IBM Contributes Kestrel Threat Hunting Tool to OASIS Open Cybersecurity Alliance (OCA)

Kestrel lets threat hunters 'devote more time to figuring out what to hunt, as opposed to how to hunt'

BOSTON, MA, USA, June 29, 2021 /EINPresswire.com/ -- Open Cybersecurity Alliance (OCA), an OASIS Open Project, today announced it has accepted IBM's contribution of Kestrel, an open-source programming language for threat hunting that is used by Security Operations Center (SOC) analysts and other cybersecurity professionals. Kestrel streamlines cyber reasoning and threat discovery, which can help analysts complete this process more quickly and effectively.

> "Kestrel is about to change the way we approach threat hunting ..."
> *Sheldon Shaw, Vice President, Innovation & Infrastructure at CyberNB*

IBM Research and IBM Security jointly developed Kestrel to enable threat hunters to express hunts in an open, composable threat hunting language. Kestrel leverages automation to execute tedious hunting tasks, allowing threat hunters to focus on higher priority tasks. Its combination of human ingenuity coupled with machine-based automation helps accelerate threat hunting. The composable hunting flows enable the reuse of best practices and helps reduce the time to create new hunts.

Because IBM Security has open-sourced this project, threat hunters across the globe are now able to collaborate, share and use the knowledge curated continuously by threat hunters using Kestrel.

This contribution from IBM marks a major milestone in OCA's mission to drive greater interoperability across the security industry. The work of the OCA connects the fragmented cybersecurity landscape and enables disparate security products to freely exchange information, out of the box, using mutually agreed upon technologies, standards, and procedures that make it possible for companies to "integrate once, reuse everywhere."

"Kestrel is designed to take advantage of the collective learned experience of the threat hunting

community – and enable that to be combined with the power of machine learning and automation to speed response to threats," said Jason Keirstead, CTO of Threat Management for IBM Security and Co-Chair - Open Cybersecurity Alliance. "By sharing new threat hunting patterns as they emerge via code that can be easily customized, Kestrel lets threat hunters devote more time to figuring out what to hunt, as opposed to how to hunt."

"This is a really exciting contribution from IBM, a founding member of the Open Cybersecurity Alliance. Kestrel is a fully open-source threat hunting language that leverages the federated data service capabilities of STIX Shifter which were previously contributed to the OCA by IBM. I cannot wait to see how OCA member organizations and the community of like-minded people, pursuing open interoperability of security solutions, leverage these tools to further enhance their security operations across heterogeneous solutions."
– Mark Mastrangeli, Lead Architect, McAfee, and Co-Chair - Open Cybersecurity Alliance

"The future of cybersecurity automation is in analyst augmentation and platform interoperability. Kestrel embodies both of these traits, enabling SOC analysts to hunt threats at scale using a standardized language. Cydarm is pleased to see this project included as an OCA capability."
– Dr. Vaughan Shanks, CEO, Cydarm Technologies

"We are proud to support the continued refinement of this standard language. It further builds confidence with the threat intelligence community and enables a true collective defense," said Avkash Kathiriya, Vice President of Research and Innovation at Cyware. "As a part of the community, Cyware understands how valuable the standard is, which is just one of the reasons we use it as a backbone for intel sharing and automation."

"It's good to see additional capabilities being built upon STIX. The Kestrel project is a great example of how the community can develop normalised methods, in this case, a threat hunting language, to easily interact with the growing security technology landscape."
– Tyler Oliver, XDR Product Manager at EclecticIQ

"Robust threat hunting is a function of data correlation and contextual analysis. For transforming threat discoveries into actionable threat intelligence at-scale, the organizations need a powerful language to communicate the threat hunting tasks and operations, and we believe that Kestrel is an answer to that."
– Renuka Nadkarni, VP and CTO Security, F5 Inc.

"To meet today's increasing threats requires tools to help defenders share both between people/organizations and between products. OCA helps with vendor-agnostic, machine-speed cyber-defense automation. The new Kestrel project is a welcome addition to that toolset to assist with sharing in threat hunting."
– Duncan Sparrell, Chief Cyber Curmudgeon, sFractal Consulting

"ThreatQuotient is pleased to continue its partnership with the Open Cybersecurity Alliance to help drive standards to encourage interoperability between security vendors to benefit network defenders," said Haig Colter, Director of Alliances. "Our continued participation in the OCA demonstrates our commitment to follow established standards that encourage the communication of security information in ways that benefit a broader audience."

The OCA is led by organizations committed to solving the costly problem of siloed cyber tools and products that create integration nightmares for cybersecurity professionals in every environment. CyberNB, Rapid7, SafeBreach, and Tenable have recently joined the governing board working alongside Center for Internet Security (CIS), Cybereason, Cydarm, Cyware, EclecticIQ, EPRI, F5, IBM Security, McAfee, NewContext, S-Fractal Consulting, SAIC, ThreatQuotient, Tripwire, and TruSTAR.

More Support for OCA

"Kestrel is about to change the way we approach threat hunting, instead of continuously rebuilding our analysis Kestrel allows us to ask what patterns or what behaviours are present during an investigation. Instead of dissecting indicators of compromise, we will be dissecting playbooks of entire hunt logic and across data sources. As adoption of the language continues to roll out, our collective hunt teams will be able to collaborate and approach cyber investigations differently – as a leader in bringing cyber collectives together to solve problems CyberNB welcomes the innovative thinking of IBM Security."
– Sheldon Shaw, Vice President, Innovation & Infrastructure, CyberNB

"For threat hunting, Kestrel fills a critical need of a common language to express data and share insights. Combining Kestrel with predictive data sources will make threat hunting far more powerful and empower security teams to drive down the risks that matter. SafeBreach is excited to be the first predictive data source that will enable querying future threats".
– Valeriy Leykin, Director Product Management at SafeBreach

About the Open Cybersecurity Alliance

The OCA is governed under the auspices of OASIS (https://oasis-open.org), which offers projects a path to standardization and de jure approval for reference in international policy and procurement.

Contact:

Dee Schur
OASIS Open
+1 941-321-6733
email us here
Visit us on social media: