Cyber Defense Organization

Fall 2019 - SIEM Workshop

Announcements

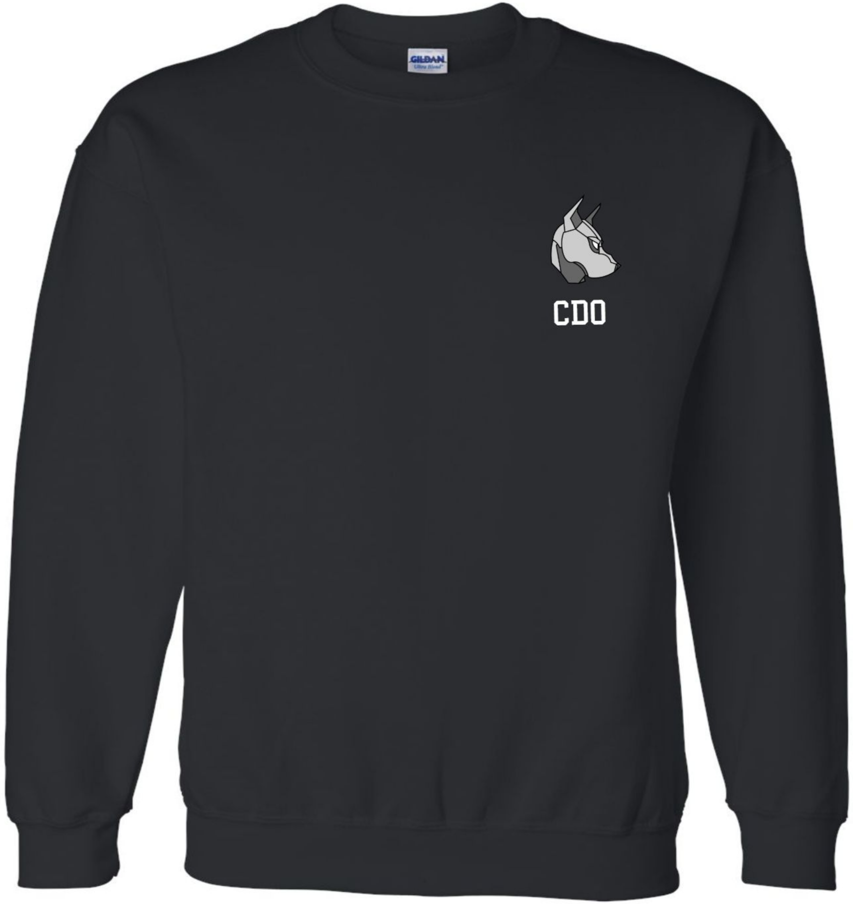
CDO Swag

Last call for CDO Crewnecks!

20$

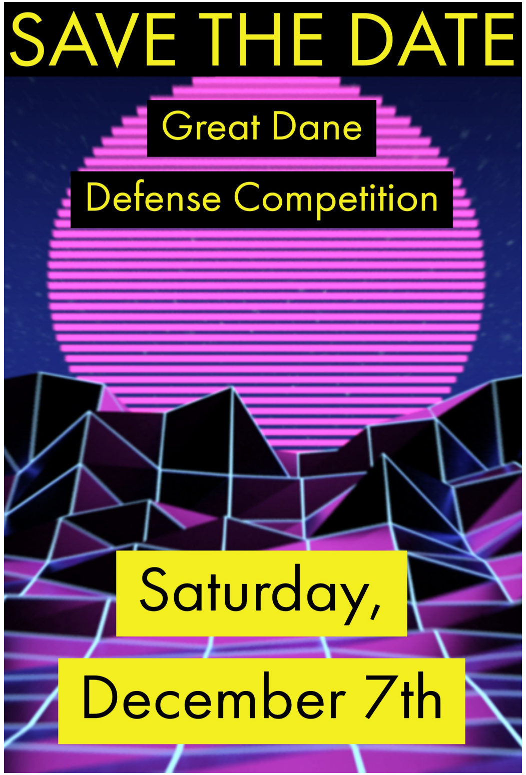
Purchase Form in CDO Emails, Give cash to Kayla Ibrahim or venmo: **@Kayla-Ibrahim**

CYBER DEFENSE
ORGANIZATION



2019 GDDC COMPETITION

GGDC - Save the Date



SAVE THE DATE

Great Dane

Defense Competition

Saturday,

December 7th

Word of the Week

YARA

YET ANOTHER REGEX ALTERNATIVE

https://github.com/mikesxrs/Open-Source-YARA-rules/blob/master/crowdstrike/Crowdstrike_index.yara

Lets Go - SIEMs
Why do should you care?

Core Enterprise Security Stack

Security Tools:

1. Vulnerability Scanner
2. IPS/IDS
3. **SIEM**
4. Anti-Virus / EDR
5. Data Loss Prevention
6. Email Gateway

System Administration

1. IAM/Okta/Active Directory
2. Firewall Rules
3. Group Policy
4. Netflow / Network Traffic
5. Patch Management

Rob Joyce (bae) Said So.

“Enable those logs, but also **look** at those logs.

You’d be amazed at incident response teams goes and there’s been some tremendous breach and **yep there it is,** right there in the logs.”

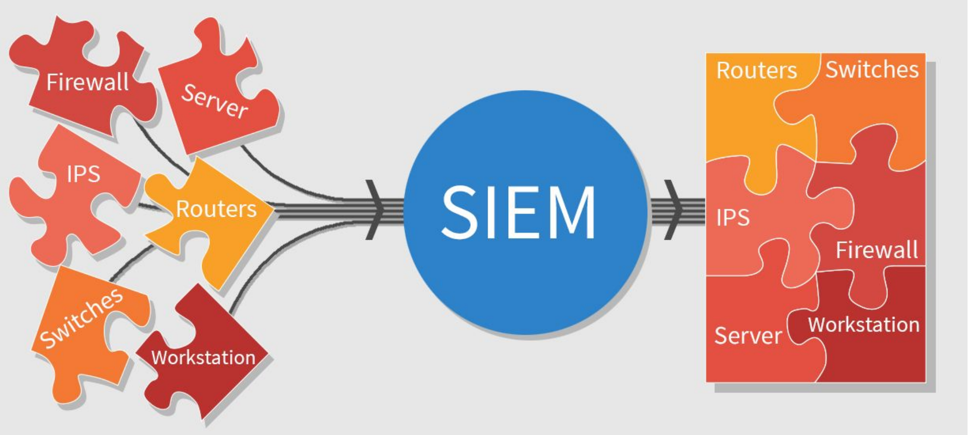
21:50

https://www.youtube.com/watch?v=bDJb8WOJYdA&feature=youtu.be&t=1312

What is a SIEM?

- SIEM (Security information and event management)
- The goal is to centralize logs in one place and allow for automated analysis
- Allows security analysts to easily read log information from a large amount of sources.
- Key word: **Log Consolidation**

TL;DR A big old Database disguised as security software



splunk>

sumologic

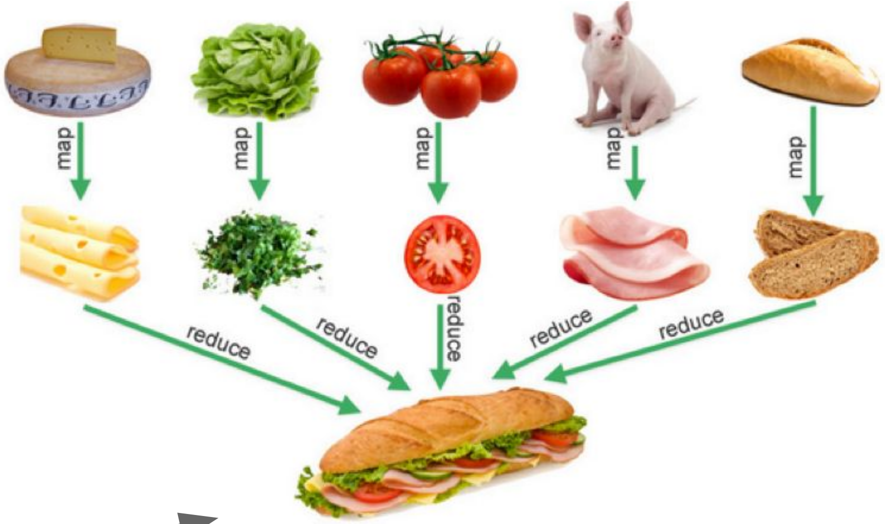
graylog

What's so good about Splunk?

- Splunk allows people to create alerts whenever an action occurs
- Splunk allows you to extend its functionality by installing apps
- Does not take up a large amount of CPU or memory in a host computer
- Pretty much it is customizable, easy to use, and allows you to view log data easily

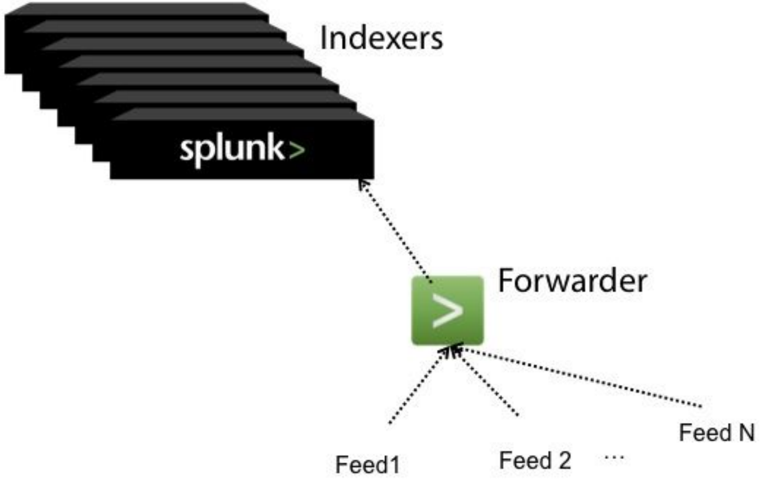
How Does Splunk Work?

- Splunk ingests log data through forwarders installed on host machines
- This log data is sent to indexers to parse the logs and organize them
- The indexed log data is searchable on the splunk instance’s GUI, all centralized in one location.



How is Splunk Deployed?

- Splunk utilizes **Forwarders,** agents installed on computer’s to forward logs to the server hosting Splunk which will be indexed by the Indexers.
- In large corporate networks, the functions I talked about are split.
- There are splunk instances that just allow for indexing data and nothing else
- There are dedicated splunk for forwarding data and nothing else, universal forwarder
- There are splunk instances just designed for searching data sent to indexers



What does our Deployment look like?

- One splunk instance that has all search, and local indexing enabled
- There are no forwarders and no indexers, everything we are drawing from is local logs
- NOT REALISTIC

Lets Boot the VM

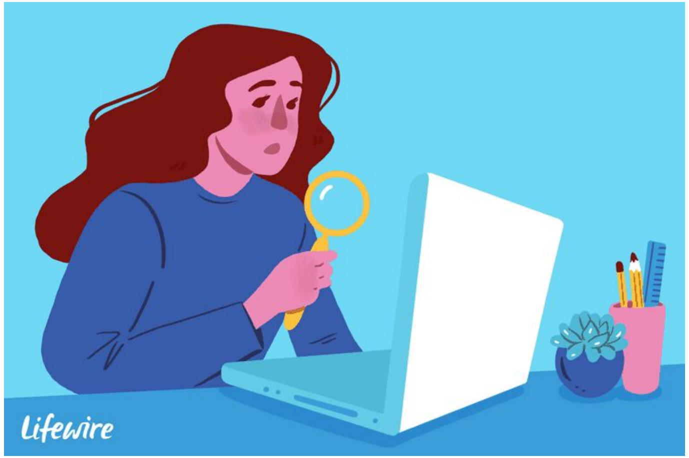
- Boot the virtual box “splunk_lab”
- User: CDO Password: (what do you think)
- bb123#123
- **https://tinyurl.com/CDOFall19SIEM**

Getting Splunk operational

- Type in: sudo /opt/splunk/bin/splunk start
  - Splunk web should bind to port 8000
- See if splunk is operational:
  - Go to firefox and type in localhost:8000
  - User: admin password:bb123#123
- Get some logging data in:
  - Click on the Unix Linux app and follow the steps to enable /var/log logging

Search

- Open up the Search App
- This is the core of Splunk: it allows you to search through indexed logs
- Methodology: know what you are trying to find, and come in with a question you want answered, mold your search around that



Fields

- All of the elements of a splunk log is parsed into fields for you to look at. You can filter based on those fields along with other criteria
- Lets try filtering off a field now

SourceTypes

- Sourcetypes are Splunk's way of identifying the format of log files
- For example, web proxy log format has different information then a syslog format
- Access_combined deals with http access logs

Reports

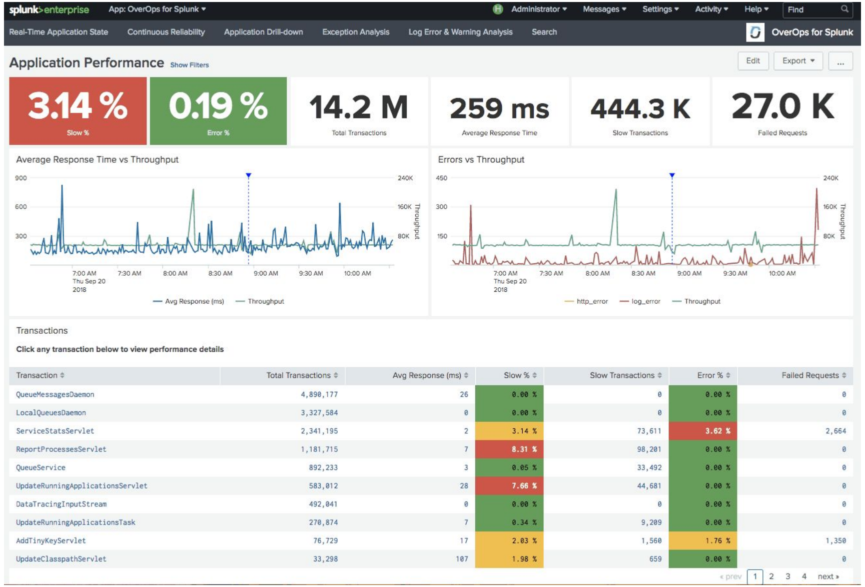
- Reports are a great way to repeat a search action and display results of a search
- Can be turned into a dashboard - that's for later
- Lets go look at the reports: go to search and reporting app and click on ______ (will fill in tomorrow)

Lets make our own report

- Go back to search and reporting and search for this: sourcetype=access_combined AND 404
- Screenshots will come later

Lets Make Our Own Dashboard

- Dashboards are a great way of showing you what you want to see immediately
- Lets modify our search query to make a dashboard
- Go back to the search app and type in the same search but add in | timechart count
- Click save as dashboard panel



Application Performance

3.14 %	0.19 %	14.2 M	259 ms	444.3 K	27.0 K
Slow %	Error %	Total Transactions	Average Response Time	Slow Transactions	Failed Requests

Average Response Time vs Throughput

Errors vs Throughput

Transactions

Click any transaction below to view performance details

Transaction ⇕	Total Transactions ⇕	Avg Response (ms) ⇕	Slow % ⇕	Slow Transactions ⇕	Error % ⇕	Failed Requests ⇕
QueueMessagesDaemon	4,890,177	26	0.00 %	0	0.00 %	0
LocalQueuesDaemon	3,327,584	0	0.00 %	0	0.00 %	0
ServiceStatsServlet	2,341,195	2	3.14 %	73,611	3.62 %	2,664
ReportProcessesServlet	1,181,715	7	8.31 %	98,201	0.00 %	0
QueueService	892,233	3	0.05 %	33,492	0.00 %	0
UpdateRunningApplicationsServlet	583,012	28	7.66 %	44,681	0.00 %	0
DataTracingInputStream	492,041	0	0.00 %	0	0.00 %	0
UpdateRunningApplicationsTask	270,874	7	0.34 %	9,209	0.00 %	0
AddTinyKeyServlet	76,729	17	2.03 %	1,560	1.76 %	1,350
UpdateClasspathServlet	33,298	107	1.98 %	659	0.00 %	0

Lets make An Alert!

- Go to search app, type in something you want to be alerted about
- So lets do the same search as before, change it to an 1 hour search window
- Click Save As Alert

Go Hunting

- That sure is a lot of 404 errors!
- Is there a pattern?
- What is causing them? Dig in!

A little take home...

- Sumologic is free and comes with some pre-built labs!
- Go to...
  - Service.sumologic.com
  - Username: training+labs@sumologic.com
  - Password: Sum0Labs!
- Worksheets
  - http://tinyurl.com/SumoCore
  - http://tinyurl.com/SumoSec

Cya Next Time!

Next time on DBZ....Cloud Security with Tyler!

amazon web services

Add us on Social Media!

Twitter: **@ualbanyCDO**

Instagram: **ualbany_cdo**

Website: **uacyber.org**

Myinvolvement: **Cyber Defense Org**

We have a discord!