NET+ Splunk Community Monthly User Group Call-2020-02-13

NET+ Splunk User Group call

Date: 2/13/2020

Agenda:

1. Introductions and reminder about the format of this call. We're going to talk about data sources.
2. What data sources do you include in your Splunk?
    a. Firewall, IDS, flow data, DHCP, NAT, AD, workstation logs, server logs, Vulnerability management, AWS and cloud logs, IDM/SSO, Physical access control systems, VPN, Database, darknet, other syslog, non-log files, enrichment data, etc?
    b. Application logs from LMS like Canvas, Blackboard, D2L, etc? EHR like Epic, Cerner, other?
    c. SIS/ERP like Banner, Peoplesoft, other?
3. What data sources provide the most value?
4. What did you have to do to get those logs?
5. How do you manage all of the logs?
6. What logs get used the most?
7. Logs from outside IT?
8. Open discussion and questions
9. Next call on March 12th 2pm ET

Attendees: 15

Presentation: 

Recording (audio only): 

Recording (with presentation): 

Zoom chat: 

Auto-generated transcript from Zoom: 

Notes:

DNS

Anyone sysloging to us, goes into us goes into Splunk

AWS, O365

Working on Google Apps for EDU

Getting auth logs and user lockout

Parsing alerts that come in and what severity

Separate domains for fac/staff GAE. Don't do much alerting on content. Use Cloudlock app for Splunk

AzureAD sign-ins?

What your own app?

- Using someone from Splunkbase – Splunk add for MS cloud services. Add-on for AzureAD

With MS, can setup SIEM exporter

One app that the sec team – blue team app for O365 and Azure

https://www.ren-isac.net/public-resources/0365resources.html

Licensing levels for logs

You can buy a single elevated license to export the data. Didn't need to have entire number of accounts to get that data.

Custom Bluecat for IPAM

Wireless logs with locations

Tracking lost/stolen devices

Some privacy implementation

Missing DNS and flow logs – concern about if affordable

Homegrown tools to do admin things – create their own logs

- Build reporting for HD

HTTP event collector – looking for cloud deployed apps – using JSON blobs

Major application stacks logging to Splunk

Dev logs into one index and servers in another

All Vuln management logs go in using Qualys – enhanced reporting

Makes the vuln mgmt. reports easier to consume. Including relative age.

Shib app going

Correlation with Radius

There's a Shib app for Splunk?

- Yes - https://splunkbase.splunk.com/app/4389/

Yes to Banner web. For IR. Logging of host and DB.

We do PeoplesoftWeb, servers, and DB

And Workday

Peoplesoft?

- Web, server, DB audit logs
- How do you get the log? Put universal forwarder?
- Performance issue?
- App owners have expressed concerns on performance
- We haven't seen performance issues from universal forwarder
- Config feature X to send right IP address to Splunk

- Load balancer

Issue to get Peoplesoft logs when looking at individual systems, but showing them how to look across multiple system

We've had a hard time in the past to universal forwarder, but haven't really had an issue

Just looking at physical, scada, camera, door swipes, etc – response to an audit

Discussion around HR investigations

EHR investigations

Central IT disconnected to HS

Surprising that more campuses didn't speak-up around the physical access

We have a need to collect this in Cbord and working to get into Splunk

Student health system – shouldn't include PII

Sakai logs – for student success logs

Standards in how fac are putting data in the system – how this difficult to do without those standards in place across the fac

Has anyone dealt with the challenge around allowing people outside IT to have access to Splunk data? Fac person interested in machine learning.

- Put into roles to give them appropriate access
- Famous athletes
- Tracking from a business perspective
- Using search filters to limit access
- Governance process
- Researcher wants access to everything – how to anonymize the data
- IRB?

IRB education – correlated data and re-identification

What do we have to do to protect the human subject?

IRB proposal give some strength to governance

Watson chatlogs – to enhance self-service for chatbot

Lower support costs to students

Fairly small amount of json data

Hold Data sources value for next month

What do you need to do to get the logs?

Build it and they will come

Show them the value

Make getting data in easy

Don’t do a lot of control of what to log

Try to stay out of their way to get the data in

Very distributed

Have lots of docs about how to do it

How to balance with license limits?

FW change and huge growth in log size

Sec team paying for the license

Much is reporting and detection about usage of system/size of logs

Something you need to track on a day-to-day basis

Smaller campus IT that need to discuss how it’s going to be handled

Need to control the growth to meet license

Pruning turns out to take a lot of effort in this process

Hardest logs have been the business logs because of data governance

Tech and business person working together

Finish up “What do you need to do to get the logs?” on next call