Day - 5

14 November 2025 08:41

Today

1. Davis AI
2. DevSec
3. Hub.
4. Workflow
5. Note book.
6. Integration of Jmeter & load Jacoco
7. Instrumentation.
8. Data Retention
9. License
10. Export the config.

09-09-09
1,
Sep 09

→ Note book

1. Notebook:-

Analysis, Troubleshooting, Data exploration.

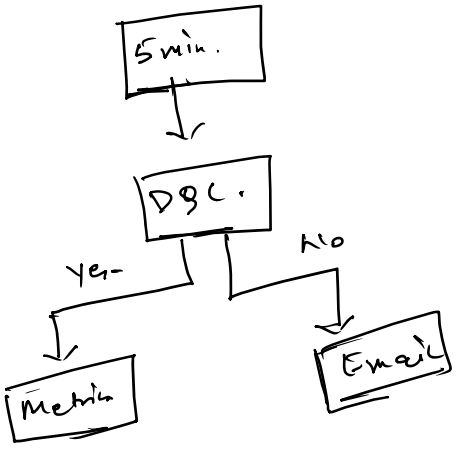
SRE, observability, Developer

1. Deep Analysis, adhoc investigation.
2. Developer, observability engineers
3. DQL,
4. Built mainly on grail + DQL.
5. Debugging & Data exploration.

Dashboard

1. End user.
2. Visualize the panel & data.

2. Workflow:-



Log level Alert

info
error > 10

Cron job → * * * * * -

* DevSecOps:-

End-to-end observability security

1. Application Security module.
2. Runtime App protection (RASP)
3. Vulnerability Detection & SCA.
   Detection & observability.

(2)
(3) Vulnerability Detection & observability
(4) Attack Detection

(1) Development phase.
(2) Runtime Phase.
(3) Prioritised & Risk based Security findings.
(4) Attack Detection & Protection.
(5) CI/CD Integration - Automation.
(6) Cloud Security Posture.
(7) Unified security

(1) Development Phase:- DT scan app. build, deploy & Runtime.

① Vulnerability Analysis → CVE Mapping
→ Version upgrade
→ Prioritised risk scoring.

② Dev Team Benefit → Dev- get immediate feedback
→ Faster Remediation.
→ Security findings integrated into CI/CD.

(2) Runtime Phase:- DT continuously monitor app in production

① Vulnerability
② Misconfiguration
③ Suspicious Behaviour
④ Exploit Attempts

(3) Prioritized & Risk Based Security findings:-

① what is Business Impact?
② Actively attacking it?
③

(4) Attack Detection & Protection:-

Actual Attack → SQL injection.
→ Command Inj.
→ Traversal.

(4) Adfeed

Actual Attack
- Command Inj.
- Directory Traversal.
- Remote code execution.

(5) CI/CD Integration + Automation

(1) Jenkins
(2) Devops
(3) GitHub Action
(4) GitHub
(5) BitBucket Pipelines.

(6) cloud Security Postures

(1) S3 Bucket.
(2) IAM Misconfig
(3) K8s
(4) Image Scan).

(7) Unified Security

(1) Dashboard - Vulnerability
Risk score.
Active Attack

Top exploited CVE

(1) Code — Library Scanning, SCA
(2) Build — Report Vulnerability
(3) Test — Runtime check
(4) Deploy — Deployment Validation, Misconfig Detection
(5) Run — RASP, exploit Detection.
(6) Monitor — Dashboard & Alert.
(7) Respond — Attack Details, RCA, Remediation Guidance.

→ DevSecOps loop.

Dynatrace Config :-

Dynatrace Config :-

1. Dashboard
2. SLO
3. Workflow
4. Notebook
5. Logging Pipeline

Tijson

Monaco
- Monitoring as code

Dynatrace Certification

1. Dynatrace Associate Certification — 60 Q - MCQ, 90 min, 75%
2. Dynatrace Professional Certification — 90 min,
3. Dynatrace Expert certification → MCQ, Practical Exam, Interview

100%.
100%.
70-75%