



Threat Hunting

Sam Bowne
Oct 26, 2020

Who

- Sam Bowne
- Twitter: **@sambowne**
- Instructor, City College San Francisco
- Founder, Infosec Decoded, Inc.
- All slides, lecture videos, projects, etc. free at
 - **samsclass.info**
- All classes free online worldwide



CNIT 50: Network Security Monitoring

Spring 2020 Sam Bowne



Course Description

This course teaches you how to search and navigate in Splunk, use fields, get statistics from your data, create reports, dashboards, lookups, and alerts. Scenario-based examples and hands-on challenges will enable you to create robust searches, reports, and charts. It will also introduce you to Splunk's datasets features and Pivot interface.

Boss of the SOC v1

Threat Hunting with Splunk

Google for Log Data

The screenshot shows the Splunk Enterprise web interface. The browser address bar displays `splunk.samsclass.info:8080/en-US/app/launcher/home`. The interface includes a top navigation bar with the Splunk logo, a search icon, and menu items for Messages, Settings, Activity, and Help. A left sidebar lists available applications: Search & Reporting, Splunk Add-on for Tenable, and Splunk Stream. The main content area, titled "Explore Splunk Enterprise", features two prominent links: "Product Tours" (with a binoculars icon) and "Search Manual" (with a magnifying glass icon). Below these links are descriptive text blocks: "New to Splunk? Take a tour to help you on your way." and "Use the Splunk Search Processing Language (SPL).".


splunk>enterprise


Messages Settings Activity Help

Apps

- Search & Reporting
- AddOn+ Splunk Add-on for Tenable
- STM Splunk Stream

Explore Splunk Enterprise

 **Product Tours**
New to Splunk? Take a tour to help you on your way.

 **Search Manual** [\[↗\]](#)
Use the Splunk Search Processing Language (SPL). Use F

Search | Splunk 7.2.4

splunk2.samsclass.info/en-US/app/search/search

splunk > enterprise App: Search & Reporting 2 Messages Settings Activity Help Find

Search Datasets Reports Alerts Dashboards Search & Reporting

Search

1 | enter search here... Last 24 hours

No Event Sampling Verbose Mode

How to Search

If you are not familiar with the search features, or want to learn more, see one of the following resources.

[Documentation](#) [Tutorial](#)

What to Search

956,045 Events INDEXED	4 years ago EARLIEST EVENT	2 years ago LATEST EVENT
----------------------------------	--------------------------------------	------------------------------------

[Data Summary](#)

Data Summary



Hosts (8)

Sources (31)

Sourcetypes (23)



Sourcetype		Count	Last Update
wineventlog		113	8/24/16 11:20:29.000 AM
wineventlog		87,430	8/24/16 11:27:41.000 AM
wineventlog		182	8/24/16 11:27:27.000 AM
WinRegistry		74,720	8/24/16 11:27:42.000 AM
XmlWinEventLog:Microsoft-Windows-Sysmon/Operational		270,597	8/24/16 11:27:40.000 AM
fgt_event		57	8/24/16 11:25:51.000 AM
fgt_traffic		55,279	8/24/16 11:27:44.000 AM
fgt_utm		25,586	8/24/16 11:27:14.000 AM
iis		22,615	8/24/16 9:38:01.000 AM
nessus:scan		65	8/24/16 9:34:37.000 AM

Data Summary



Hosts (8)

Sources (31)

Sourcetypes (23)



Sourcetype		Count	Last Update
stream:icmp		12,858	8/24/16 11:17:35.000 AM
stream:ip		62,111	2/8/19 5:49:10.000 PM
stream:ldap		344	8/24/16 11:18:37.000 AM
stream:mapi		7,025	8/24/16 9:37:58.000 AM
stream:sip		12	8/24/16 9:34:24.000 AM
stream:smb		151,568	8/24/16 11:27:38.000 AM
stream:snmp		12	8/24/16 9:33:51.000 AM
stream:tcp		28,330	2/8/19 5:49:41.000 PM
stream:udp		1	2/8/19 5:45:44.000 PM
suricata		125,584	8/24/16 11:27:43.000 AM

Demonstration

Boss of the SOC v1: Threat Hunting with Splunk

- <https://samsclass.info/50/proj/botsv1.htm>