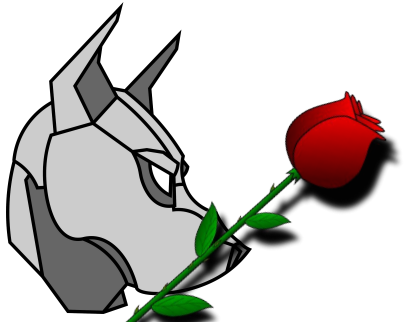
Cyber Defense Organization

Spring 19’ - Threat Hunting (at scale)



Agenda

Note: Last week was a pure lecture/do as I do. This week is 50/50.

- Who are you?
- Small Term of the week
- What is a SIEM
- Why Do I care?
- Do as I do
- Labs

Who are you:

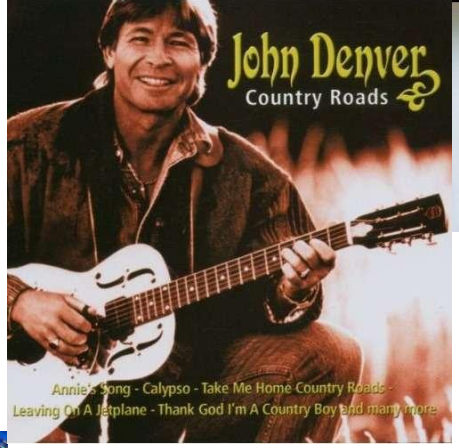
Liam Smith

President of CDO. Interned at the MLB and DMV. CCDC main windows guy. Got a CySA+.

Met Michael Christakis once.

Epic ‘shop skills.

Liam Starter Pack



"I'm literally dying"
"Hi literally dying I'm Liam"

npr

Confluence

Small Term of The Week

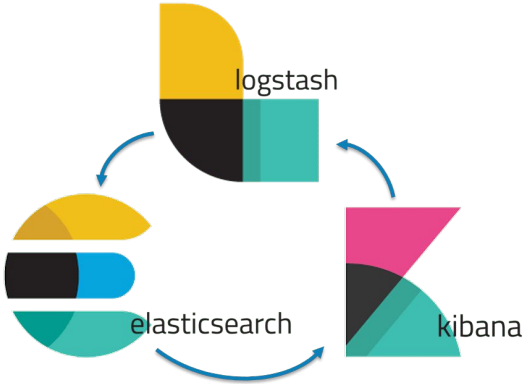
Pneumonoultramicroscopicsilicovolcanoconiosis: lung disease from inhaling volcanoes

What is a SIEM?

Security information and event management (SIEM): The underlying principles of every SIEM system is to aggregate relevant data from multiple sources, identify deviations from the norm and take appropriate action.

TL;DR A big fanny database disguised as security software.

splunk>



sumologic®

Why Should I Care?

Core Enterprise Security Stack

Security Tools:

1. Vulnerability Scanner
2. IPS/IDS
3. **SIEM**
4. Anti-Virus
5. DLP

System Administration:

1. Active Directory Group Policy
2. Firewall Rules
3. NetFlow
4. Patch Management

Policy:

1. Password
2. Acceptable Use
3. BYOB
4. Patching Schedule

Rob Joyce 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 is it is**, right there in the logs.”

https://youtu.be/bDJb8WOJYdA?t=1312

Finally: Jobs

These technologies are everywhere and it's a core skill for any InfoSec professional.

Also, if you are Interning, odds are it will be something you do.

Information Security Analyst

ING ★★★★☆ 1,599 reviews - Totowa, NJ

Apply Now | Save this job

supervision.

Main Duties and Responsibilities:

- A solid understanding of SIEM solutions; examples of related technologies include Arcsight, RSA Envision, Alienvault, Splunk
- Ability to develop, document, and maintain use cases
- Identify key events to be monitored, continuous evaluation and recommendations to change configurations to match risk appetite

indeed

What: Job title, keywords, or company — Splunk

Where: City, state, or zip code — New York, NY

Splunk jobs in New York, NY

Page 1 of 293 jobs

Plans for Today

We are going to be using a SIEM called SumoLogic.

Why?

Its a growing in popularity,

it has almost the same query language as Splunk,

and it has an open free training environment.

Getting On Sumologic

Goto:

Site: service.sumologic.com

User: training+labs@sumologic.com

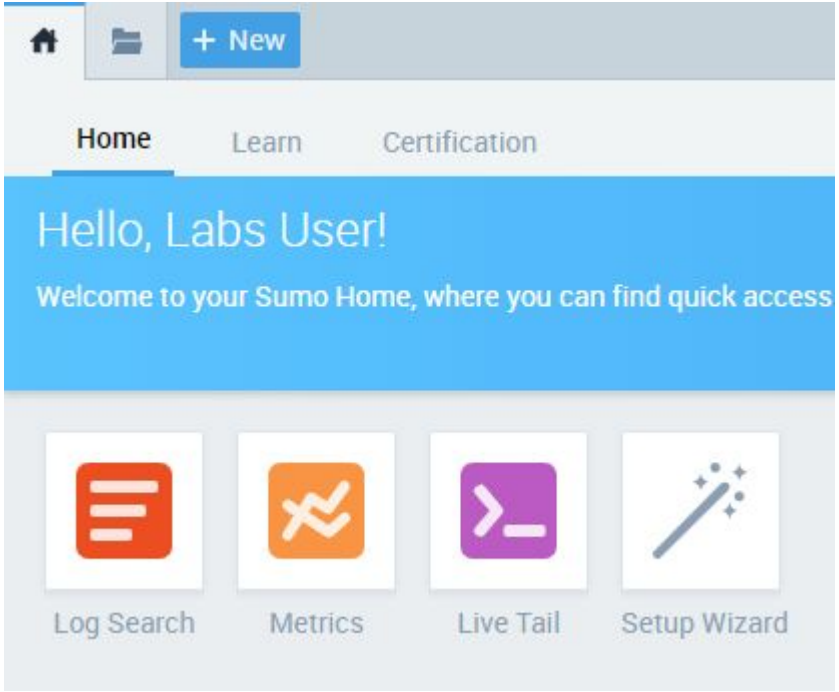
Pass: Sum0Labs!

https://tinyurl.com/SumoCore

https://tinyurl.com/SumoSec

Basics - What Logs?

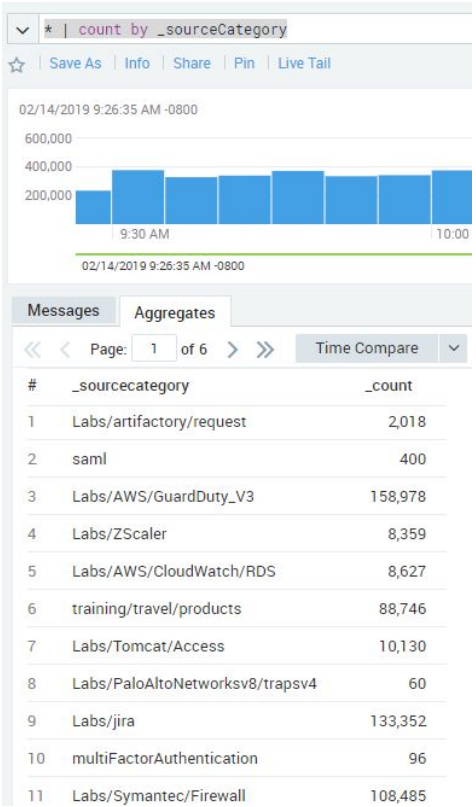
Select Log Search



Your Very First Search

* | count by _sourceCategory

What does this do?



#	_sourcecategory	_count
1	Labs/artifactory/request	2,018
2	saml	400
3	Labs/AWS/GuardDuty_V3	158,978
4	Labs/ZScaler	8,359
5	Labs/AWS/CloudWatch/RDS	8,627
6	training/travel/products	88,746
7	Labs/Tomcat/Access	10,130
8	Labs/PaloAltoNetworksv8/trapsv4	60
9	Labs/jira	133,352
10	multiFactorAuthentication	96
11	Labs/Symantec/Firewall	108,485

Sumologic Internals

All data/Logs that Sumologic ingests are tagged with metadata.

_sourceCategory Is the “bucket” or category the team wanted it to be in.

_collector is the name of the collector agent.

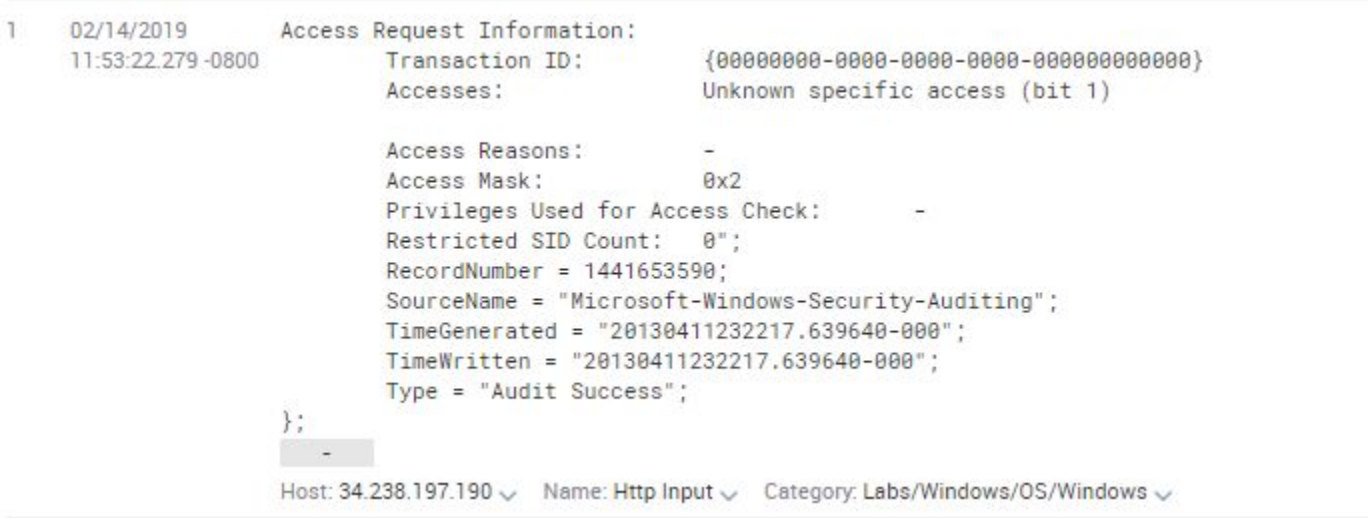
_sourceHost is the name of the host the log came from.

Name	Description
`_collector`	The name of the Collector (set when the Collector was installed) that received the log message.
`_messageCount`	A sequence number (per Source) added by the Collector when the message was received.
`_messageTime`	The timestamp of the message in milliseconds. If the message doesn't have a timestamp, messageTime uses the receiptTime.
`_raw`	The raw log message.
`_receiptTime`	The time the Collector received the message in milliseconds.
`_size`	The size of the log message in bytes.
`_source`	The name of the Source, determined by the name you entered when you configured the Source.
`_sourceCategory`	The category of the Source that collected the log message. This can be a maximum of 1,024 characters.
`_sourceHost`	The host name of the Source. For local Sources the name of the Source is set when you configure the Source. For remote Collectors, this field uses the remote host's name. The `_sourceHost` metadata field is populated using a reverse DNS lookup. If the name cannot be resolved, `_sourceHost` is displayed as `localhost`. This can be a maximum of 128 characters.
`_sourceName`	The name of the log file, determined by the path you entered when you configured the Source.
`_format`	The pattern used for parsing the timestamp. See here for more details.

Parsing Logs

_sourceCategory=Labs/Windows/OS/Windows

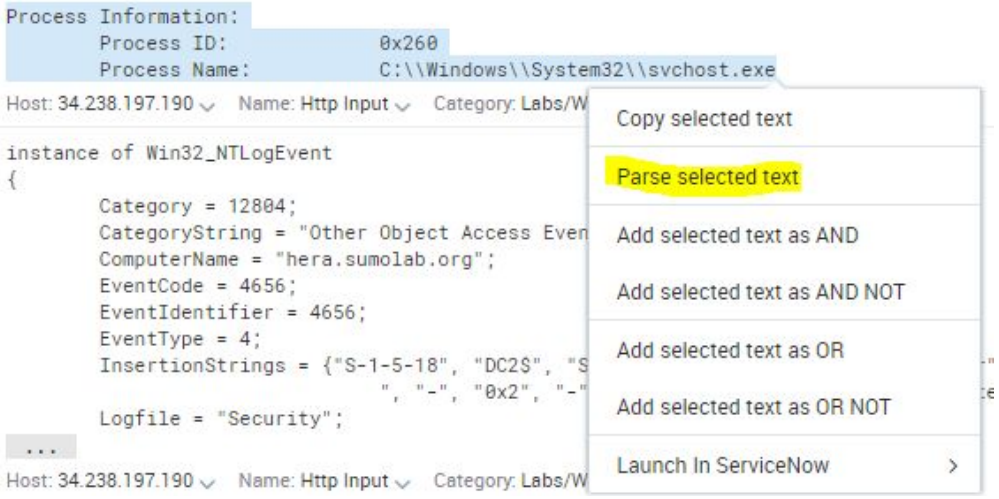
What the hell is this...and how do I work with it?

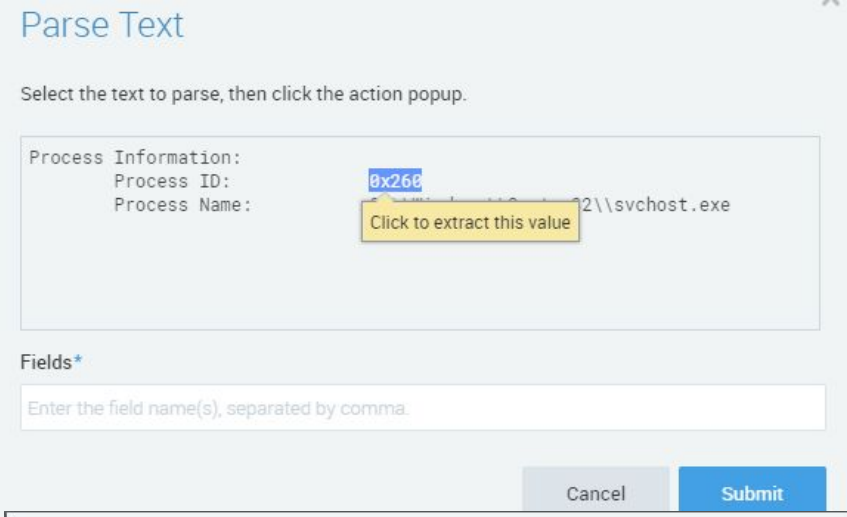


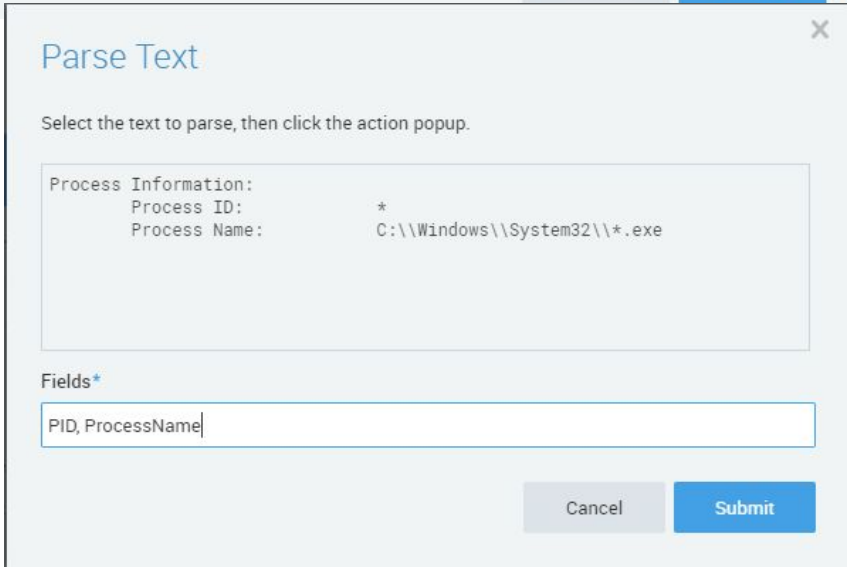
Parsing for Real

Find a Process Information Log

Highlight All of it, and select Parse.







Query

_sourceCategory=Labs/Windows/OS/Windows

| parse "Process Information:\n\tProcess ID:\t\t*\n\tProcess Name:\t\tC:\\\\Windows\\\\System32*.exe" as ID,ProcessName

| **count by ProcessName**

Finally: Snort

Snort is an IPS and we have some fun logs!

_sourceCategory=Labs/Snort

Parse the time, attackerIp, Attackerport,
localIP, Lport

| count by attackerIp

Investigate

Where can else can we see this IP?

When I made this, this IP was mention in the logs 2.7k times.

Last Thing: Outlier Analysis

_sourceCategory=Labs/Snort

| parse "* WEB-PHP Typo3 translations.php file include [Classification: Web Application Attack] [Priority: 1] {TCP} *:* -> *:*" as time,attackerIp,Aport,localIP,Iport

| timeslice 5m

| count (attackerIp) as AIP by _timeslice

| outlier AIP window=5, consecutive=1, threshold=2, direction=+-

Pretty Right?

To Summarize

SIEMs are huge databases of important log data.

You can query them to find specific things, (IP addresses), trends (attacks over time) and so much more.

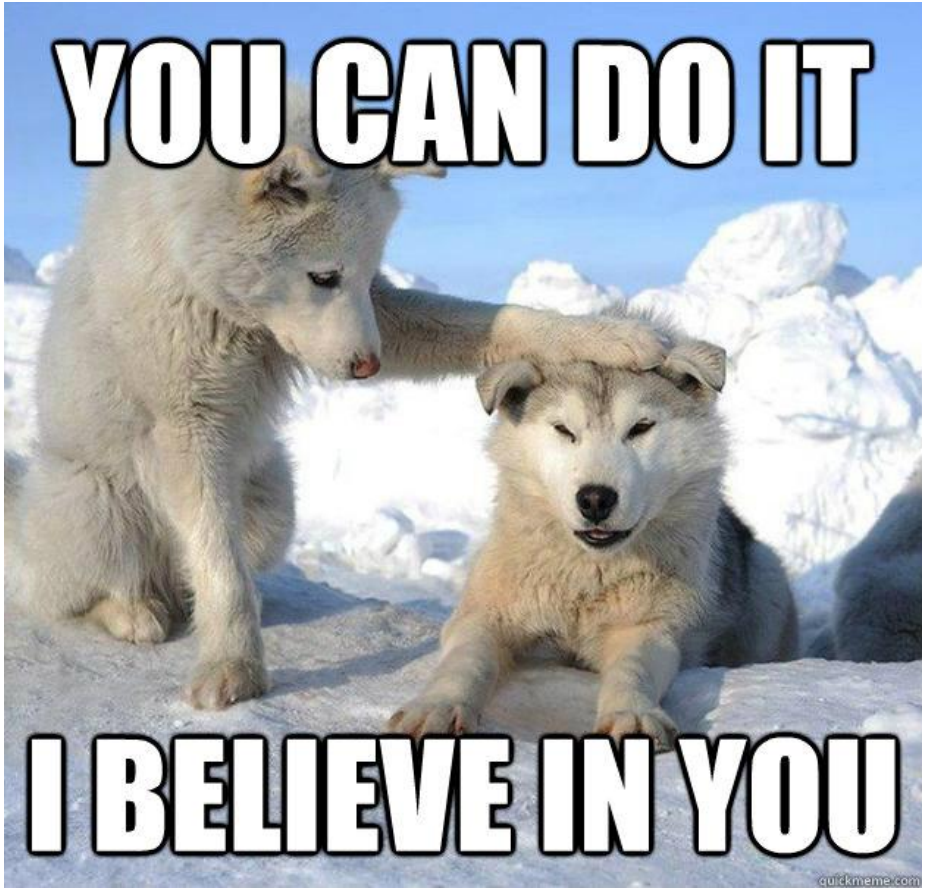
Lab Time!

If you want to get a good foundation in querying:

https://tinyurl.com/SumoCore

If you have a good grasp of SQL/Querying and/or are only here to look at security suff:

https://tinyurl.com/SumoSec



Announcements

Working on an interesting project? Have a specialty? Present

If you are interested in a topic/want to present email us!

cyberdefenseorg@albany.edu

J-Board Applications!

OPEN POSITIONS:

Treasurer
IT-Chief Technology Officer
Competition Captain
Competition Co-Captain

EVERYONE SHOULD APPLY (:

Certification Study Group - Security +

Tuesday nights at 7:15 in bb123.

Study as a group

Talk to Mark

Other Updates!

Cyber Jobs week is coming up:

RSVP:
https://doodle.com/poll/7crgg264hbkgzdy8

Send Resumes in for critique.

"Our second Cyber Jobs Fair is scheduled for March 6, 2019.

10:00 – 12:00: Company Pitches (Location: TBA)

Pizza will be available for students around 11:30

12:00 – 3:00: Student Interaction with Employers / Business Building Living Room

Please fill out the Doodle Poll to RSVP for the Cyber Jobs Week by Tuesday 2/22. By RSVPing you are enabling us to create your name tags and order a sufficient amount of food. The final list of attendees will be compiled on 2/24."

Cya Next week!

If you have any good memes send them to the email below.

wcsmith@albany.edu

Follow us on Twitter? Add on myInvolvement?

PC Assembly Workshop- February 19th(?)

CCDC! - Mondays 7:30-9:00pm

BB123 (Check email).

MyInvolve

Twitter

Discord

https://discord.gg/9Dh6R5R