Lab 0

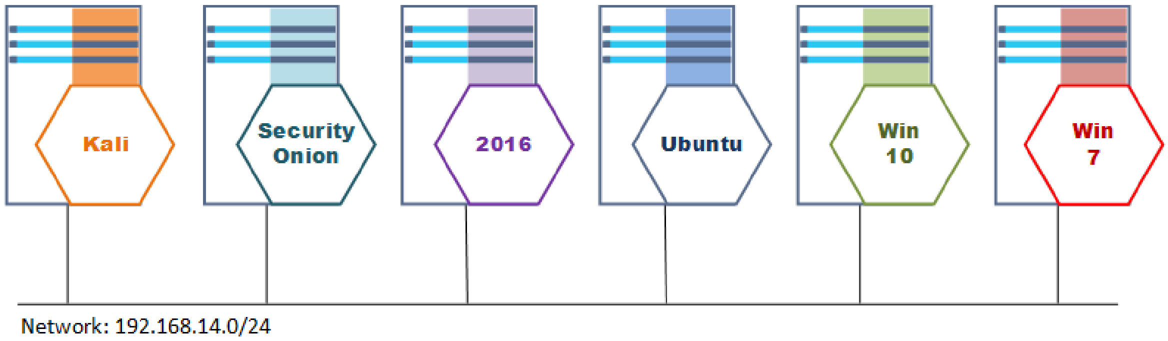
Governance, Risk Management and Compliance (GRC)

Summary:

This workshop addresses the knowledge and skills need to students to be prepared for the Qualified Security Assessor (QSA) exam. A Qualified Security Assessor is a person who has been certified by the PCI Security Standards Council to audit merchants for Payment Card Industry Data Security Standard (PCI DSS) compliance.

The GRC workshop will teach you how to perform assessments of merchants and service providers who must comply with the PCI Data Security Standard. The course focuses on the 12 high level control objectives and corresponding sub-requirements that are required for compliance. Split into two parts, the course consists of an online component and a two-day instructor-led session.

Lab Setup:



Machine Name	IP Address	Username	Password
Kali	192.168.14.5	root	toor
Security Onion	192.168.14.201	sysadmin	Password123
WinServer2016(std)	192.168.14.105	Administrator	Password123
Ubuntu Desktop	192.168.14.67	sysadmin	Password123
Windows 10	192.168.14.28	Student	Password123
Windows 7	192.168.14.89	Student	Password123

Lab Visual Queue:

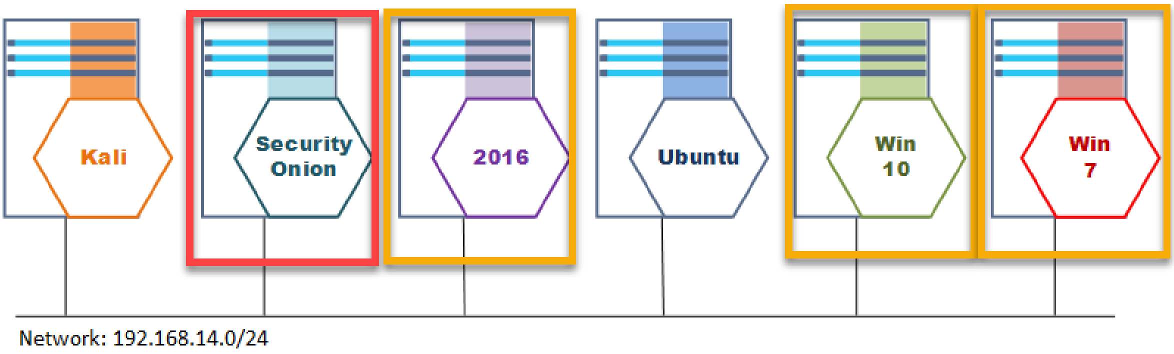
In the labs a YELLOW square around a machine identifies a machine that is being audited.

- If parsing logs, this is the machine that is generating the log files
- If scanning, this is the machine that is being tested for compliance.

In the labs a RED square around a machine identifies a machine that is being used by an auditor.

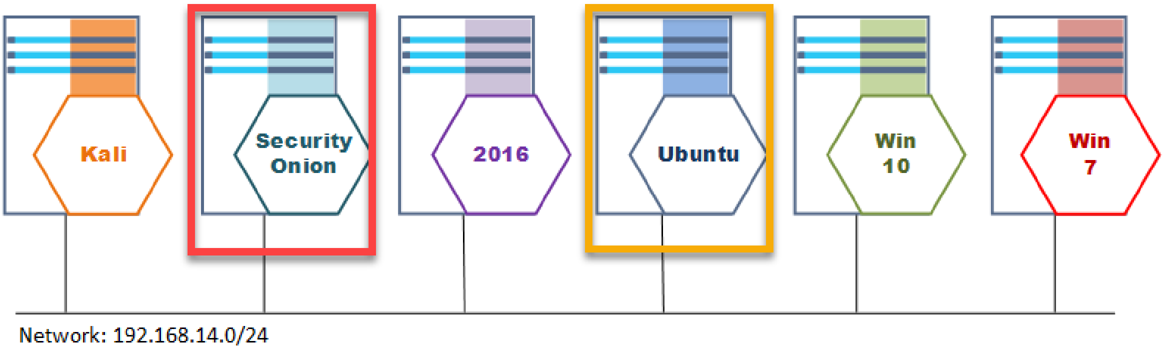
- If parsing logs, this is the central log collector (Security Onion in our case)
- If scanning, this is the security scanner (Kali Linux in our case)

Ex:
In this example Security Onion received log file data from Win2016, Win10, and Win7.

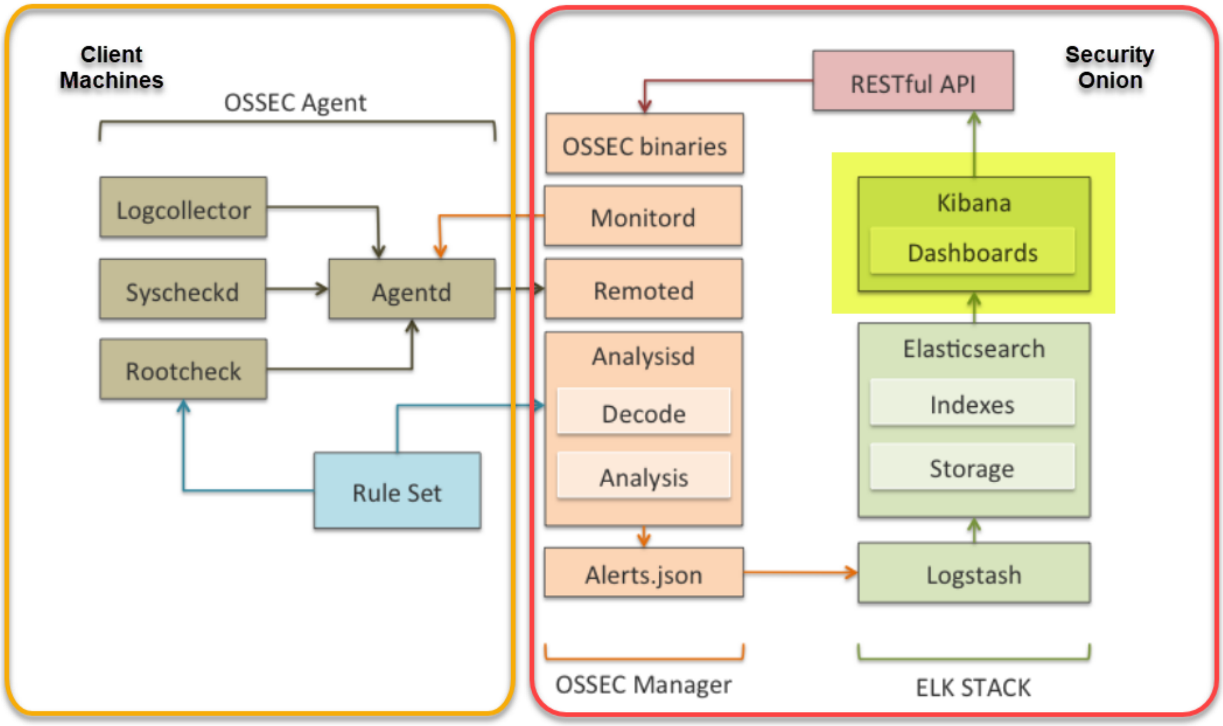


Ex:

In this example the Kali Linux machine is scanning the Ubuntu machine for firewall compliance.



The setup we are using to get visibility into the logs and configuration data is Security Onion. The OSSEC Agent (Wazuh) in the graphic is a Host Intrusion Detection System (HIDS) that runs on each of the machines in your network. The logs from this agent are sent to Security onion where they are processed, stored and indexed for fast search. The only part in this graphic that we will actually be interacting with is Kibana.



Kibana:

We need to do some fundamentals of Kibana to understand how the filters we use work and how to apply them in Kibana.

Kibana is an open source analytics and visualization platform designed to work with Elasticsearch. You use Kibana to search, view, and interact with data stored in Elasticsearch indices. The combination of Elasticsearch, Logstash, and Kibana is referred to as the "Elastic Stack" (formerly the "ELK stack").

Note: Some of the visualization plugins are not configured on our lab machine and are outside the scope of what we need to know here.

Get Started

1. To get started, in Security Onion you want to click the Kibana Icon on the desktop.

   Username: student
   Password: student

Bug:

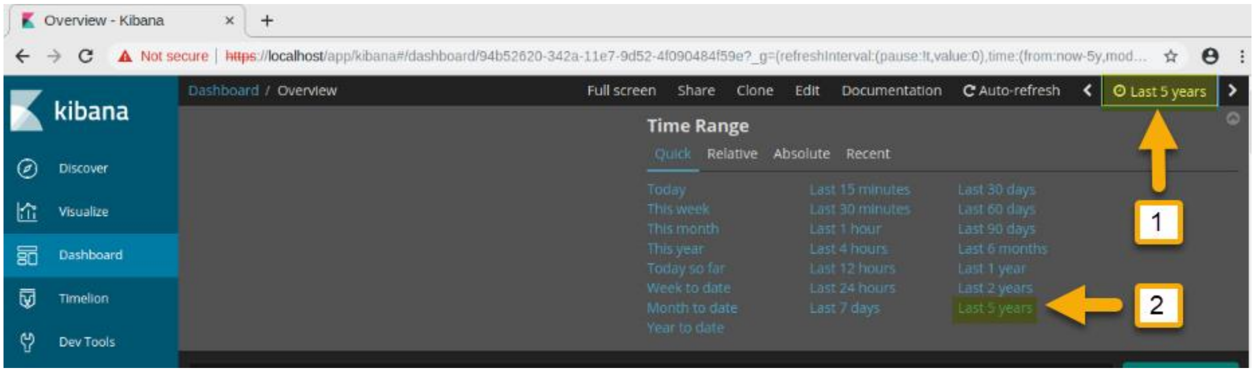
What went wrong:

- Make sure Kibana is running

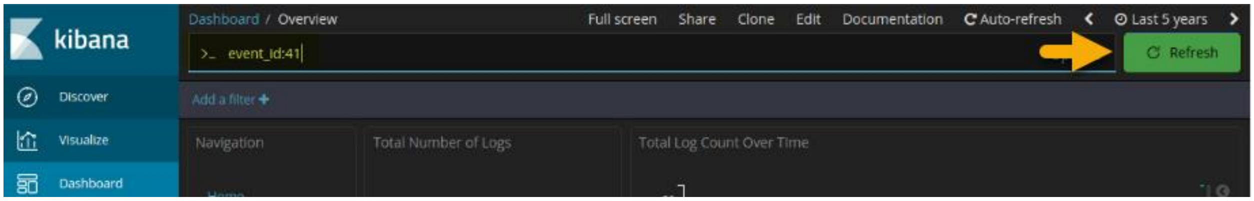
  ```
  sudo so-kibana-start
  ```

- Make sure to check the data range in the upper right corner. This defaults to 24hrs and what you are looking for may be outside that range. Tip: Try using “Year to date”
- If you have a spelling error anywhere in your search string the result simply matches nothing (no warning)
- When you combine search strings the ‘AND’ must be uppercase

2. Once the default “Dashboard” is open the first thing we want to do is set the date range so we can look at all of the logs that are stored in the database. Note: We are looking at all records, normally you would set this date to match the time period required by your audit. You can also change this to look for specific date ranges depending on what you are trying to do as you go along.



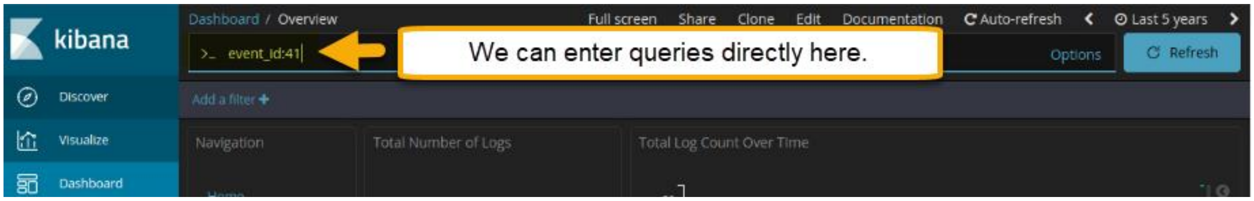
3. Next click the refresh button in the upper right corner. This will tell Kibana to update the records (if you are trying to add new events to the lab systems you will want to do this after causing a system to write to its log (there may be a short, few minutes delay)



event_id:41

Filtering (Type it in):

4. At this point we can start trying to type in some queries just to see how they work
   Try this one:
   - . event_id:41

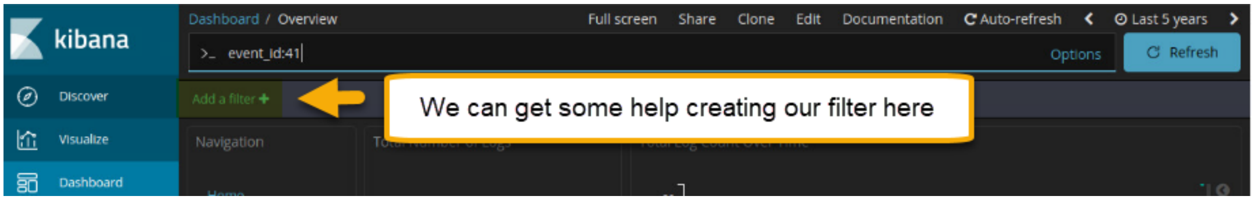


event_id:41

We can enter queries directly here.

Filtering (Use the Wizard):

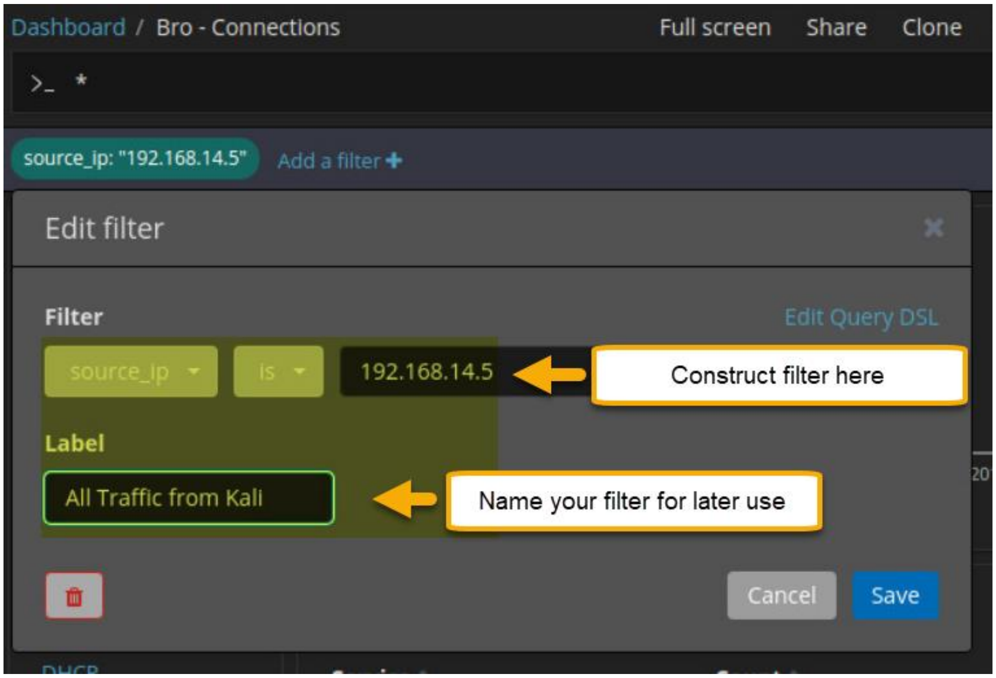
5. We can also use the “Add a filter” tool to walk through selecting a filter



>_ event_id:41

We can get some help creating our filter here

You can name and save useful filters:



>_ *

source_ip: "192.168.14.5"

source_ip is 192.168.14.5

Construct filter here

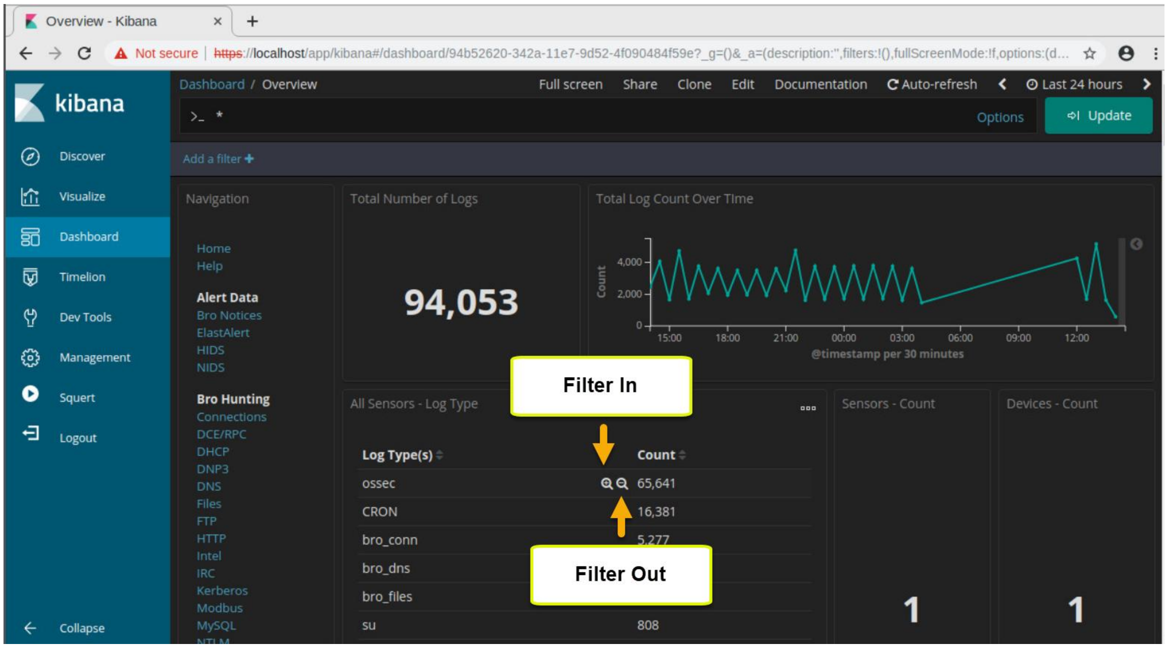
Label: All Traffic from Kali

Name your filter for later use

Filtering (Drill down):

6. When you hover over any of the fields that you can filter by, 2 small magnifying glass will pop up (one with a “+” and one with a “-”)
   - + = Look for all records containing this value in this field
   - - = Look for all records that do not contain this value in this field.

   Click the “Filter in” magnifying glass

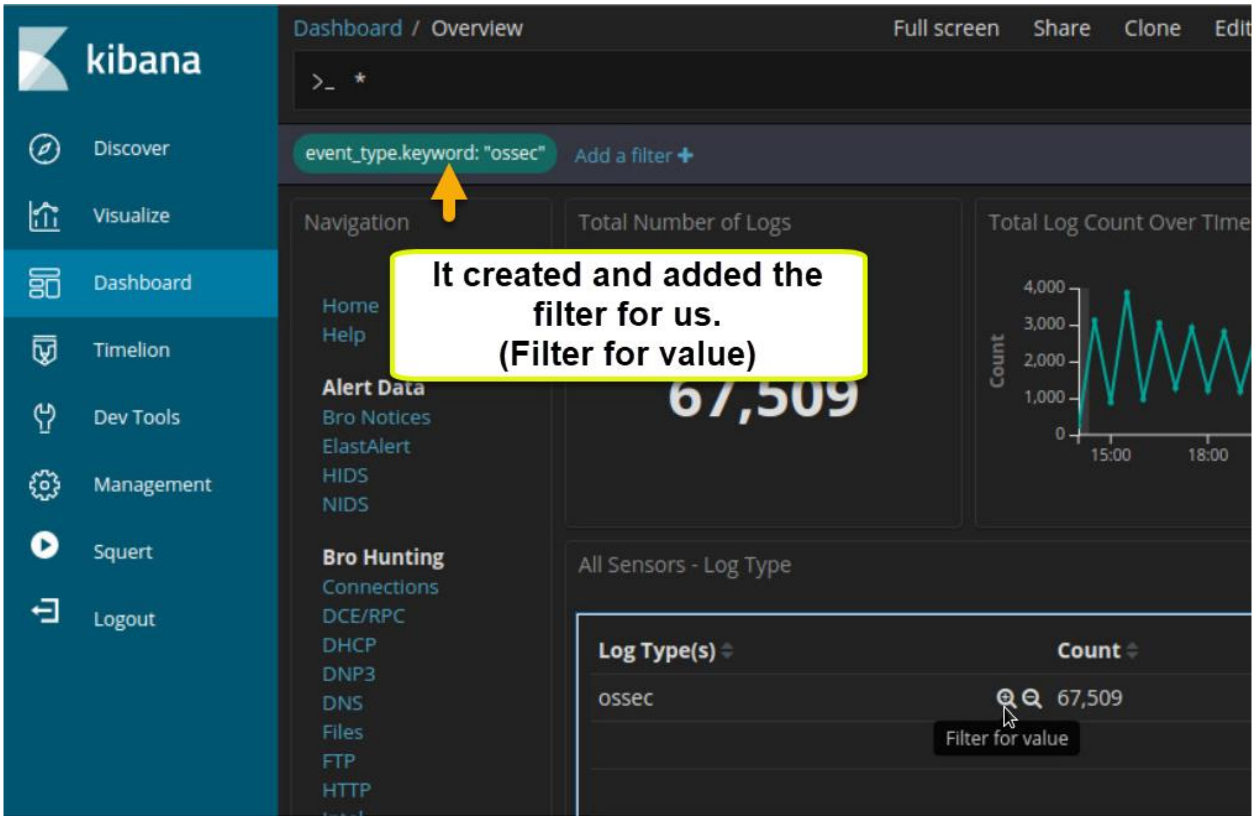


Log Type(s)	Count
ossec	65,641
CRON	16,381
bro_conn	5,277
bro_dns	
bro_files	
su	808

Filter In

Filter Out

It ran the “Add a filter +” Wizard for us and added the filter to bar.

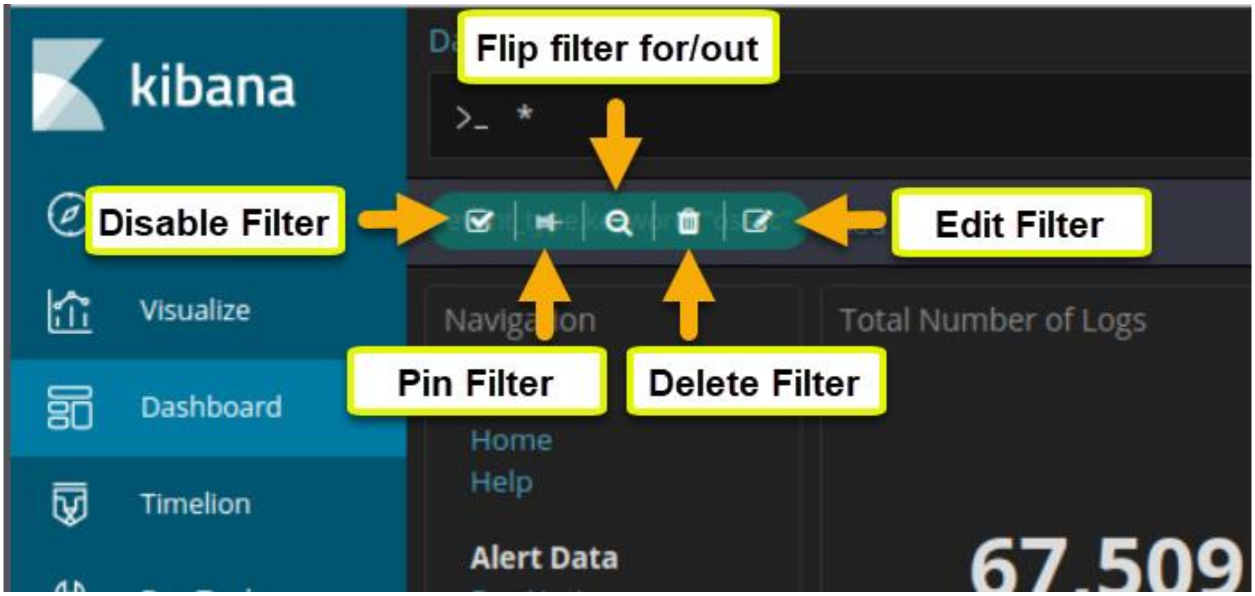


Log Type(s)	Count
ossec	67,509

It created and added the filter for us. (Filter for value)

Filtering (Edit/Delete/Disable):

7. To edit or delete any filter you just hover over the filter in the “Add a filter” bar.



This should be enough to allow you to go through most of the labs. We will demo specific searches as needed for the lab.