DEVSECOPS BOOTCAMP

BUILDING RUGGED SOFTWARE

YEAR ONE / WEEK FOUR/ LESSON ONE

Copyright © DevSecOps Foundation 2015-2016

Agenda

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

Copyright © DevSecOps Foundation 2015-2016

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

Copyright © DevSecOps Foundation 2015-2016

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

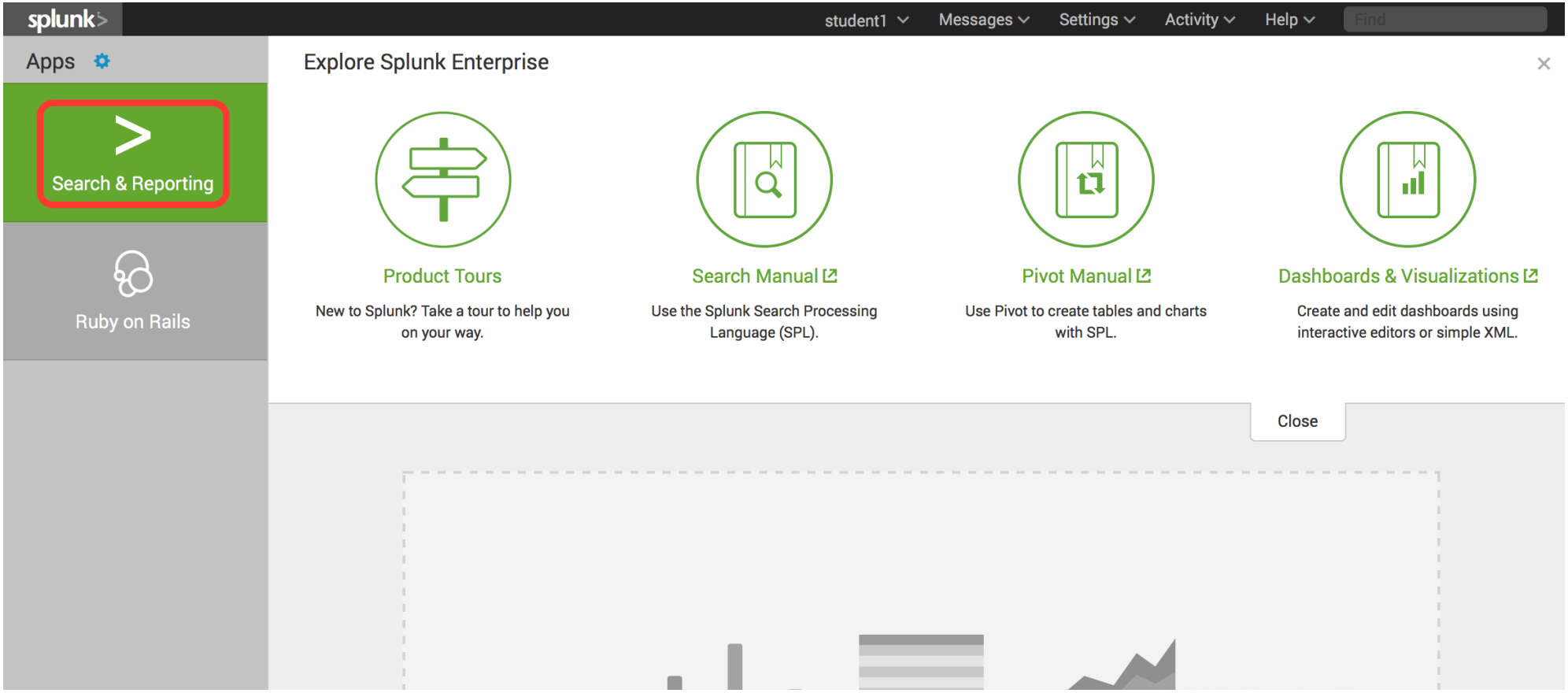
Copyright © DevSecOps Foundation 2015-2016

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

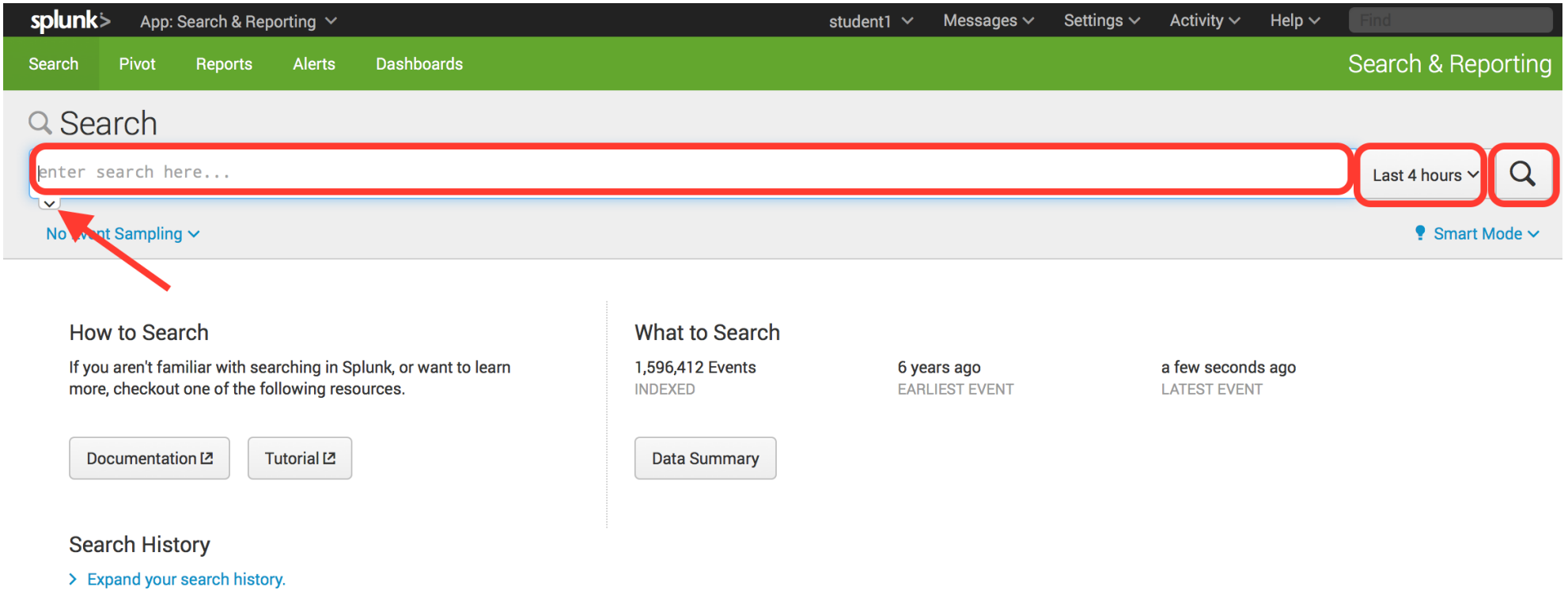
Copyright © DevSecOps Foundation 2015-2016

Splunk Basics



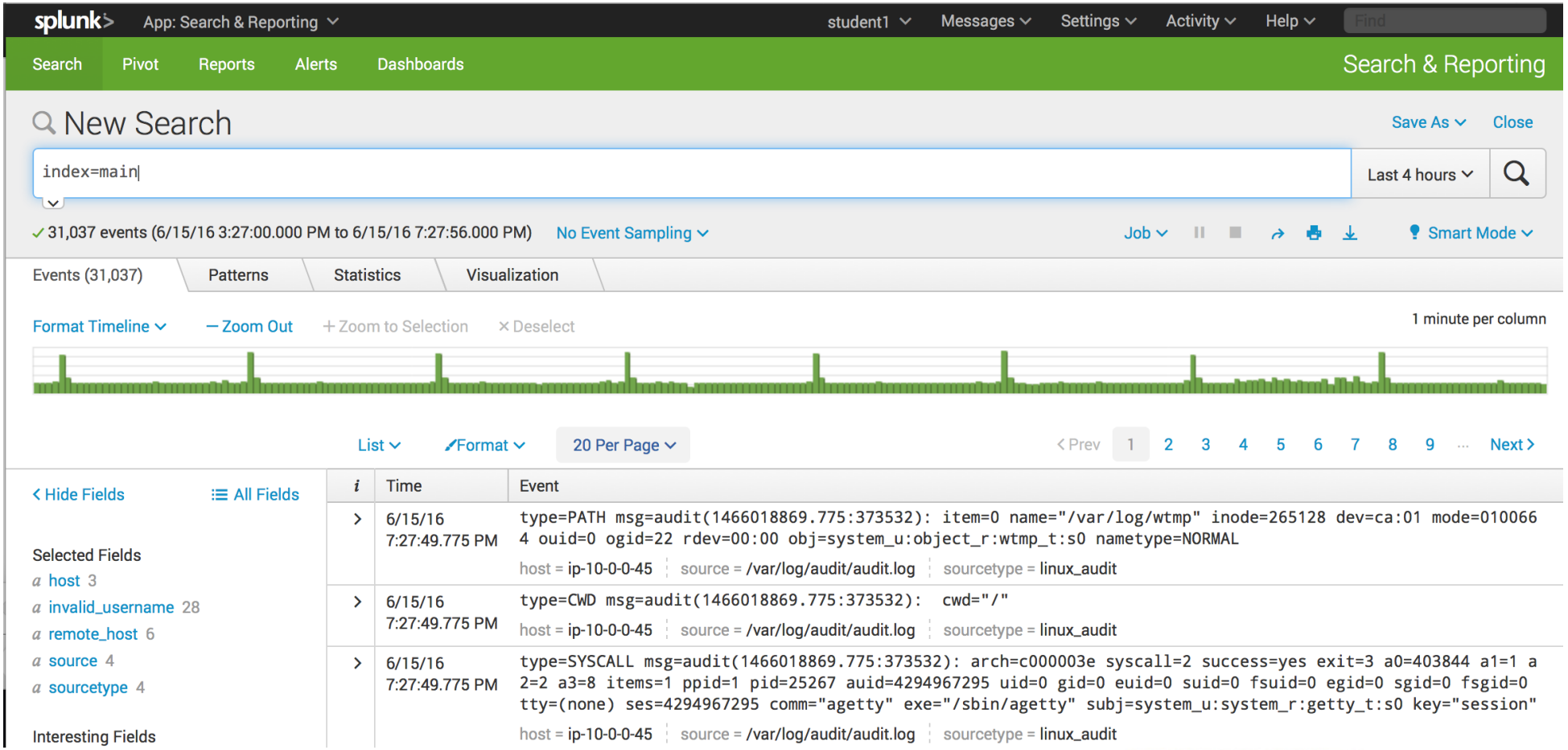
Copyright © DevSecOps Foundation 2015-2016

Splunk Basics



Copyright © DevSecOps Foundation 2015-2016

Splunk Basics



Copyright © DevSecOps Foundation 2015-2016

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`

Copyright © DevSecOps Foundation 2015-2016

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.

Copyright © DevSecOps Foundation 2015-2016

Questions?

Copyright © DevSecOps Foundation 2015-2016

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

Copyright © DevSecOps Foundation 2015-2016