**Splunk Specially designed for Logs Monitoring Tool.**

**It is Ultimate Solution for Log Processing.**

**Why need for Explore Logs?**

**Logs are very important today’s which are running the business through internet.**

**Example:**

**Edureka! It is running the business over the internet**

**Basically, they are having lot of Server same they are having lot of logs who are all access their website.**

**Logs are generating inside the server.**

****

**Even System have Logs which will be stored in one location and one directory**

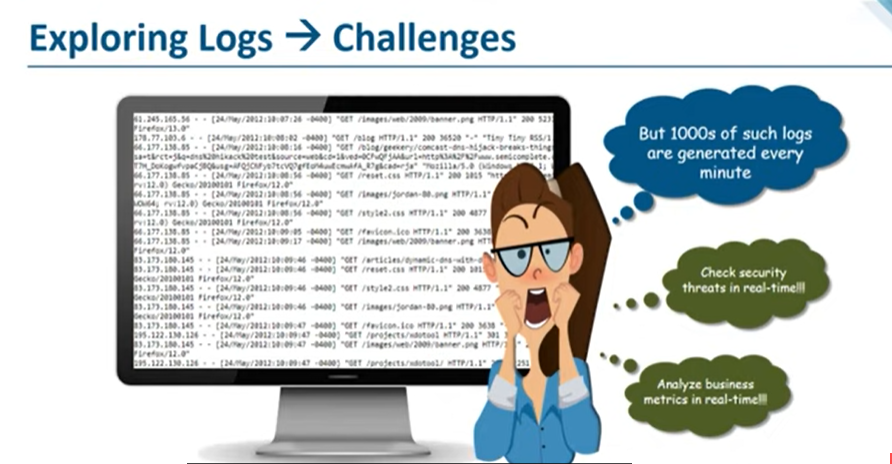
**But challenging we unable to read the log because which are unreadable format.**

**But we have something important over the logs for every single transaction.**

**For Improving Operations is called as operational intelligence the solution is everything hidden in our logs.**

**Now a days internet is ruling this is most important we must follow the logs.**

**Understanding the logs are not easy?**

****

**Logs are Mostly not in human readable Form.**

**There is Some Security Breach We should know the problem.**

**We need to check the logs, but real time logs generate Massively.**

**Almost 1000 Lines of get generated in every single minutes.**

**Example:**

**Web Server of e-commerce company like Flipkart, Amazon .com**

**Every single user has hit the browser everything will generate in logs like Customer IP address along with that whatever clicks and whatever links they open. Everything will store in logs at server.**

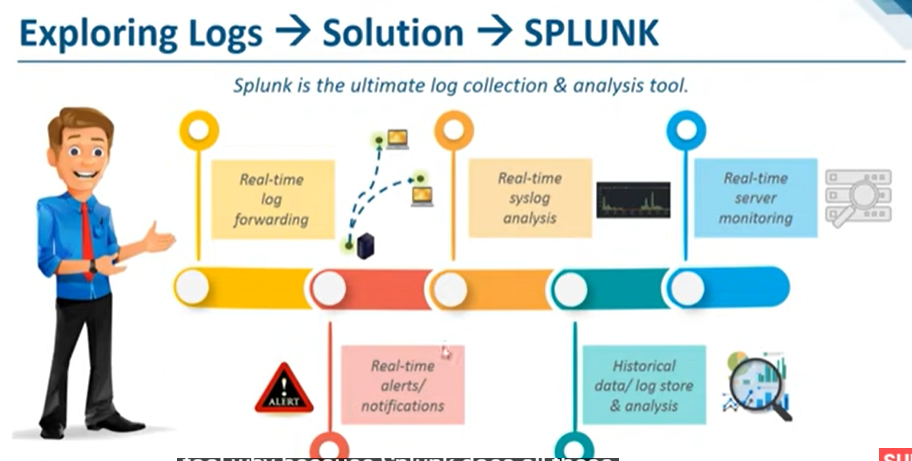
**If there is security breach, we need to arrest issue then how it possible to instantly arrest the issue**

**It is impossible to arrest issue suddenly.**

**“For this Case”**

**We need a tool to understand our logs , which is very Simple manner .**

**So, that’s why to use “SPLUNK MONITORING TOOL”**

****

**Splunk is the ultimate log collection & analysis tool.**

**Because Splunk does all this thing**

**Real – Time Log Forwarding:**

**Splunk does real time log forwarding which means collect log from one instance/server and forward those logs to the remote instance.**

**It makes a job lot of easy to handle the issue.**

**Real-Time Sys Logs Analysis:**

**Splunk does syslog’s analysis like server log analysis**

**Real-time server Monitoring:**

**We can Monitoring how many peoples are there in website**

**What action are they trying to perform?**

**E-Commerce they are trying the TARGET MARKETING and RETARGETING**

**So, everything happens based on inside the customer behavior.**

**Based on the customer behavior they give the offer to customer.**

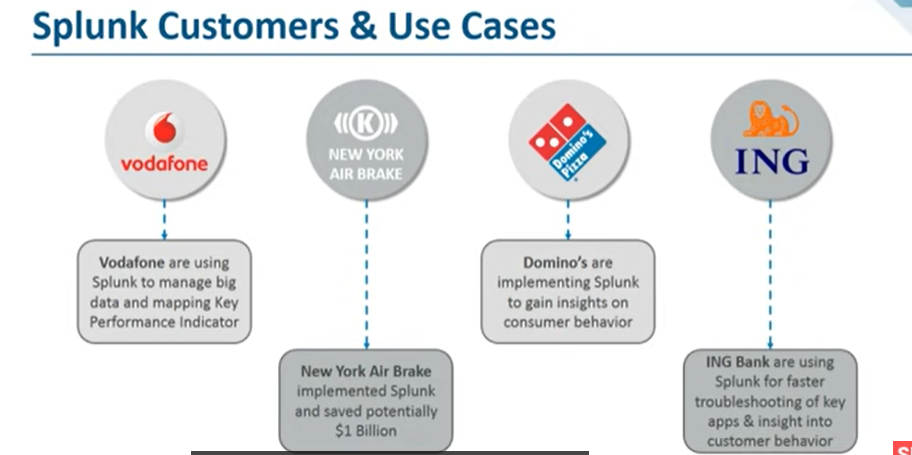
**And we can analysis security threat too.**

**Real – time alerts / notification :**

**When System crossed CPU utilization threshold that time notification will send to the Receiver.**

**Historical data / log store & analysis:**

**Every log will store in index**

****

**=================================================================================**

**Logs Monitoring Tool**

**Splunk, does it monitor the overall infrastructure.**

**Below Mentioned LOGS:**

* **Application**
* **Network**
* **Database**
* **Security**
* **Storage**
* **Server**

**It will view the logs in that Splunk Dashboard**

**Here we are creating the Master and Slave Concept**

**Mostly It is used for Banking.**

**For Root Analytics we are used to viewing the Logs.**

**Proactive / Reactive**

**Proactive-We analytics the Problem before which will occur.**

**Reactive-We analytics the Problem after which will occur.**

**Splunk which is monitoring the Overall Infrastructure (entire Logs).**

**In Realtime Developers will define the logs file(FS) path.**

**For Example, below :**

1. **/var/log/server.log**
2. **/var/lib/sysapp.log**
3. **Var/log/generalquerry.log**
4. **Var/log/event.log**

**Above mentioned path we able to view Manually it is very difficult to analysis the problem .**

**Therefore, we are going to use Splunk in real time for easily analysis the Root Cause.**

**So, this kind of FS will be Creating the developer.**

**For this case , we identify logs files system in Splunk , then Splunk will trigger the logs and it will generate in Dashboard.**

**So, we can easily find out the accurate Report.**

**We assign the alert .**

**Once alert will generate which is send notification to Receiver . So that we easily find out the issue Pro-actively before problem occur.**

**Example Alert:**

**Alert : Count issue (db catalog >=5)**

**Similarly, if we are using traditional method, it will take longer time to analysis the problem.**

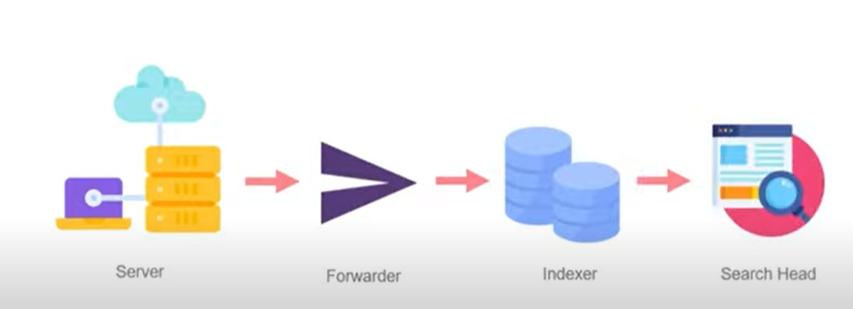
**Likely , if we are using the Splunk . we able to investigate the Problem Shortly.**

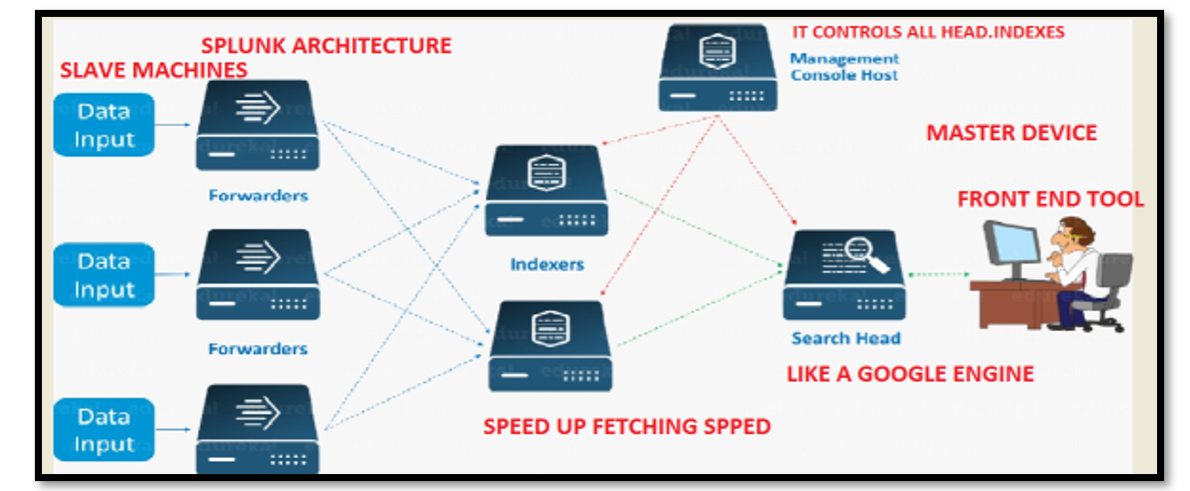
**Therefore, we able to sustain the system like**

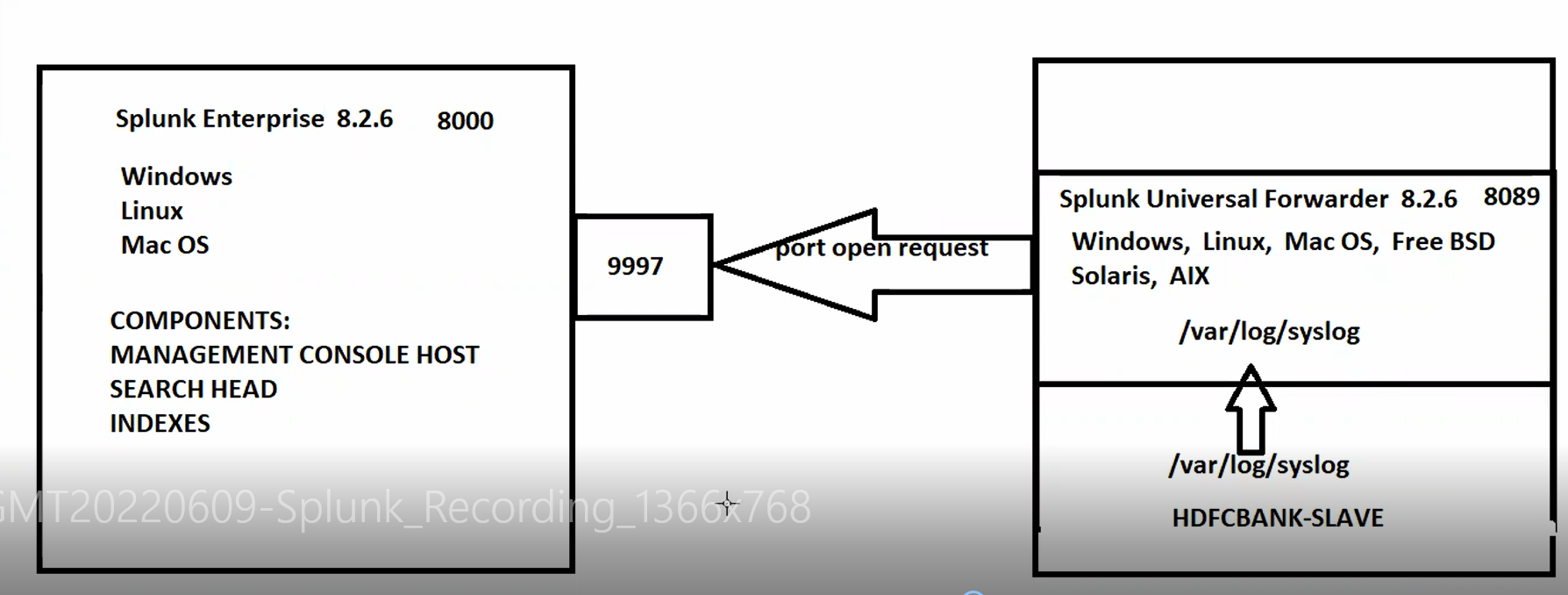
**Stability, Reliability, Availability, Durability**

**It will automatically improve.**

**for this method generally called as CSI – Continual Service Improvement.**







**Pre-Requesting:**

**Splunk it is Enterprise Tool which is free for 60 days**

**Step-1**

**Splunk.com (60 days Free trial)🡪free trail-> Create the Account in Splunk**

**Login into Splunk 🡪download the free trail package->Splunk enterprise->**

**Step-2**

**We launch two servers in ec2 one is Master and another one is Slave (ubuntu)**

**Login in the Master**

**Cd /opt**

**#ls -lrt**

**Then go to Splunk login page**

**(Splunk Master only run-in windows,Linux,MacOS)**

**Click 64 bit download tar.gz🡪 Copy wget Link.**

**Then go to server**

**#cd /opt**

**#wget (link)**

**#tar -xvzf splunk tar file**

**#ls -lrt**

**#cd splunk**

**#ls -lrt**

**Important directory Bin.**

**#cd bin**

**#ls**

**Now we are going to run the Splunk in Script Format.**

**#./splunk start**

**Now it is showing license and agreement . it is only 60 days trail**

**Click tab (until 100%)**

**Click “Y”**

**Create Splunk master username and password**

**Now we able to view Splunk master port number “8000”**

**Now go to chrome**

**Publicid:portnumber**

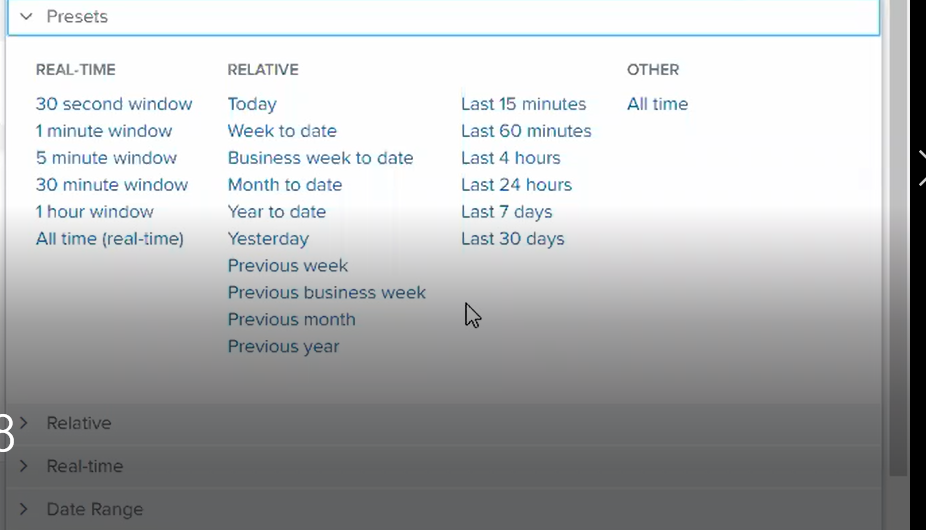
**Example 192.10.8.1:8000**

**Login in the Splunk**

**Overview of Splunk Console:**

**Now we able to view the Management Console Host**

**Search Reporting head🡪we able to view the search box**

****

**We can take log above mentioned optional.**

**Settings🡪indexes (We able to view number of indexes same we have option to customize the indexes too.)**

**Now go to Slave.**

**#cd /opt**

**#apt-get update**

**Then go to splunk page**

**We able to see Universal Forwarder**

**(Slave we able to run ( windows,Linux,MacOS,Free BSD,Solaris,AIX))**

**Click linux 🡪 Click .tgz (download now) 🡪 Copy Wget link**

**Then log into Slave Server.**

**#wget (link Past)**

**#tar -xvzf Splunkforwarded**

**#ls -lrt**

**#cd /bin**

**#./splunk start - -accept-license**

**#set up the username and password**

**Then we able to view Splunk forwarded port number : “8089”**

**Port Open Request:**

**The Slave universal Forwarded will be creating the Port 9997 . It has used this port then push logs to Master Server.**

**Go to slave Server**

**Step 1:**

**Navigate to /opt/splunkforwarder/bin**

**#cd /opt/splunkforwarder/bin**

**#./splunk add forward-server masterpublicid:9997**

**Example: #./splunk add forward-server 192.186.2.0:9997**

**#Splunk username: <slave username>**

**#password:<password>**

**Step2:**

**Take Logfile:**

**Open WinSCP**

**\*Transfer log file ( local PC to Slave server)**

**then go to slave machine**

**go to home ubuntu page**

**#ls**

**file will show ( Syslog)**

**then copy the files to path /var/log**

**#cp syslog /var/log**

**#cd /var/log (/var/log/syslog – Universal log Path)**

**Then go to push the log slave to master**

**#cd /opt/splunkforwader/bin**

**# ./splunk add monitor /var/log/syslog -index main -sourcetype slavelogs**

**Then it shows Added Monitor of ‘var/log/syslog’**

**Then go to master Server:**

**Go to bin path**

**./splunk enable listen 9997**

**#Splunk username: <master username>**

**#Password: <master password>**

**Now it shows “Listen has been Successfully”**

**Then go to Splunk Console.**

**Go to search🡪 index=”main”**

**Log will come in console**

**Statistics**

**==================================================================================**

**If incase we want to setup the disk error issue:**

**#cd /opt/splunk/etc/system/local**

**#vi server.conf**

**disk usage processor settings**

**[disk usage]**

**minfreespace = 50**

**pollingfrequency = 100000**

**pollingtimeFrequency = 10**

**here we need to edit the minfreespace 50 instead of 5000**

**esc**

**:wq!**

**Changing the splunk Port**

**Go to master Server:**

**Cd /opt/splunk/bin**

**./splunk set web-port 10000**

**./splunk restart**

**sql**

**index="main" | table \_time sourcetype (which is showing time and source type)**

**Tables Command**

**index="main" | table \_time "sourcetype" "date\_hour"**

**Rename Command (rename the field for own understanding)**

**index="main" | table \_time "sourcetype" "date\_hour" | rename date\_hour as hours**

**field Command ( we able to remove the field)**

**index="main" | table \_time "sourcetype" "date\_hour" | rename date\_hour as hours | fields – hours**

**dedup command (count it is showing )**

**index="main" | table \_time "sourcetype" "date\_second" | dedup date\_second**

**sort command**

**index="main" | table \_time sourcetype date\_second | dedup date\_second sortby -date\_second (descending)**

**index="main" | table \_time sourcetype date\_second | dedup date\_second sortby +date\_second (ascending)**

**Top command**

**index="main" | table \_time "sourcetype" "component" | top date\_hour**

**index="main" | table \_time "sourcetype" | top date\_second**

**Rare command (it is showing least command/ Reverse Format)**

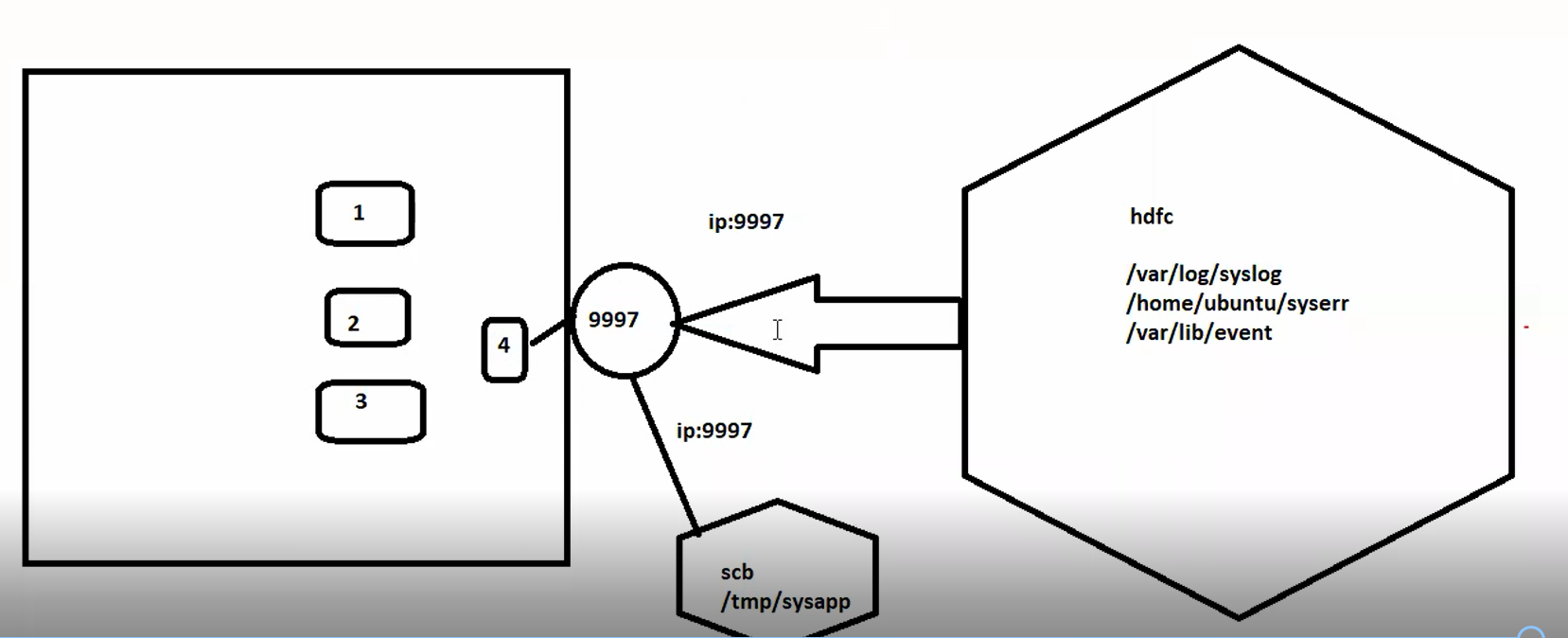
**index="main" | table \_time "sourcetype" | rare date\_second**

**stats**

**index="main" | stats avg(date\_second) by sourcetype**

**index="main" | stats sum by sourcetype**

**index="main" Deactivated successfully | stats distinct\_count by sourcetype**



**Different & Different Index:**