ATTENDEES

Beal, Helen – VSMC
Cullinane, Kelly - Copado
Davis, Robert - Plutora
Kanser, Heather - Broadcom
Pereira, Steve - VSMC
Sparrel, Duncan - sFractal Consulting
Valani, Altaz - Security Compass
Grad Speaker: Jason Keirstead, IBM

AGENDA

- Call to order & welcome
- OCSF Discussion with Jason Keirstead of IBM
- Review remaining differential analysis
- New Business: Task 2 - outlining key components

NOTES

- Call to order & welcome
- Please log your attendance
- Discussion of OCSF with Jason Keirstead
  - Problem Space: Lots of vendors, products don't interoperate well
  - Focused on log and event telemetry. Not the same use cases as other standards, like STIX/TAXII, threat intel or threat modeling.
  - Telemetry has high volumes of data and automatic data - temporal in nature, not a graph. This makes telemetry unique.
  - Key purpose - Structure data in a way that it can be stored and searched efficiently in data lake sand facilitate analytical use-cases of log data
  - Define a classification scheme, attribute & object dictionaries and a common type system from which specific schemas can be constructed
    - Take high volume data and analyze it. Need normalization to a common taxonomy to be able to search/analyze it.
  - 5 Key use cases:
    - Low Cost - store large volumes of data economically.
    - Federated Data Access - normalize data across multiple stores
    - Performant Search** - maintain high performance for simple monitoring @ low cost (key use case) multi terabytes stored for multiple years
    - Open Formats & Access - support search & storage using ecosystem tools
    - Simple Data Management - filter, transform, route right data to right place and have it be understood. Compliance implications will/could dictate what is kept/not kept and how – storage and access rule easier when data is normalize
Large crowdL Splunk, AWS, Broadcom, Symantec, Cloudflare, Zscaler, DTex, JupiterOne, Crowdstrike, Sumologic, IronNet, Tanium, IBM, Securonix, Rapid7, Salesforce, SentinelOne – later additions

**Fundamentals**
- Github minimal viable governance model – not homed in an SDO under LinuxFoundation or OASIS.
- Trying to work with community to move it to a more substantial governance structure
- Want version 1 out the door first. Changes occurring on a weekly basis

Duncan: This has been submitted to the ITU

- Meant to be open, unambiguous, self-describing. Slack is open to anyone. Calls as well.
- Both a framework and a schema.
  - Global dictionary to create field types
    - Any given class will reference a field/attribute
    - Can group these together to make a meaning
  - Dictionary is in JSON can look at see what is defined in the dictionary

Server - web app that hosts a browsable version of the schema


Duncan: VSMI centric viewpoint – we are more the process than the answer. How does OCSF go back one step in the development chain?

Jason: Focus is still telemetry and cybersecurity operations. Wouldn't expect to see things about CI/CD pipelines, SBOMS, unless you use OCSF to create a finding. (Findings is a category in the schema). This is what is being worked with in the SOC.

Duncan: Tying back what is happening in the SOC to root causes. Optimize on where to spend money and time. Not always an obvious answer.

Jason: CSNF - Run by ONUG - New standard in development. The ONLY purpose is cloud findings. Been working for 2 years trying to get cloud providers to standardize. Use cases are different so they are tackling a different problem. Only focused on security findings. Could be brought into OCSF at one point, but working on a different problem at this time. Participation is very restricted.
Next Steps:
  ○ Next meeting is Nov 1
  ▶ Canceling October 18 due to a conference most are attending
  ○ Bob is going to see if Plutora would like to share their schema so we can being on task 2

Action Items

● Kelly & Duncan - Research NIEM to see if it includes a software dev process
● Bob - talk to Simon to see if Plutora would like to present data model