Day - 4

17 April 2025 14:36

1. network Domain
2. Vulnerability
3. WebCentre.
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
- → DBlookup
- → Geospatial.
- → External

CSV:-

1. when? } → 1. Small Dataset. 2. Static.
2. How?
3.

CSV → upload in splunk
↓
No License.
↓
No index.

1. upload the CSV.
2. inputlookup
3. output lookup.
   ↓
   upload the csv file
   ↓
   lookup.
4. lookup

+

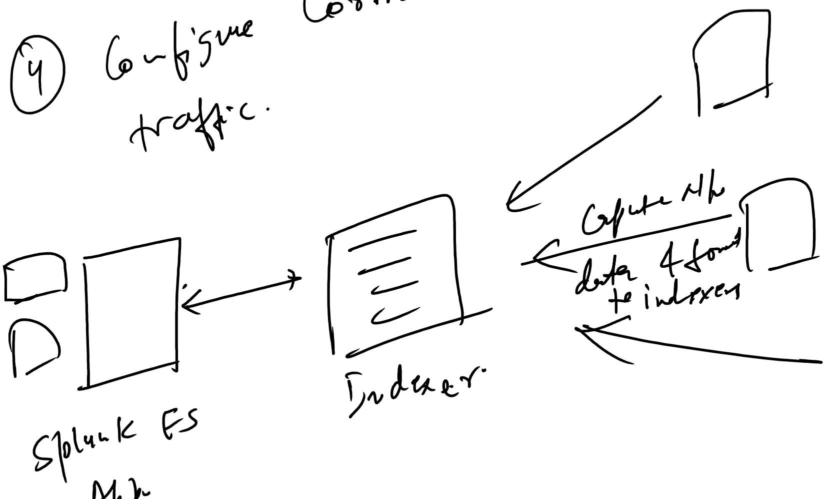
lookup.

Protocol Intelligence:-

1. Protocol Centre → Protocol Across the Network
2. Traffic Size. → N/w Traffic rate & trends.
3. DNS → DNS Query & Search Interface.
4. SSL → Analysis the SSL Certificat Activity
5. Email → Analyzing 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.



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

Ex + tcp, udp, dns, smtp, http

stream:tcp

stream: udp

stream:http

Http → Cookies, req. parameter etc.

subject, summary of body

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 Enviorment.

① Http Category → Type of website → URLs

② Http User Agent → Web User Agent on your N/W → Long or Malformed

③ New Domain. → External Domain. → High count of new domain can indicate botnet or

④ URL Length. → Req. URL, Unusual Content. → embedded SQL, Cross site scripting

Per Panel Filter:-

① Analysis dashboard enable Analyst to highlight filter item out of Dashboard.

[illegible]

① of Dashbo

② ES Admin

② User Intelligence

① User Activity

② Access Anamolis to detect suspecion access pattern.

③ Asset & Identity

④ Investigate to Analyze event related to an asset or identity,

Insider Threat:- Inside your Org.

① Active Account

② What!

③ equipment.

④ logging on

⑤ Risk each user or device!

① Asset Investigator → Specific Asset, Ex - Serve, Workstation,

② Identity Investigator → specific Identity & Compare event over time.

③ Access Anamolies → A survey of N/W Activity by users, host.. (One account by multiple times)

④ User Activity → High-risk

① Threat

② IDS Attack

③ Authentication

④ Malware.

⑤ Notable event.

User Activity Panels:-

① Users by Risk Score-

Large Web upload & email Activity.-

① Users by Risk score
② Non-corporate Web upload & emai.
③ Watchlisted sites. -
④ Remote Acces → Rdp
⑤ Ticket Activity →

Watchlisted User & site:-

① User & site → ES Admin..
Incident Review. → Update
→ Inputs
→ Script

* Acces User Activity from Action Menu:-

User → User Activity
open User Activity Dashboard.

Splunk Upgrade:-

① Pre Implementation. → ① Backup config, Dashboard
② Version
③ Backup Index
④ DBConnect
↓
JRE + Driver

② Implementation. → ① Upgrade Splunk & Dependent apps & addo
with their dependence.

③ Post Implementation → Matching the final output.