Day - 4

17 April 2025 14:36

1. Network Domain
2. Vulnerability
3. Web Centre.
4. Risk Analysis.
5. Web Intelligence.
6. User Intelligence.
7. Threat Intelligence.
8. Protocol Intelligence.
9. Data Model Acceleration.

Lookup:-

- CSV
- Kvstore → Key Value pair → entry ⟷ Key → big | huge dataset. Dynamic in nature
- DB lookup
- Geospatial.
- External

CSV:-

1. When?
2. How?
3.

→ (1) Small Dataset.
(2) static.

CSV → upload in splunk

↓

[No License.
↓
No index.]

(4) lookup

(1) upload the CSV.
(2) inputlookup
(3) output lookup.

(3) output as lookup.

↓

upload the csv file

↓

lookup.

Protocol Intelligence:

(1) Protocol Centric → Protocol Across the network

(2) Traffic Size → N/w Traffic rate, trend.

(3) DNS → DNS Query & Search Interface.

(4) SSL → Analysis the SSL certificate Activity

(5) Email → Analyze email Activity.

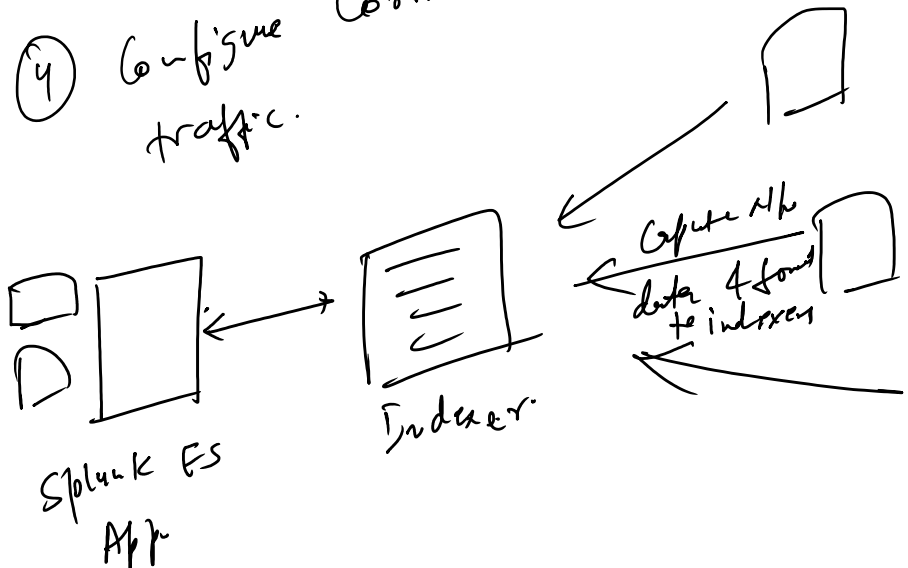
Use Case:

(1) Monitor Suspicious n/w traffic.

(2) Correlate logged vs Actual Activity

(3) Gained direct Access to N/w traffic for SSL, HTTP, DNS & SMTP Activity.

(4) Configure Correlation Searches that can monitor N/w traffic.



App

Stream:: —— smtp, http
ex: tcp, udp, dns,

Stream: tcp
Stream: udp
Stream: http

HTTP → Cookies, req. parameter etc.
SMTP → Sender, reciever, subject, summary of body
DNS → DNS query, type, host etc.

Risk Analysis:-
① Enable you to examine event in your ES indexes.
② Risk Value to the object.
- Systems or Users.
③ Amount of Risk Assigned can be configured per object ←
per event.
④ Risk → Value → ↑ Higher Risk

Ad-hoc Risk Entry:-
① Add or substract risk for any object.
② Add (+ve), —, —

Web Intelligence
① Network Environment.
① Http Category → Type of website → URLs
② Http User Agent → Web User Agent on your N/W
③ New Domain. → External Domain. → High count of Long or Malformed indicate botnet or Unusual content.

(2) Http ...
(3) New Domain. → External Domain
(4) URL Length. → Req-URL, indicate some Unusual content.
↙
embedded SQL, Cross site scripting

Per Panel Filter:-

(1) Analysis dashboard enable Analyst to highlight filter item over of Dashboard.

(2) ES Admin.

(2.) User Intelligence →

(1) User Activity
(2) Access Anamolis to detect suspicious access pattern.
(3.) Asset & Identity
(4) Investigate to Analyze event related to an asset or identity.

Insides Threats:- Inside your Org.

(1) Active Account
(2) What!
(3) equipment.
(4) Missing org
(5) Risk each user or device!

(1) Asset Investigator → Specific Asset, Ex - Server, Workstation,
(2) Identity Investigator → specific Identity & compare event overtime.
(3) Access Anamolies → A survey of w/o Activity by user, Wgt.. (one account by multiple times)

(2) [illegible]

(3) Access Anamolies → A -

(4) User Activity → High-risk

(1) Threat
(2) IDS Attack
(3) Authentication
(4) Malware.
(5) Notable event.

User Activity Panels

(1) User by Risk Score -
(2) Non-Corporate Web upload & email Activity -
(3) Watch listed sites. -
(4) Remote Access → Rdp
(5) Ticket Activity →

Watchlisted User & Site -

(1) User & Site → ES Admin..
Incident Review. → Updated
→ Notable
→ Security

* Access User Activity from Action Menu -

User → User Activity
Open User Activity Dashboard.