

---

# DEV/SECOPS BOOTCAMP

BUILDING RUGGED SOFTWARE

YEAR ONE / WEEK FOUR/ LESSON ONE

---

# Agenda

- Splunk Basics
  - Why Splunk?
  - What is an index
  - Data classification
- Splunk commands

---

# Splunk Basics

- Why Splunk?
  - De facto log aggregation and analysis tools
  - Enables us to
    - monitor for security threats across disparate environment
    - analyze and identify anomalous behavior
    - automate initiation of incident response procedures
    - build metrics to visualize our resource
    - Correlate data streams to discover meaningful security events

---

# Splunk Basics

- What is an Index?
  - A bucket of data, commonly logs
  - Default index is main, e.g., `index=main`
- What can you do with an index?
  - Separate and query data type or classification
  - Access controls to data
  - Retention policy, by time or size
  - Performance tuning, sharding

---

# Splunk Basics

- Data classification
  - Index – data bucket
  - Source – where the data came from, e.g., `/var/log/messages`
  - Sourcetype – the data type, often auto detected by Splunk
    - Splunk will attempt to automatically detect the source type based on predefined patterns

# Splunk Basics

The screenshot shows the Splunk Enterprise web interface. At the top is a navigation bar with the Splunk logo, user 'student1', and links for Messages, Settings, Activity, and Help. A search bar is on the right. On the left is a sidebar with 'Apps' and a gear icon. The 'Search & Reporting' app is highlighted with a red box. The main area is titled 'Explore Splunk Enterprise' and contains four tiles:

- Product Tours**: New to Splunk? Take a tour to help you on your way.
- Search Manual**: Use the Splunk Search Processing Language (SPL).
- Pivot Manual**: Use Pivot to create tables and charts with SPL.
- Dashboards & Visualizations**: Create and edit dashboards using interactive editors or simple XML.

A 'Close' button is visible in the top right of the main content area. At the bottom of the main content area, there is a dashed box containing a bar chart and a line graph.

# Splunk Basics

The screenshot shows the Splunk Search & Reporting interface. At the top, there's a navigation bar with the Splunk logo, 'App: Search & Reporting', and user options like 'student1', 'Messages', 'Settings', 'Activity', and 'Help'. Below this is a green bar with tabs for 'Search', 'Pivot', 'Reports', 'Alerts', and 'Dashboards'. The main search area has a large search bar with the placeholder text 'enter search here...'. To the right of the search bar are buttons for 'Last 4 hours' and a search icon. Below the search bar, there's a dropdown menu for 'No event Sampling' and a 'Smart Mode' button.

## How to Search

If you aren't familiar with searching in Splunk, or want to learn more, checkout one of the following resources.

[Documentation](#)

[Tutorial](#)

## Search History

[Expand your search history.](#)

## What to Search

1,596,412 Events  
INDEXED

6 years ago  
EARLIEST EVENT

a few seconds ago  
LATEST EVENT

[Data Summary](#)

# Splunk Basics

**splunk** App: Search & Reporting student1 Messages Settings Activity Help Find

Search Pivot Reports Alerts Dashboards Search & Reporting

## New Search

index=main | Last 4 hours

31,037 events (6/15/16 3:27:00.000 PM to 6/15/16 7:27:56.000 PM) No Event Sampling

Events (31,037) Patterns Statistics Visualization

Format Timeline Zoom Out Zoom to Selection Deselect 1 minute per column

List Format 20 Per Page

< Prev 1 2 3 4 5 6 7 8 9 ... Next >

< Hide Fields All Fields

Selected Fields

- host 3
- invalid\_username 28
- remote\_host 6
- source 4
- sourcetype 4

Interesting Fields

i	Time	Event
>	6/15/16 7:27:49.775 PM	type=PATH msg=audit(1466018869.775:373532): item=0 name="/var/log/wtmp" inode=265128 dev=ca:01 mode=010066 4 ouid=0 ogid=22 rdev=00:00 obj=system_u:object_r:wtmp_t:s0 nametype=NORMAL host = ip-10-0-0-45   source = /var/log/audit/audit.log   sourcetype = linux_audit
>	6/15/16 7:27:49.775 PM	type=CWD msg=audit(1466018869.775:373532): cwd="/" host = ip-10-0-0-45   source = /var/log/audit/audit.log   sourcetype = linux_audit
>	6/15/16 7:27:49.775 PM	type=SYSCALL msg=audit(1466018869.775:373532): arch=c0000003e syscall=2 success=yes exit=3 a0=403844 a1=1 a2=2 a3=8 items=1 ppid=1 pid=25267 audit=4294967295 uid=0 gid=0 euid=0 suid=0 fsuid=0 egid=0 sgid=0 fsgid=0 tty=(none) ses=4294967295 comm="agetty" exe="/sbin/agetty" subj=system_u:system_r:getty_t:s0 key="session" host = ip-10-0-0-45   source = /var/log/audit/audit.log   sourcetype = linux_audit



---

# Splunk Commands

- Splunk Search
  - Retrieves events from indexes
  - Filters results of a previous search
  - Uses Search Processing Language
  - Implicit command when a search is performed or can be used further filter search results, e.g., `index=main sourcetype=linux_secure| search field=value`

---

# Splunk Commands

- Field Extraction
  - Key value pairs extracted by Splunk during a search
  - Field creation by custom field extraction commands
  - Commands used to perform field extraction: rex, extract, stats, etc.

---

Questions?

---

# Lab 1

- If you weren't here last week team up with someone who was or quickly do week 3 lab 2 (get AWS credentials from Instructor)
- If you were here last week:
  - Login into AWS, start your instance and note your public IP address (it may have changed)
  - SSH into your instance cd into railsgoat directory and run
    - `export RAILS_ENV=mysql`
    - `bundle exec rake db:setup`