Day - 2

15 April 2025 14:32

1. Dashboard
2. User & Role creation.
3. Sourcetype.
4. Splunk Enterprise Security.

---

1. Dashboard:-

Dashboard → classic Dashboard.
Dashboard → Studio Dashboard

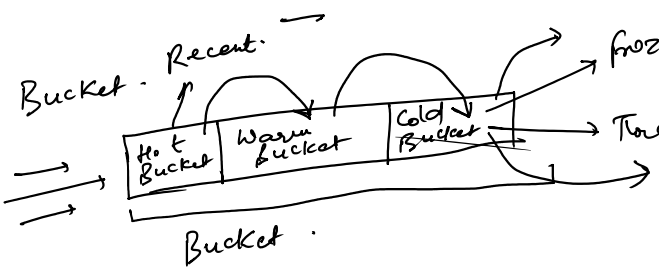
① classic Dashboard :- ① XML
② stable Version of splunk
③ HTML, CSS, JS
④ Feature Driven.

② Studio Dashboard:- ① - json
② splunk Version v 8.2+
③ JS.
④ cosmetic/visualization

Classic Dashboard:-

② Dashboard.
① Panel.
③ XML
④ Input filter.
⑤ Drilldown
⑥ few small feature

Index:- Bucket - Recent →



Bucket.

While searching, the data is very limited.

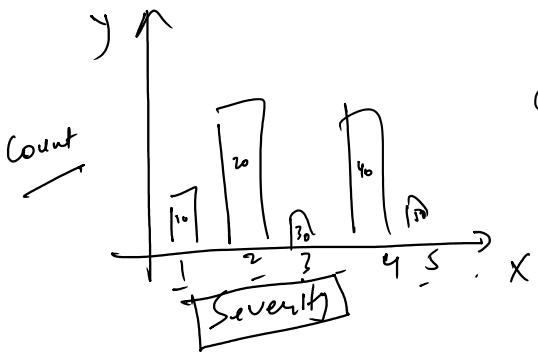
Two factor:-

① Size of the Bucket.
② Age of the Data in a Bucket.

Ex:- 10 GB 7d.

Drilldown:- It will select the value & pass on the dashboard / panel.

Drilldown:- It will select next Dashboard / Panel.



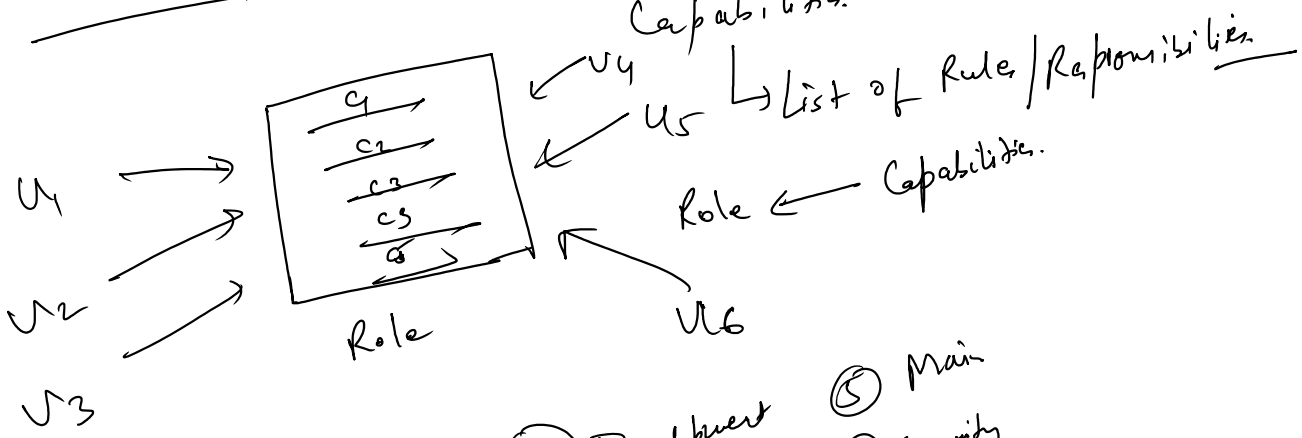
click.name → x-axis
↳ Severity

click.value → Value of x axis
↓
1, 2, 3, 4, 5

click.name 2 → y-axis
Name of ↑
↓
count

click.value 2 → Value of y axis
10, 20, 30, 40.

(2.) User & Role Creation:-



① Development
② Admin
③ Arch
④ End users
⑤ Main
⑥ Security

Role — ① Admin. → Sole owner
② User → Create / delete.
③ Power. → Modify

→ Delete the data from index.

(3) Power. →

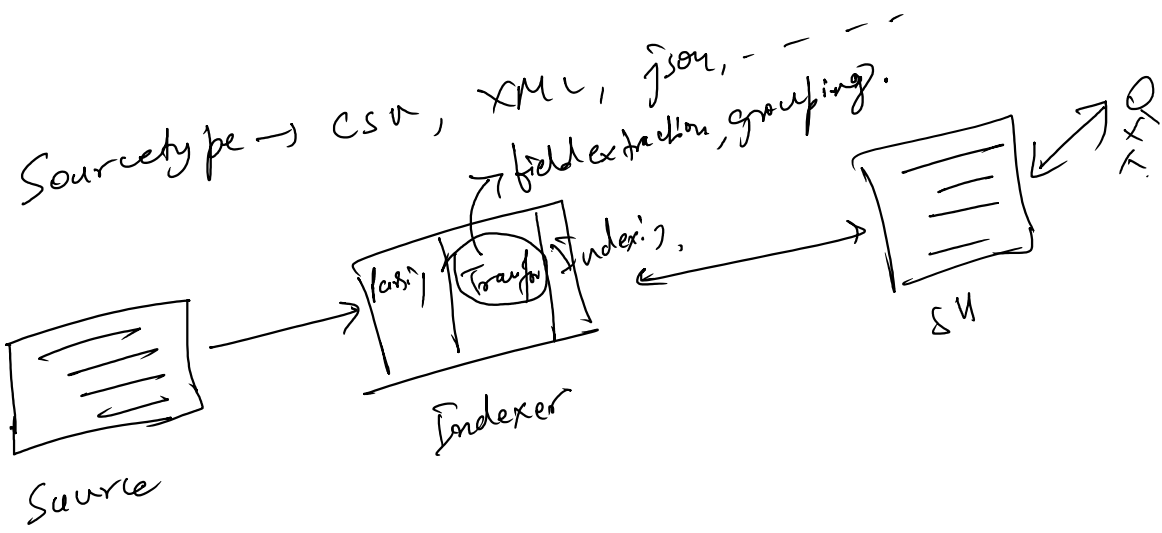
(4) Can_delete. → Delete the data.

(1) Native - Role you assigned explicitely.

(2) Inherited - Role that is inherited from the other role.

Sourcetype:-

Sourcetype → csv, XML, json, - - - -

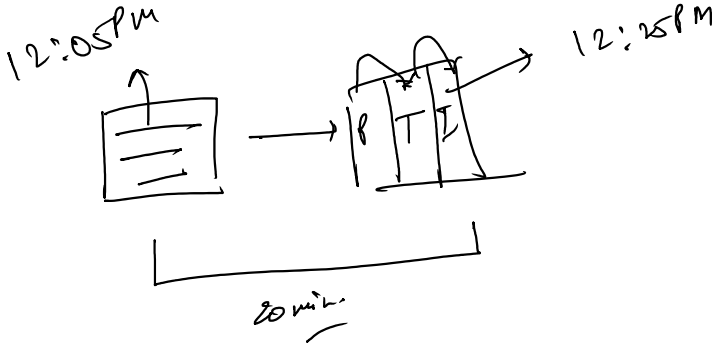


Timestamp

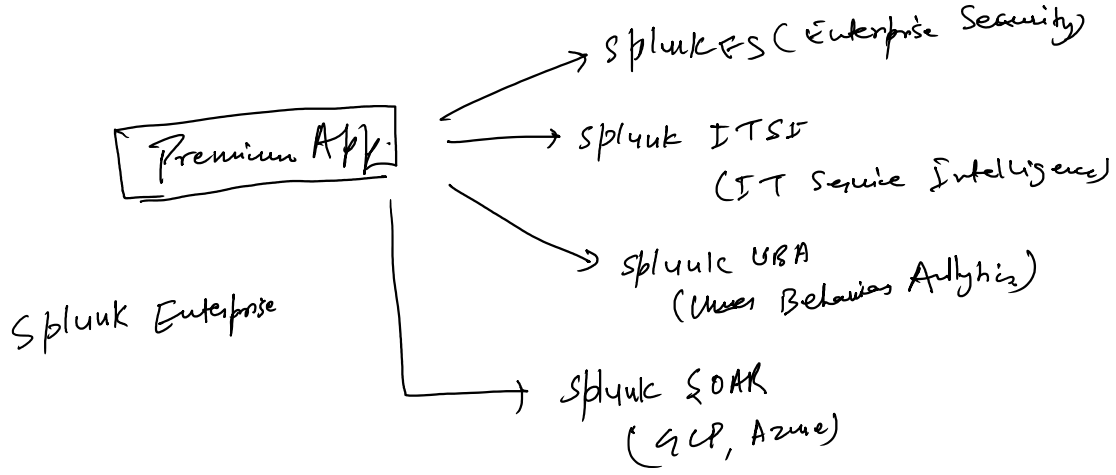
2 Time

(1) Ingest date in splunk.

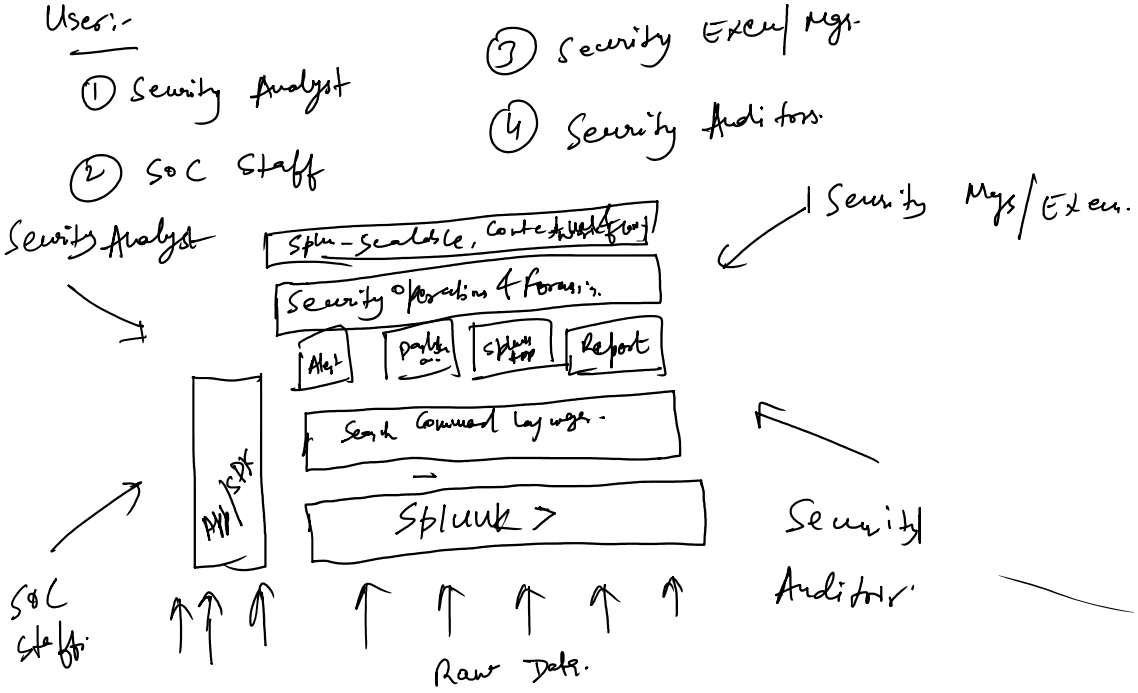
(2) Date is created or coming from log.



Splunk Enterprise Security Application



(1) Feature or Capabilities
(2) Pre configured Dashboard
(3) Detect, Prevent & Respond to Security threats & incidents.



Advanced Persistent Threat (APT)

(1) Growing, Global Threat.
(2) Focussed Attack on specific System

② Focussed Attack on specific System
ex:- yahoo, JP Morgan chase.

③ Goal - Undetected Insertion, long term Visibility, extract/delivery valuable Info

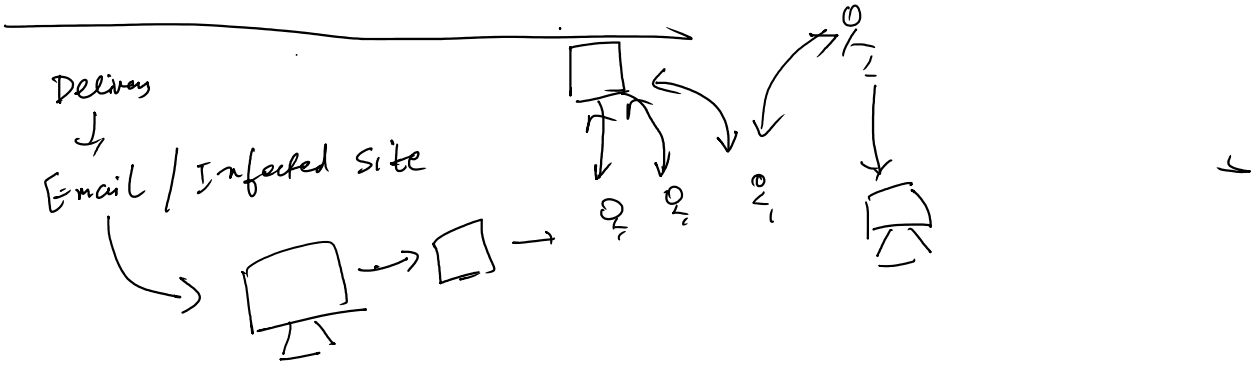
④ Target:- Busines, Gov., Individual.

⑤ Constantly changing & Adapt Method.

Kill chain:-

Stage	Attacker Activity	ES Countermeasures
Delivery	Email, website, Malware, Social engineer	Threat list, Vulnerability Scan, Real time monitoring, Access Monitoring
Exploitation / Installation	Open Attachment, download from site, Memory upload.	Protocol Intelligence, file system Alert, Intrusion detection, post Monitoring.
Command & Control	Execute code, open/copy file, changed Configs etc	Malware tracking, Process Alert, change Alert, Analytics
Accomplish mission	upload payload to remote Server, disable Servi-	Traffic Alert, N/W Analysis, Audit.

Anatomy of an APT Attack:-



How ES Works:-

① Data ⟶ Splunk Indexed ⟶ Events

② Real Time. ⟶ Threat, Vulnerability & Attack.
& Locate the issue ⟶ Track it ⟶ Analyze it

2. Real Time. → [illegible]

3. Investigate the issue → Track it → Analyze it → Appropriate Action.

ES Data Flow