Day - 3

15 April 2025 22:16

1. Correlation Search
2. Security Monitoring & Incident Investigation.] → Data Model.
3. Investigation.
4. Forensic
5. Risk Analysis.
6. Web Intelligence.
7. User Intelligence.
8. Threat Intelligence.
9. Protocol Intelligence.

---

1. Correlation Search:-

Run in the background to detect evidence of attack, threat, Vulnerabilities.

- Real time.

Correlation Search finds something that requires attention | threat | Vulnerability

↓

Alert → Notable event

Enable, script, update risk score etc.

Correlation Search → Notable event (breach, vulnerability / issue)

↓

Notable index

Notable Event:-

↓

breach, Vulnerability, other issue.

index = Notable

DDos Attack

↓

Denial of Service

Assets & Identities:-

Asset → Devices (router, Server)

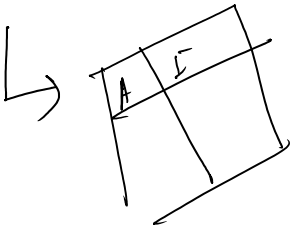
Identities → People (username, email)

Asset

Identities → People (user...

Lookup Table's — csv file.

↳ Uploaded in splunk.



1. Risk & threat Analysis
2. Web & user Intelligence.
3. Protocol (Stream) Intelligence.
4. Adaptive Response.

3 ES Roles

1. ES User → Run real-time searches & view all ES dashboards.
2. ES Analyst → Own notable events & perform notable event status changes
3. ES Admin. → Configure ES-Admin, users, manages correlation Search, adding new data sources.

Macros:- Kind of function.

```
function a ( 5, 6)
{
  d = 5 * 6;
  return d;
}
```

a(3,4)

a(5,6)

a(-7,4)

a(8,-3)

arg1 arg2

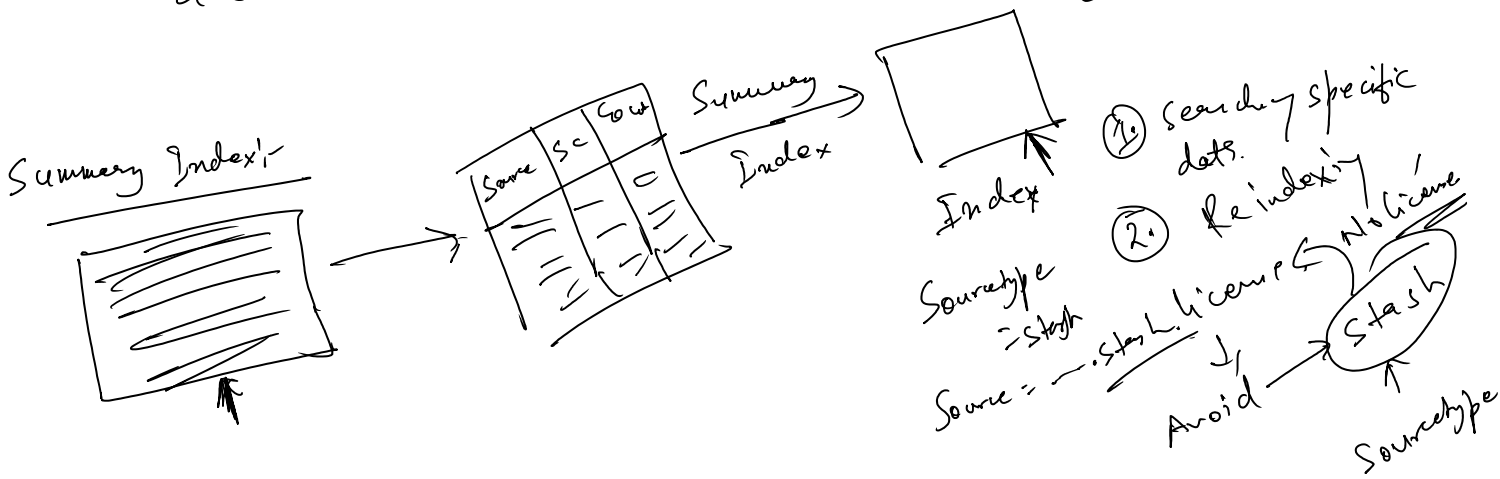
Macros → Template | function

↳ arg1 →

a C

Macros → Temp...

e.g. arg.



Creating & Suppressing the Notable event:-

Manual Creation:- Source event data that has not yet identified by ES as suspicious.

Suppression:-

Investigation:-

(1) Manage incident response activity
(2) Investigative Timeline.
(3) Add items to investigation.

Visualise progress.
Document work.
Share information
→ Investigation

Forensic Investigation:-

Security Domain.

- Access
  - Access centre
  - Access tracker.
  - Access search.
- Endpoint
  - Account Management.
  - Default Account Activity
- Network
- Identity

Access Domain Correlation:-

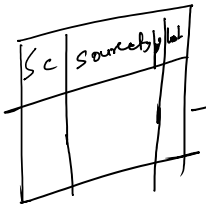
1. Account Deleted. →
2. Brute force. →
3. Cleartext password. →
4. Inactive Account. →
5. Default Account usage →
6. Excessive failed login →

End point Domain Investigation Scenarios:-

1. Vulnerability :- Missing update or patches.
2. Malware :- spyware, ransom, malicious code.
3. Unexpected running process or Services
4. Unexpected registry change.

Data Model:-

Define all the fields in advance itself



→ Explicitly define the fields.

Root

→ child + c'

→ S child + c''

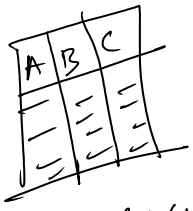
→ SS child + c'''

Lookup - csv file

.csv

(1) upload in splunk

(2) No license consumption.



access.csv