate and Talent/Partnership Development Manager, CIC

Cydarm
“Cybersecurity is a team sport, and collective defense is the best way to impose costs on attackers. Threat actors can easily change payloads and infrastructure to evade detection by Indicators of Compromise, but it is much harder for them to change their Tactics, Techniques, and Procedures. As an OCA member and a leader in Cyber Response Management, Cydarm supports the OCA's IoB Sub-Project, toward sharing of tradecraft, to enable better collective defense.”
– Dr. Vaughan Shanks, Co-founder and CEO, Cydarm Technologies

Cyware
"As the threat landscape and attacker sophistication continue to evolve rapidly, collaboration around tracking, monitoring, and aggregating IOCs provides an attractive path forward for more capable, collective defense. Cyware is thrilled to join this OCA initiative designed to define a structure for exchanging IOBs that shorten the window of success for evolving attacker behaviors and methodologies."
- Avkash Kathiriya, VP Research and Innovation, Cyware

IBM Security
“Identifying attackers based on their behavior patterns is one of the most effective ways to

detect advanced threats - but defenders need an easier way to share this information with each other, as attackers are constantly evolving their techniques. By creating open standards for these behavior-based attack indicators, this project will allow more proactive and complete threat detection analytics to be shared in the community, shining a light on previously undiscovered threats."
– Jason Keirstead, CTO, Threat Management, IBM Security

Prophecy International
"We continue to give enthusiastic support to the OCA as it goes hand-in-hand with our mission to improve our customers' cyber posture worldwide and ensure that our products support the growth and evolution of the global cybersecurity community. The mission is to improve trust, interoperability and to create a network of industry leaders committed to working together to solve the hard problems in cyber security, and the OCA is a powerful vehicle to drive towards those goals."
– Brad Thomas, CEO, Prophecy International & OCA Project Governing Board Member

sFractal Consulting
"IoB, along with the OCA sub-projects Kestrel, PACE, and STIX-Shifter, help automate more sophisticated responses to today's complex cyber attacks. Threat actors are increasingly using coordinated, automated attacks that are more frequent, more impactful, and more sophisticated. To successfully defend against these attacks, it is essential for security teams to cooperate and automate their defenses. IoB goes a step further than traditional cooperation because IoB includes information about the behavior of the attackers."
– Duncan Sparrell, Principal, sFractal Consulting

About the Open Cybersecurity Alliance (OCA)
The 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 Open, which offers projects a path to standardization and de jure approval for reference in international policy and procurement.

Media inquiries:
communications@oasis-open.org

Carol Geyer
OASIS
+1 941-284-0403
email us here
Visit us on social media:
LinkedIn
Twitter

Facebook