splunk>

PRESS RELEASE

Cybersecurity and Technology Industry Leaders Launch Open-Source Project to Help Organizations Detect and Stop Cyberattacks Faster and More Effectively

Together with 15 companies, Splunk, AWS and Broadcom collaborate on a broad-based effort to integrate security tools and resources and break down data silos

LAS VEGAS, Aug. 10, 2022 – A coalition of cybersecurity and technology leaders announced an open-source effort to break down data silos that impede security teams. The Open Cybersecurity Schema Framework (OCSF) project, revealed today at Black Hat USA 2022, will help organizations detect, investigate and stop cyberattacks faster and more effectively.

The OCSF project was conceived and initiated by AWS and Splunk, building upon the ICD Schema work done at Symantec, a division of Broadcom. The OCSF includes contributions from 15 additional initial members, including Cloudflare, CrowdStrike, DTEX, IBM Security, IronNet, JupiterOne, Okta, Palo Alto Networks, Rapid7, Salesforce, Securonix, Sumo Logic, Tanium, Trend Micro, and Zscaler. Starting today, all members of the cybersecurity community are invited to utilize and contribute to the OCSF.

Detecting and stopping today's cyberattacks requires coordination across cybersecurity tools, but unfortunately normalizing data from multiple sources requires significant time and resources. The OCSF is an open-source effort aimed at delivering a simplified and vendor-agnostic taxonomy to help all security teams realize better, faster data ingestion and analysis without the time-consuming, up-front normalization tasks.

The OCSF is an open standard that can be adopted in any environment, application, or solution provider and fits with existing security standards and processes. As cybersecurity solution providers incorporate OCSF standards into their products, security data normalization will become simpler and less burdensome for security teams. OCSF adoption will enable security teams to increase focus on analyzing data, identifying threats and defending their organizations from cyberattacks.

Member Quotes:

"Security leaders are wrestling with integration gaps across an expanding set of application, service and infrastructure providers, and they need clean, normalized and prioritized data to detect and respond to threats at scale," said Patrick Coughlin, GVP Security Market, Splunk. "This is a problem that the industry needed to come together to solve. That's why Splunk is a proud member of the OCSF community — security is a data problem and we want to help create open standard solutions for all producers and consumers of security data."

"Symantec and Broadcom Software are proud to have contributed our ICD schema as the foundation for the OCSF project. This is another proof-point of how we support open standards across the security industry," said Rob Greer, GM, Symantec Enterprise Division at Broadcom. "The OCSF community will streamline Security Operations for the many thousands of organizations that rely on telemetry from a wide range of sources to power their cybersecurity investigations."

“Having a holistic view of security-related data across tools is essential for customers to effectively detect, investigate, and mitigate security issues. Customers tell us that their security teams are spending too much time and energy normalizing data across different tools rather than being able to focus on analyzing and responding to risks,” said Mark Ryland, Director, Office of the CISO, AWS. “By increasing interoperability between tools, the OCSF aims to greatly accelerate our customers’ ability to understand and respond to cybersecurity concerns. Security is our top priority at AWS, and we are excited to work with the OCSF community to drive industry standards that make it easier for customers to operate more securely.”

"Every business deserves a simple, straightforward way to analyze and understand the security landscape – and that starts with their data," said John Graham-Cumming, CTO at Cloudflare. "By participating in the OCSF, we hope to help the entire security industry focus on doing the work that matters instead of wasting countless hours and resources on formatting data."

"At CrowdStrike, our mission is to stop breaches and power productivity for organizations," said Michael Sentonas, Chief Technology Officer, CrowdStrike. "We believe strongly in the concept of a shared data schema, which enables organizations to understand and digest all data, streamline their security operations and lower risk. As a member of the OCSF, CrowdStrike is committed to doing the hard work to deliver solutions that organizations need to stay ahead of adversaries."

"Modern cybersecurity operations is a team sport, and products must integrate with each other to provide value beyond what a single product can. Sure, it's possible to make that happen with open APIs and mapping data structures, but development and processing resources are not infinite," said Mohan Koo, Co-founder and CTO with DTEX Systems. "The OCSF initiative is about eliminating the inefficiencies and making it possible to achieve frictionless integration through standardized data, meaning faster time to detection, response and resolution at a lower total cost."

“Cybersecurity is one of the most pressing challenges of the 21st century, and no single organization, agency, or vendor can solve it alone,” said Sridhar Muppidi, IBM Fellow, Vice President and Chief Technology Officer, IBM Security. “IBM Security is a long-standing supporter of open-source and open standards, and believes that common data formats like the OCSF will help improve interoperability among many different cybersecurity products, allowing the “power of the crowd” to be used as a force multiplier against increasingly sophisticated adversaries.”

“Collaboration is at the heart of IronNet’s mission, so we are proud to join Splunk and AWS as members of the OCSF. By developing an open standard for cybersecurity data, we can work together to strengthen cyber defenses as a whole,” said General (Ret.) Keith Alexander, co-CEO and founder, IronNet. “As one of the first members of the OCSF, we look forward to growing the framework and sharing relevant insights to enable quicker visibility and a higher level of cyber protection.”

“The OCSF initiative is truly unprecedented,” said Erkang Zheng, CEO and founder, JupiterOne. “Normalizing data prior to ingestion has been one of the biggest pain points for security professionals, and the universal framework proposed by the OCSF, powered by a common domain knowledge across several security vendors, simplifies this time-consuming step, ultimately enabling better and stronger security for all.”

“At Okta, our vision is to enable everyone to safely use any technology. In a world of broad and deep technology adoption, seamless integration and interoperability across applications is critical, especially

in security tooling," said Christopher Niggel, Regional Chief Security Officer for the Americas, Okta. "Coalitions like the OCSF help security teams make every user and organization more secure by streamlining access to data from the entire ecosystem of applications in the business, enabling faster detection and investigation of threats."

"We, as security vendors, need to do right by the security teams who work tirelessly to protect not only their organizations, but the greater community, against a constantly evolving array of threats," said Sam Adams, Vice President of Detection and Response, Rapid7. "A step towards that is standardizing the data on which these teams rely. If we can minimize the complexity of using security data from disparate sources, we can save security professionals millions of hours every year. Rapid7 has a proud history of supporting the open-source community. We are thrilled to join our peers who share this belief and build a solution that will break down data silos, removing a heavy burden that hinders security teams' efforts to stay ahead of threats."

"Adding speed and efficiency to cybersecurity is one of the key challenges of organizations fighting ongoing threat inflation," said Augusto Barros, Vice President Cybersecurity Evangelist, from Securonix. "The OCSF simplifies sharing security data and enables organizations to quickly apply new threat detection analytics and hunt for threats regardless of the source providing the underlying data. This common framework also simplifies the adoption of independent data stores, as organizations pursue a new, non-siloed approach to store and obtain value from their cybersecurity data."

"Companies have long recognized the need to share threat data across and between systems, and the scope of today's threat landscape requires standardization so that critical information can be integrated and shared to support the highest levels of efficiency and protection," said Dave Frampton, VP and GM of Sumo Logic Security Business Unit, Sumo Logic. "Our participation in the OCSF enhances the value of security data for all - to deliver trusted insights to detect, investigate and stop cyber threats."

"As our customers and partners continue to standardize on Tanium's real-time endpoint data, it is important for us to adapt quickly to the everchanging cybersecurity landscape," said Tanium Vice President of Partnerships and Integrations Michael Martins. "By adding support in our platform for the Open Cybersecurity Schema Framework, we are committing to a future where disparate data sources come together to improve the ability to detect, investigate, and thwart cybersecurity attacks."

"Data silos and misalignment add unnecessary risk to businesses and headaches for security teams," said Mike Gibson, Vice President of Global Customer Success and Threat Research at Trend Micro. "The industry needs an open community to break down the silos and minimize risk by making security more manageable. We are proud to join our peers in building this solution so security teams can focus more on intelligence and spend less time worrying about formats."

"As a leader in zero trust, Zscaler is proud to collaborate with partners on the OCSF universal framework to help customers transform IT and Security," said Amit Raikar, VP of Technology Alliances at Zscaler. "Zero trust is a team sport. The framework proposed by the OCSF will help break down barriers leading to improved analytics and detections, resulting in better enforcement policies."

"A critical challenge modern SOC teams face today is normalizing disparate data across their multitude of security tools. By defining an open and extensible standard for security event data, the OCSF simplifies the data normalization required to detect and defend against modern security threats," said

Michelle Abraham, Research Director, Security and Trust, IDC. “Customers who adopt tools implementing the OCSF standard will benefit from less complexity in the building of their data ingestion workflows."

About OCSF
The OCSF is an open-source effort aimed at delivering a simplified and vendor-agnostic taxonomy to help all security teams realize better, faster data ingestion and analysis without the time-consuming up-front normalization tasks. The OCSF project is guided by a steering committee with representatives from AWS and Splunk and jointly managed by a team of maintainers in collaboration with contributors.

For information on how to be a part of the OCSF project, including how to contribute, visit https://github.com/ocsf/.

Über Splunk Inc.
Splunk Inc. (NASDAQ: SPLK) hilft Unternehmen auf der ganzen Welt dabei, Daten in Taten zu verwandeln. Die Splunk-Technologie wurde entwickelt, um Daten jeder Art und Größe zu untersuchen, zu überwachen, zu analysieren und als Basis für konkrete Maßnahmen nutzbar zu machen.

Für weitere Informationen wenden Sie sich bitte an

Medien
Mandy Kuhl
Splunk Inc.
mkuhl@splunk.com

Investoren
Ken Tinsley
Splunk Inc.
ir@splunk.com