black hat ASIA 2022

MAY 12–13

BRIEFINGS

black hat ASIA 2022

Patronus

Swiss Army Knife SAST Toolkit

About us

Ashwin Shenoi

Security Engineer @ CRED

@__c3rb3ru5__

Akshansh Jaiswal

Security Engineer @ CRED

@Akshanshjaiswl

Akhil Mahendra

Security Engineer @ CRED

@Akhil_Mahendra

Agenda

- Why we built this
- How Patronus stands out
- Design Solution
- False Positive Reduction
- Demo
- Future roadmap

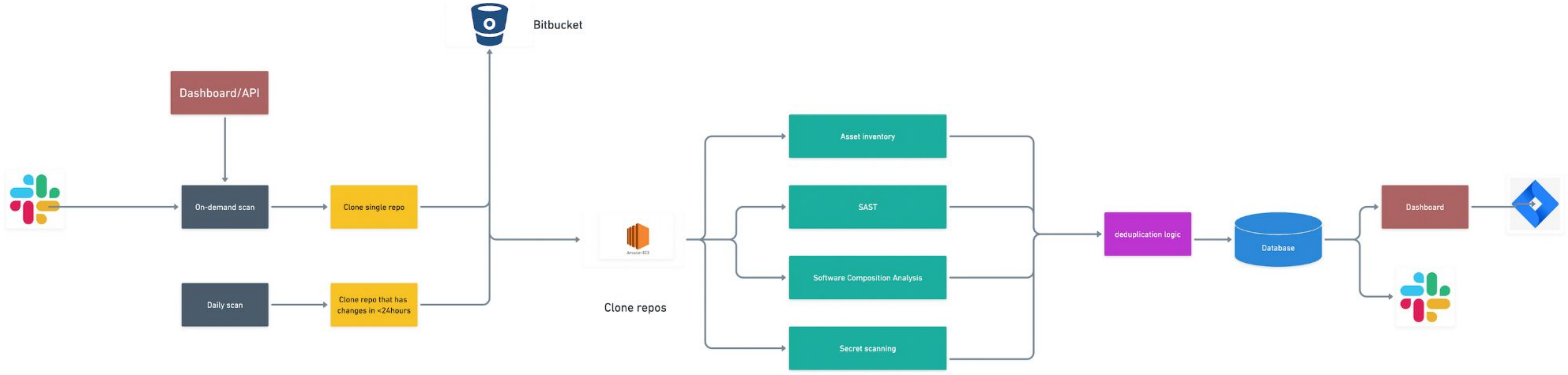
Why we built it?

- Single security framework for vulnerability management & assets inventory
- High levels of false positives and huge operational overheads
- Lack of visualisation of organisation’s security posture and metrics
- Ease for devs to adapt to shift left without interfering in production code pipelies
- Cater to organisational needs and keep source code always within the ecosystem
- Actionable approach to security vulnerability findings rather than being a blocking function
- Developer-friendly security scans for their projects in real time

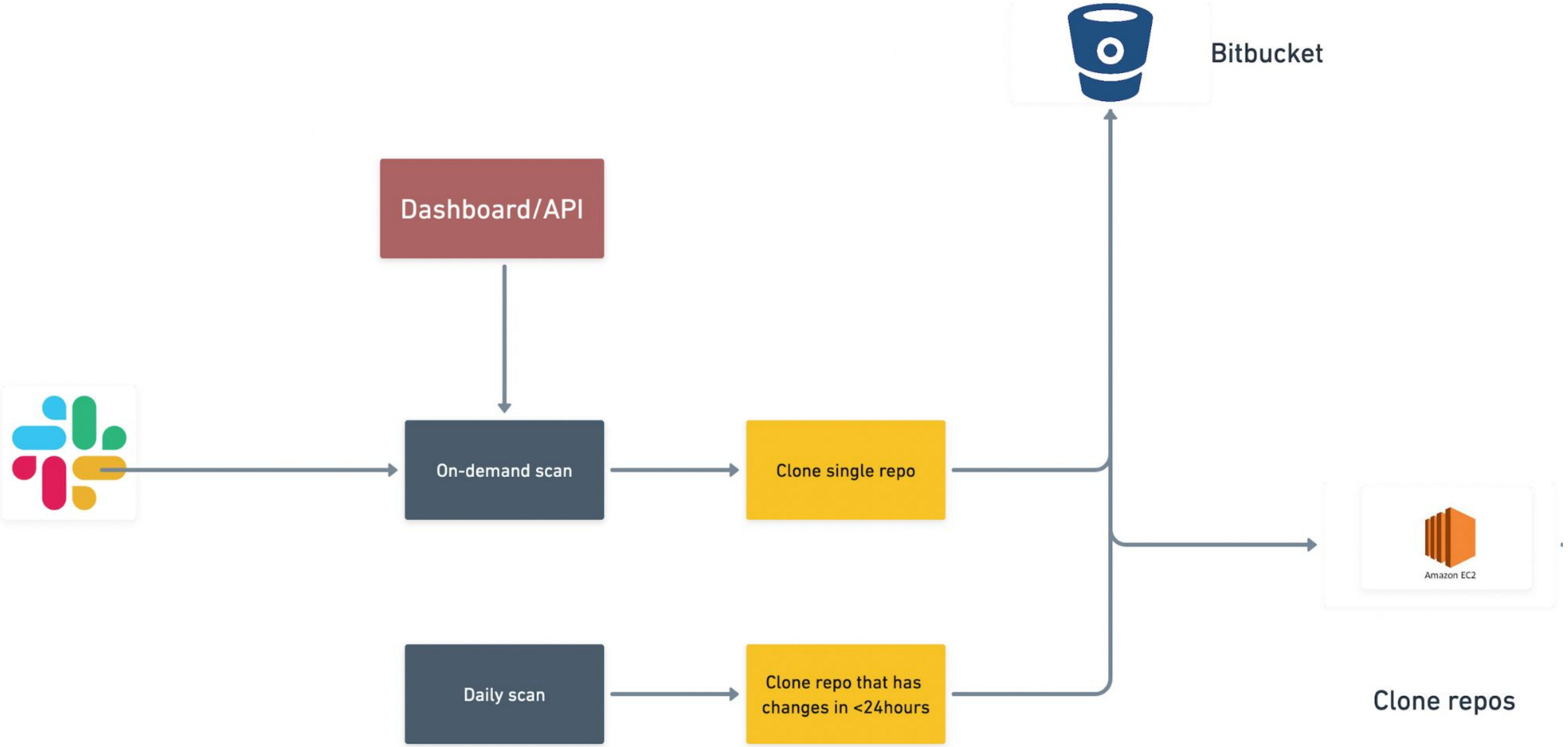
How Patronus stands out

- Secret Scanning✓
- SAST✓
- Asset inventory ✓
- Scanning only latest code commits ✓
- Security vulnerability stats and trends ✓
- Configurable scans ✓
- Custom integrations ✓
- SCA ✓
- On-demand scan ✓
- All in one dashboard ✓
- REST API Support ✓
- Multi-language support ✓
- Fully dockerized ✓
- Single Sign On ✓

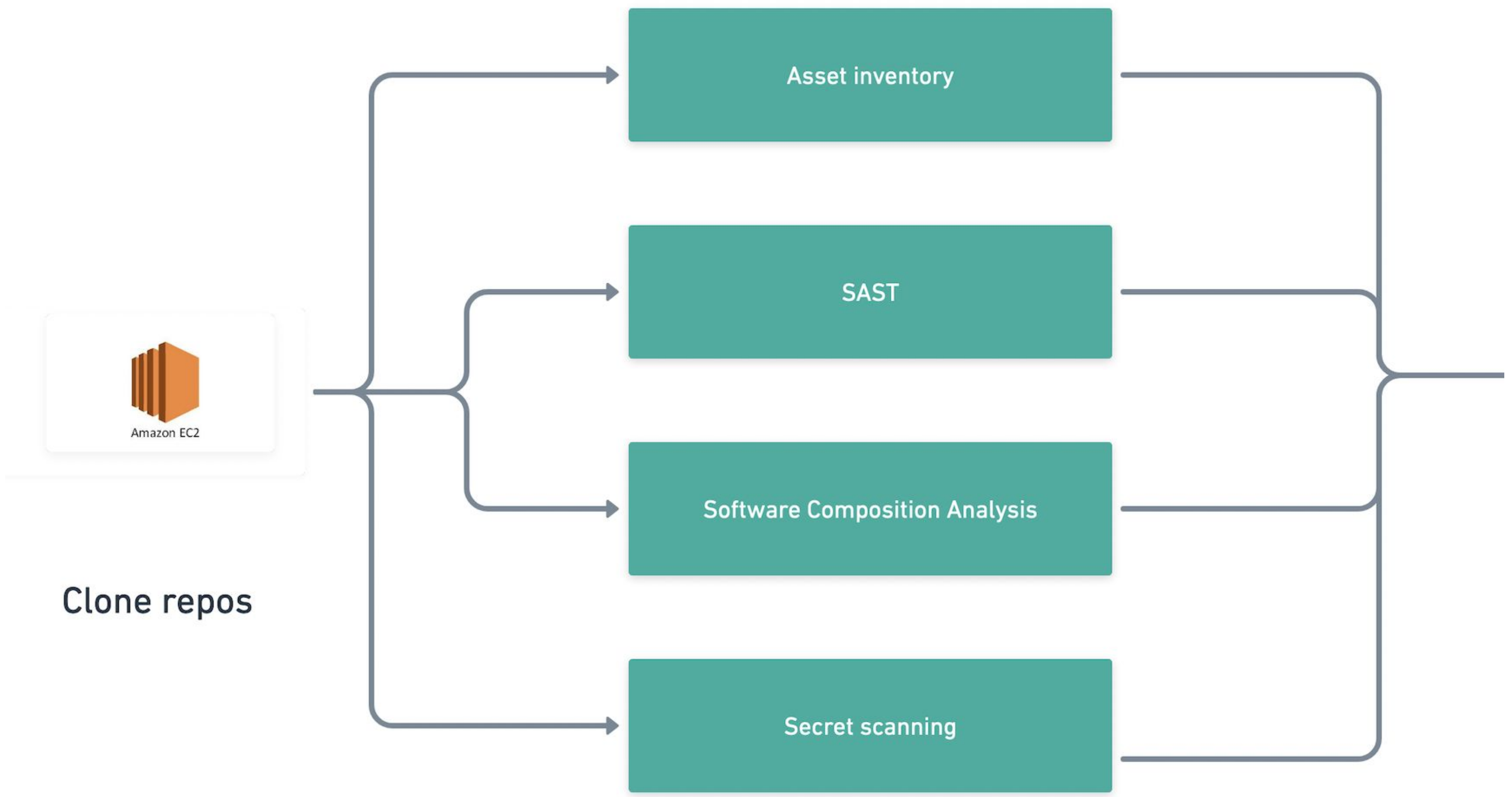
Design Solution



Initiation

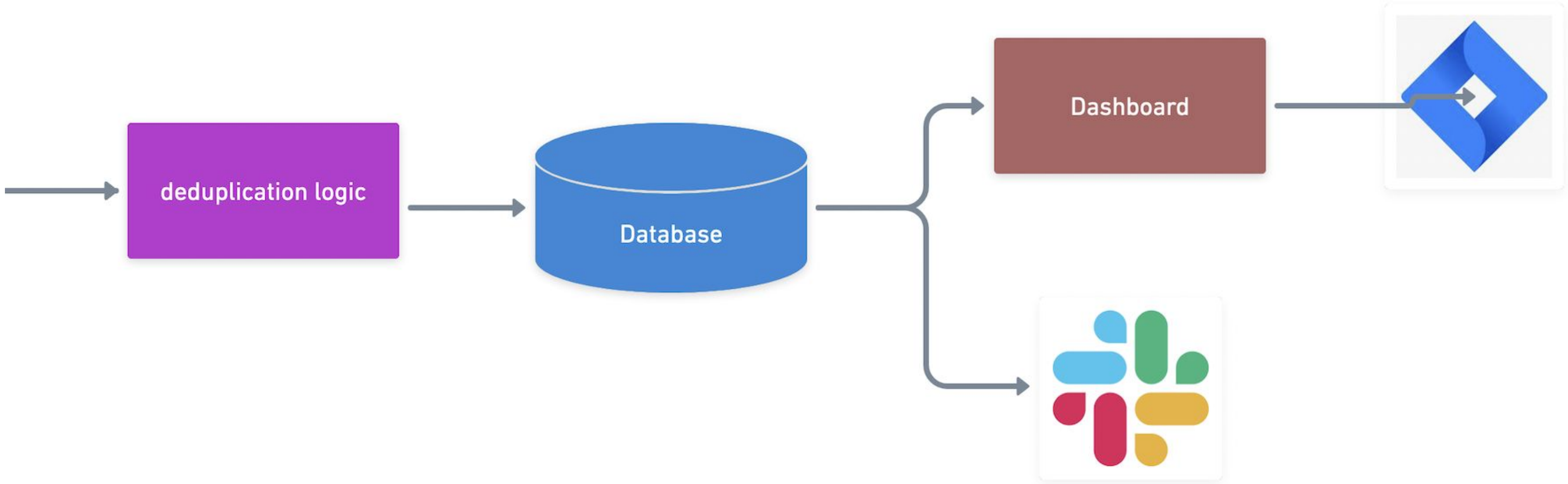

Bitbucket
Dashboard/API
On-demand scan
Clone single repo
Amazon EC2
Daily scan
Clone repo that has changes in <24hours
Clone repos

Scanning



Clone repos

Enrichment



False Positives reduction

- Validation of active tokens and secrets
- Actively searching for publicly available exploits for identified CVEs
- Classify findings based on configurable CVSS scores to prioritise remotely exploitable CVEs.

Demo

Future Roadmap

- Introducing new verticals:
  - SBOM
  - Licence management
- Increase coverage for more languages
- Integration with VCS like github/gitlab
- One click automated patching of SCA issues.
- CI/CD integration

Thank You

https://github.com/th3-j0k3r/Patronus