Highlights

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.

Private, unstandardized data is the status quo in the cybersecurity industry today. Data siloing and a lack of standardization makes it much more difficult to fight back against hackers, as thwarting 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.

As if you needed a reason…

Don't Listen to Janet Jackson's 1989 Rhythm Nation

Janet Jacket's song Rhythm Nation will crash some laptops, including laptops nearby the one playing the song. MITRE Corporation has added it to the register of Common Vulnerabilities and Exposures (CVEs) list of cybersecurity vulnerabilities (CVE-2022-38392). The song contains one of the natural resonant frequencies for a model of 5400 RPM laptop hard drives.

The manufacturer that found the problem added a custom filter in the audio pipeline to detect and remove the offending frequencies during audio playback. Few modern machines have hard disk drives, never mind drives that rotate at the unfashionably slow speed of 5400 revolutions per minute. Also, hardly anybody listens to Janet Jackson anymore so it may not be a huge concern. However, owners of laptops with old, slow, hard disks therefore need to be very careful if they hear Janet Jackson tunes from a nearby computer.

Cybersecurity & Insider Threats

Insider threats and employee sabotage provide cyber threat for companies, big and small:

GE Employee Sabotage

Two General Electric (GE) employees downloaded thousands of files with trade secrets from company servers and convinced a system administrator to grant them access to sensitive corporate data. Then, one of the employees started a new company using the stolen intellectual property and competed with GE for projects. GE lost several bids for turbine calibration to this new lower priced competitor. When GE discovered that the company had been founded by their prior employee, they reported the incident to the FBI. The FBI investigated and both pled guilty to conspiracy to steal trade secrets. They were sentenced to prison and ordered to pay $1.4M in restitution to General Electric.

Capital One Data Breach

A former Amazon software engineer took advantage of a misconfigured web application firewall, and accessed more than 100 million customer accounts and credit card applications. She used her access to mine cryptocurrency. The company has since fixed the vulnerability and stated that “no credit card account numbers or log-in credentials were compromised”. She then shared her hacking method with colleagues on Slack, posted the information on GitHub (using her full name), and bragged on social media about it. She was arrested and found guilty of wire fraud and hacking. Capital One was fined $80M settled customer lawsuits for $190M.

Tesla Employee Sabotages Company After Not Getting Promotion

An employee, angry over not receiving a promotion, changed the code to Tesla Manufacturing Operating systems using false usernames and exported highly sensitive data to unknown third parties.

Dallas Police Department Evidence Deleted

An Dallas Police Department employee attempting to transfer files from cloud storage accidentally deleted 8.7 million evidence files that the department had collected as evidence for its cases: video, photos, audio, case notes, and other items. Most of the deleted files were owned by the family violence

unit. 22 terabytes of data was deleted, and only around three terabytes were recovered. Around 17,500 cases with the Dallas County District Attorney's Office may have been impacted.

[Lawyers Allegedly Stole Firm Trade Secrets]

Elliott Greenleaf claims four former lawyers stole files and deleted emails in order to launch a competing firm. For four months the lawyers were downloading files to person account and used a personal USB device but all malicious activity went unnoticed.

[SGMC Employee Quit Job and Took Data with Him]

A SGMC hospital employee in Valdosta, Georgia, downloaded private data of the South Georgia Medical Center to his USB drive the day after he quit. The employee had access to the data and had no obstacles in capturing the data. South Georgia Medical Center's security software reacted to an incident of unauthorized downloading of data in the form of an alert. It notified cybersecurity staff about an employee copying sensitive information to a USB device. He was arrested and charged with felony computer theft.

Automotive Cybersecurity Market Worth $5.3B by 2025

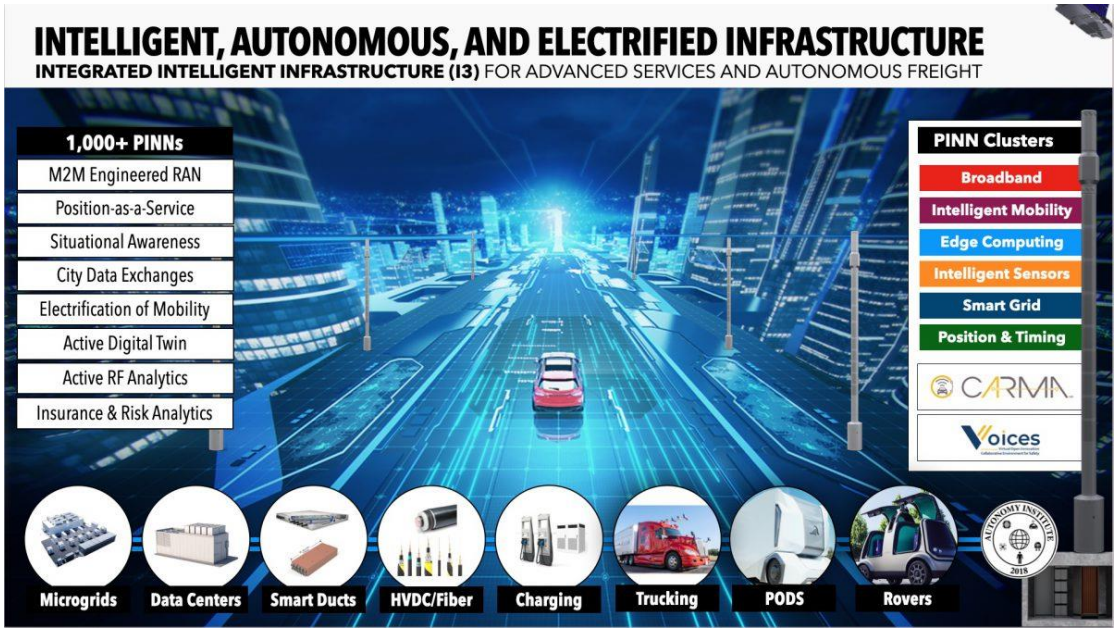
US Lags Behind European Union in Automotive Security Standards

The Internet of Things (IOT) brings with it a wonderful assortment of possibilities and new frontiers, especially in conjunction with automated driving. In-vehicle services promise to revolutionize the car driving experience. Many auto manufacturers are also embracing IOT devices in their factories in order to better manage factory assets and production. IOT-enabled Programmable Logic Controllers (PLC's) provide real time performance data, alerting staff if a fault occurs or if a machine is operating inefficiently. As vehicle manufacturing processes have grown increasingly complex over time, being able to act quickly on this data can lead to large cost savings for automotive companies. Harley Davidson was able to save 200M as a result of overhauling their factory with IOT connectivity:

In 2016, Harley-Davidson leveraged IoT to change its York (Pennsylvania, USA) manufacturing facility and reduce the time it takes to produce a motorbike from a 21-day cycle to six hours. Now, one motorcycle comes off the assembly line every 89 seconds.

While IOT is and will be very valuable to companies, connected automotive factories and the IOT expand the size and scope of cyberspace itself, giving hackers new vulnerabilities to target. Accompanying this broad expansion of connected factories is an urgent need for data encryption and multi-factor authentication to strengthen edge nodes.

Industrial networks will need to scale rapidly as industrial IoT users adopt new technologies to expand the services available on their networks. However, IoT platforms must ensure that the security processes can scale alongside this network growth.



Connected Vehicles

Similar steps need to be taken with connected vehicles in the United States. Europe has a rigorous set of cybersecurity standards that apply to all new vehicles sold in the EU. While it's possible that European regulations will result in automakers investing in vehicle cybersecurity technology that will eventually end up in US vehicles, that doesn't help US consumers in the short term. Modern luxury cars have more embedded code then fighter jets:

The F-22 Raptor fighter jet uses about 1.7 million lines of software code, while Boeing's upcoming 787 Dreamliner passenger jet is expected to use close to 6.5 million lines of code, and a modern luxury vehicle "...probably contains close to 100 million lines of software code," according to Technical University of Munich professor Manfred Broy. This number is only expected to increase with a major innovation that is set to accompany autonomous vehicles and the expansion of IOT: telematics infrastructure. This includes everything from smart roads and connected electric vehicle charging, to city data exchanges and position as a service applications.

One of the biggest issues today with vehicle cybersecurity is the Controller Area Network (CAN) protocol that is used by all major auto manufacturers. One of the advantages of such a protocol is its simplicity, allowing vehicles to combine the protocol with cheap chips. However, the CAN bus protocol does not secure data at all, as data is easily readable off of the device itself. This underscores not only the importance of replacing (or redesigning) CAN for automakers, but also the importance of protecting CAN access points for the time being. On an individual vehicle level, the four major device entry points are Telematics, Infotainment, Direct Interfaces and Sensors:

Researchers have also shown how to attack vehicles from within a vehicle using direct interfaces and infotainment systems via the On-Board Diagnostics port (OBD-2), USB and CD player and from outside the vehicle using medium and long distance communication such as Wi-Fi, Bluetooth, mobile (phone) networks, and sensors signals such as keyless fob attacks and tire pressure monitoring system sensors. - Cyberattacks and Countermeasures for In Vehicle Networks

Due to the volume of different CAN access points, the most elegant authentication methods might be biometric. A camera sensor in the vehicle that could identify the driver using an iris or thermal face scan could provide an additional layer of security to vehicle entry points, and a fingerprint sensor in the keyless fob could protect against a CAN attack while still allowing users to lock/unlock their vehicle while outside of it. It is imperative the automakers move quickly to a better system of cybersecurity management considering the stakes involved as cars become fully autonomous.

Cybersecurity is a Critical Short-Term Risk

Eighty percent of companies over the last year have been attacked by hackers. Thirty percent of companies faced one cybersecurity attack per day. Despite this high volume of attacks, it's questionable that IT professionals are doing enough to protect their employer's data - as nearly half (47%) of IT Managers are not even using multi-factor authentication solutions to prevent security breaches. Traditional single factor password authentication methods are vulnerable to brute-force attacks. But multi-factor authentication requires biometric verification, or cell phone verification, removing this brute-force vulnerability.

Cybersecurity breaches cost firms an average of $4.35M per attack, according to IBM. Breaches can lock up corporate data, inhibiting the company's ability to operate until the data can be freed. Board of director members' primary job is to protect the interest of shareholders, and because the cost of a breach is so high, securing corporate data needs to be a key priority of board members.

In 2021, the World Economic Forum published the Principles for Board Governance of Cyber Risk. These are the foundation for a solid cybersecurity defense. Additionally, it's vital that each organization has one employee who owns the cybersecurity risk. Ideally this person is Chief Information Security Officer (CISO) in the company. The company's risk profile by business unit, as well as the creation and monitoring of key cybersecurity metrics can inform board members about the company's cybersecurity position. Two of the key pillars of any cybersecurity defense involve cybersecurity training and cybersecurity communication with employees. Training for cybersecurity breach responses is important in reducing the damage that a breach can cause. Communicating with employees is critical for securing data and protecting entry points into the company's data. With the right structure in place, board members and CISO's can reduce shareholder risk and protect valuable company data.

Upcoming Conferences

August 27-28	Blue Team Con, Chicago
August 29-Sept 1	VMwear Explore, San Francisco
September 8	FutureCon, Des Moines
September 12-14	Gartner Security & Risk Management Summit, London
September 13-14	CISO Forum, Virtual
September 14	Cybersecurity Expo, Phoenix
September 19-20	Industry of Things World, Berlin
September 20-22	Dreamforce, San Francisco
September 22-23	Global Cyber Conference, Zurich
September 26-28	InfoSec World, Colorado Springs
September 27-28	International Cyber Expo, London
September 28-29	IoT World, Santa Clara
September 28-30	Spiceworld, Austin, Hybrid
October 3-4	451Nexus, Las Vegas
October 5-6	Evolve, Vegas
October 10-12	ISC Security Congress, Vegas
October 11-13	Google Cloud Next, Virtual

October 17-19	Authenticate 2022, Seattle
October 17-20	Gartner IT Symposium/Xpo, Orlando
October 24-27	ICS Cybersecurity Conference, Hybrid/Virtual
November 16	San Diego Cybersecurity Conference, Hybrid
November 16	Threat Hunting Summit, Virtual
November 18-19	Data Strategy & Insights (Forrester Research), Virtual
December 1-2	AI & Big Data Expo Global, London
December 6	Security Operations Summit, Virtual