Open Cybersecurity Schema Framework

Splunk, AWS and Symantech are the leaders in the new Open Cybersecurity Schema Framework (OCSF) that was revealed last week at BlackHat USA 2022. The Open Cybersecurity Schema Framework is an open-source project, delivering a framework for developing schemas, along with a vendor-agnostic core security schema. Vendors and other data producers can adopt and extend the schema for their domains. Data engineers can map differing schemas to help security teams simplify data ingestion and normalization, so that data scientists and analysts can work with a common language for threat detection and investigation. The goal is to provide an open standard, adopted in any environment, application, or solution, while complementing existing security standards and processes. AWS is a co-founder of the OCSF effort and has helped create the specifications and tools that are available to all industry vendors, partners, customers, and practitioners. Key security vendors engaged in this project include co-founder Splunk, Broadcom, Salesforce, Rapid7, Tanium, Cloudflare, Palo Alto Networks, DTEX, CrowdStrike, IBM Security, JupiterOne, Zscaler, Sumo Logic, IronNet, Securonix, and Trend Micro. Going forward, anyone can participate in the evolution of the specification and tooling.

The project is not restricted to the cybersecurity domain though the initial focus of the framework has been a schema for cybersecurity events. OCSF is agnostic to storage format, data collection, and ETL processes.

Why Does the Open Cybersecurity Schema Framework Matter?

"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. 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."

Patrick Coughlin, Group Vice President Security Market, Splunk.

cybercrime often involves countering the latest type(s) of hacking attack. Thus, information sharing is paramount to protecting cyber attack surfaces and specific intrusion methods. Much like a virus, modern hacking involves evolution in intrusion methods, and then the replication of successful methods of attack against new targets. By sharing information immediately and in a standardized manner, data can be easily ingested, and data systems can be quickly protected against specific methods of attack.

> "The way cybercriminals behave is not siloed; it's networked and we must take a unified approach to addressing the threat. Businesses must be adaptive and collaborative to compete. Fraud is not a problem that any one organization, industry or government can tackle independently. The formation of the OSFC is a stepping stone in delivering an extensible framework for developing a vendor-agnostic core security scheme. Data vendors can adopt and extend the schema for specific domains still allowing a common language for threat detection and investigation."
> Carey O'Connor Kolaja, CEO at AU10TIX.

The Open Cybersecurity Schema Framework is designed to be extremely adaptable. It is agnostic to storage format, data collection, and ETL processes. The schema framework definition files and the resulting normative schema are written as JSON. For more technical information about the framework, feel free to examine this white paper: Understanding the Open Cybersecurity Schema Framework.

Keys to Success

- Industry Buy-In: Cybersecurity companies need to follow Splunk, AWS and others in implementing this new standard. Additionally, it would be very beneficial if non-security companies that produce data (ex. CRM, HCM, ERP) would join and use OCSF.
- Collaboration: OCSF users must not only ingest data, but also export data, in order for the true collaborative power of OCSF to be realized.
- KPI's: We need key performance indicators (KPIs) on visibility and security outcomes.

What's the Next Step?

Chief Information Security Officers need to change their security architectures to use OCSF as their core schema. By having all of their data sources (SaaS applications, internal apps) speak the same language, CISO’s will be able to rely exclusively on this framework for their data manipulation and analytics. With trust in the framework, data will become more actionable and CISO’s will be able to quickly respond to threats.

“The OCSF project team is looking at success along two axes: implementation of OCSF-compliant schemas in security products and increased engagement within the cybersecurity community. Within the next year, the OCSF steering committee members are encouraging all initial member organizations to implement OCSF standards within their solutions while working together to provide the improvements to integration that cybersecurity teams are asking for,” explains Paul Agbabian, VP, distinguished engineer, security at Splunk.