NET+ Splunk Community Monthly User Group Call-2021-08-18

NET+ Splunk Community Call

Date: 8/18/2021

Agenda is:

1. Intro – call is recorded
    a. Please rename yourself in Zoom to include your campus name.
    b. Introduction to the call, announcements, reminder the call is being recorded, etc
    c. Registration, awareness, emails, etc – how did that work?
2. Agenda bash / round table of issues of submitted questions
    a. Managing getting log data into Splunk with Cribl or other tools
    b. Using Splunk in CMMC/research environments in AWS.
    c. Campus plans for 2021 for your Splunk deployments
    d. Your item here
3. Open discussion
4. Any feedback on the NET+ Splunk program
5. Next call is Sept 15th, 2021 at 3pm ET

Numbers: 16 campuses

Recording: GMT20210818-190412_Recording_1920x1120.mp4

Auto-generate transcript from Zoom: GMT20210818-190412_Recording.transcript.vtt.txt

Chat transcript: GMT20210818-190412_Recording.txt

Notes:

Managing getting log data into Splunk with Cribl or other tools

90% of traffic through Cribl into Splunk

Thur Aug 26th – Cribl next step

De-dup a lot of events

Forward data to an S3 bucket

Like a heavy forwarder

Cribl getting O365 logs

Timeliness of the logs?

Few minutes delayed. 5-10 minutes operating on an interval timer.

Pulling from MS service hub.

De-duping fields – depends on the firewall rule

With quantifier. Depends on the context of the traffic

Regex and UI for Cribl to configure workflows

Running on single instance for 200GB

Going to keep in prod

DNS query logs

Need to do some de-dup

Not sure about cost

Free up to 2TB a day

Community based support

Can summarize data over longer period of time

Volume license – in Splunk

Netflow license:

- Netflow/DNS license:

https://www.splunk.com/en_us/legal/licensed-capacity.html

Where it has a section on "Splunk Enterprise for DNS & Netflow Data"

Is that useful for adding data for enrichment

- Using Threat intel
- Useful for searchers or dashboards
- Abstracting how this might be done in Apache Kafka
- How to include internal databases for how to do that lookup
- Increase size of events in Cribl
- Palo Alto packs for stripping out unnecessary fields
- https://github.com/criblpacks/cribl-palo-alto-networks

Cribl architecture?

- Running Redhat 8 VM using RPM
- Typical RPM upgrade
- Nothing crazy for VM specs for the 200GB per day
- Licensing/pricing?
  - Using free tier
  - 10 workers as part of cluster

What is ingested into Cribl and then to Splunk?

- 200GB to Cribl and think 25% reduction for Splunk

1. Using Splunk in CMMC/research environments in AWS.

Worked with Deloite – using centralized log

Splunk Security

Splunk Cloud

Pricing really added up on Splunk Cloud/Security App

Splunk license centrally

Standalone Splunk and ES to monitor logs

Lots of work done quickly in controlled environment

Used this to learn about on-prem and what needs to be done in AWS

ControlTower not available in GovCloud

Recording for UCLA Health AWS with Splunk mention:

https://www2.internet2.edu/l/66332/2021-07-30/dxzd7y/66332/1627668530LGUmtkGr/doc_I2_UCLA_AWS_Webinar.pdf

Community Voices: The UCLA Health Sciences HIPAA-Compliant Cloud Journey for Academic Research, July 30 – using Splunk in AWS

https://internet2.hosted.panopto.com/Panopto/Pages/Viewer.aspx?id=621e3de5-2b14-47ca-86ee-ad750157e6aa

Using Docker?

Used for development

Makes sense for forwarders or dev boxes

Cribl? Did POC with free? Commercial vs non-commercial?

- Splunk Slack channels
- Pretty good community support
- Also a Cribl slack: cribl-community.slack.com
- Using Logstash or Kafka?
- Cribl better than Heavy forwarder
- DNS log data parsing and summarizing
- Sending data to a long term archive
- Metrics have been really valuable
- Free tier and pay for support?
    - Don't know

Splunk Slack channel

- https://docs.splunk.com/Documentation/Community/1.0/community/Chat
- phantom too: phantom-community.slack.com
- High concentration of Splunk fezs

Summarization

- Can be configured based on fields
- https://sandbox.cribl.io/course/metrics
- Tstats

Just starting metrics. Where to save on license overhead

Moving Splunk instance to AWS

Use of metric indexes

- Lots of development for app and getting deprecated

RFP for Splunk vs Elastic. Anyone done the proof of concept?

- Free Elastic doesn't seem to be enough
- Number of staff needed for reporting and dashboards was significant effort

- Probably need to do RFP
- Visualization better with Splunk
- License constrained running Elastic
- Large Elastics a lot of work
- Did bakeoff IR using Splunk review logs vs GreyLog
    - Found this valuable to demonstrate value of Splunk
    - Gather more actionable data in Splunk
    - Needed to know Elastic much better to get data out
    - Didn't write a report

Education programs for your users?

- Welcome App?
- Success with that
- Used for creating Apps
- https://splunkbase.splunk.com/app/2991/

Education credits or discounts for Splunk

Some credits used for Splunk team, but need Splunk power user for 80 people on campus

Free training helps with more users using Splunk

Splunk sees as revenue source

Current free training from Splunk: https://events.splunk.com/public-sector-virtual-workshop-series

.conf – anyone going?

This article touches on metrics, but it also makes mention of data replay to an ephemeral log system. Might be a use-case for Elastic container. https://cribl.io/blog/extract-metrics-from-logs/

Next call is Sept 15th, 2021 at 3pm ET