Credential mitigation
in large scale organizations

Watch the live recording here: https://youtu.be/kCo0OJZHRX8

Tobias Gabriel, SAP
Nikolas Krätzschmar, SAP
May 2020

Tobias Gabriel

Developer Tools Team SAP

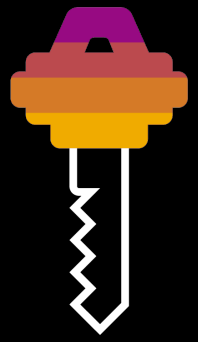
Internal GitHub Administration

Nikolas Krätzschmar

Master Student Computer Science – Heidelberg University

Working student at SAP Tools Team

>250 000
repositories



?
credentials

>5 TB
source code

Credential Types

- Private keys
- GCP service accounts
- AWS Keys
- Slack tokens and webhook URLs
- Bitcoin WIF-keys

Extracting Repository Content

Patches

git log --full-history --all -p

Blobs

git rev-list --all --objects --in-commit-order | ... | git cat-file --batch

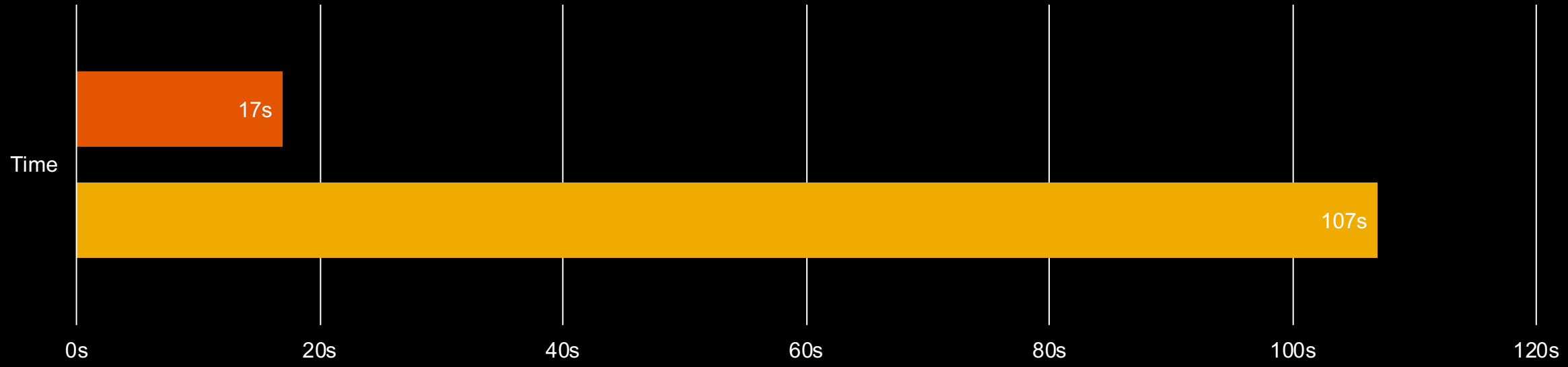
Scanning of Raw Content

PCRE grep

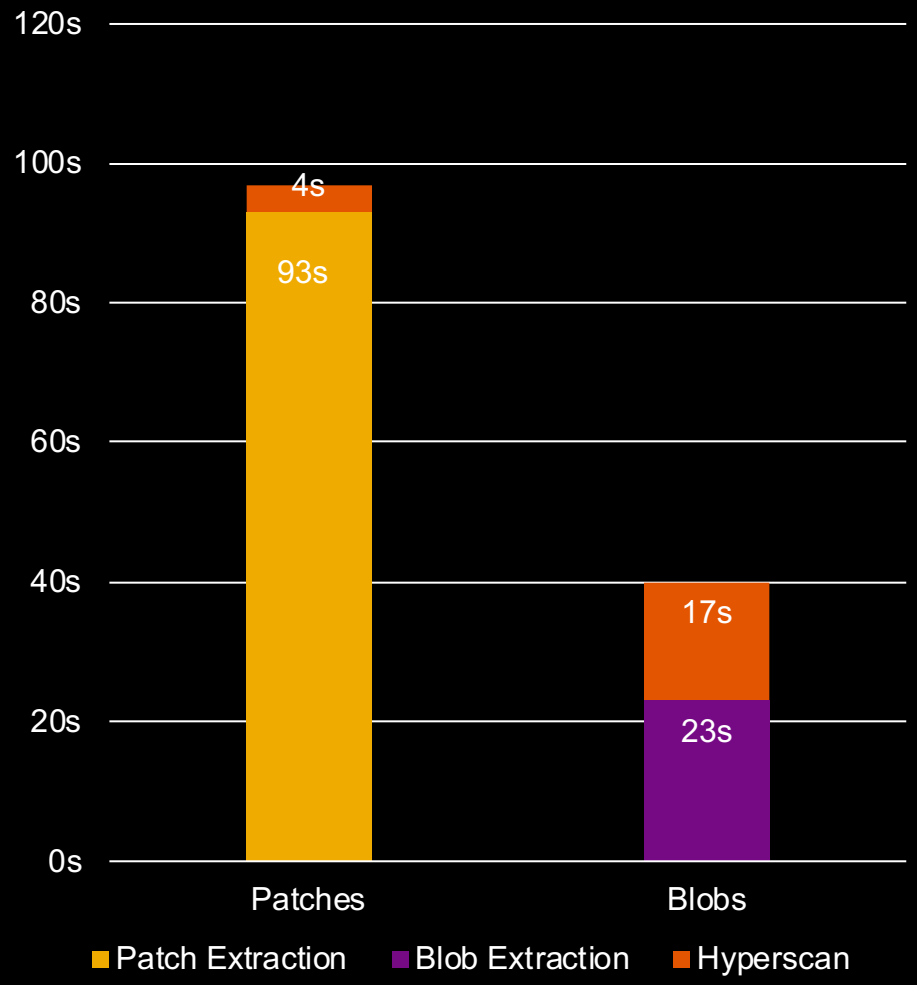
- multiline mode
- perl compatible regex

Hyperscan

- precompiled patterns
- optimized for CPU architecture



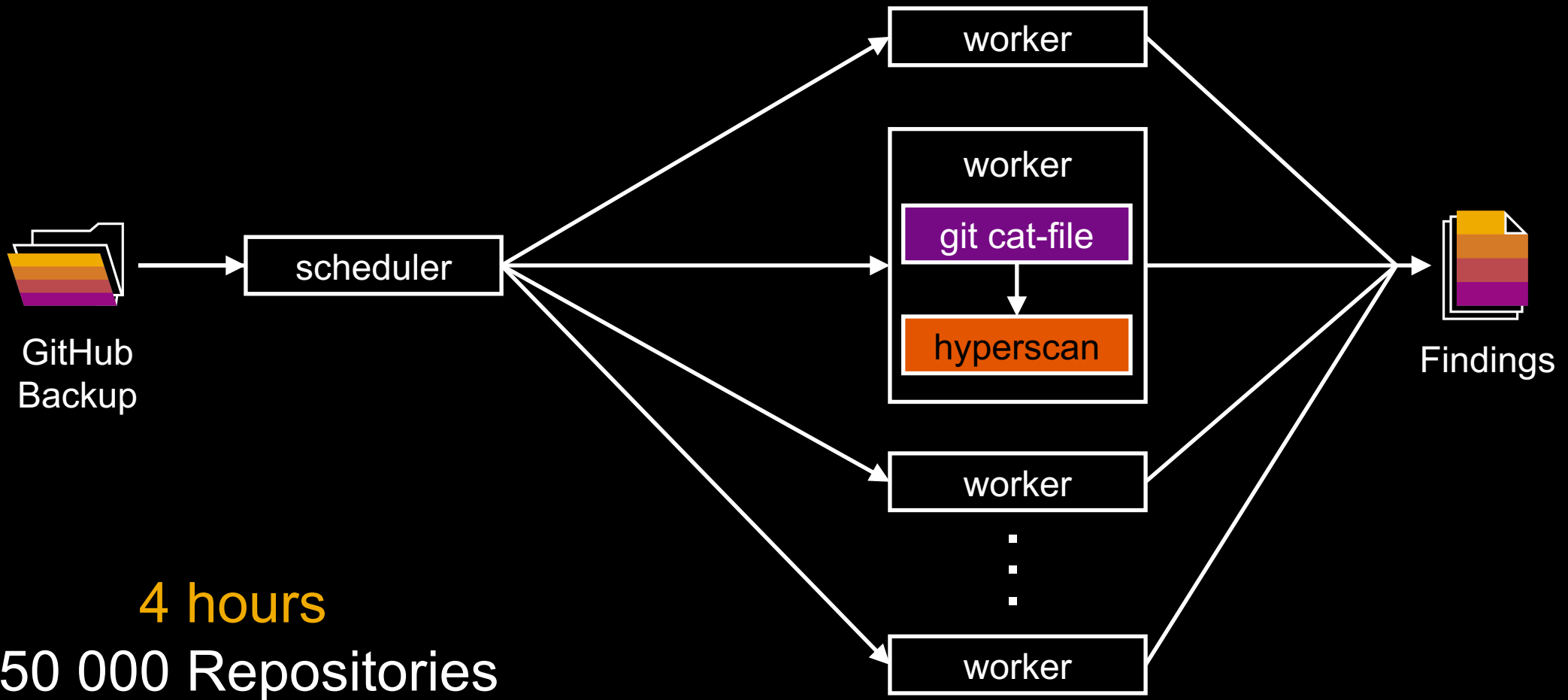
Building the Scanner



22s/100 Repos

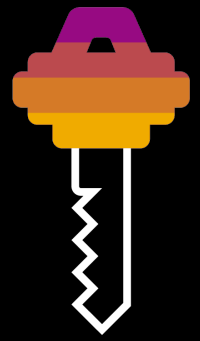
Blob Extraction + Hyperscan + Blob Size Filter

Full Scanner Setup



4 hours

250 000 Repositories



At least 1 ;)

Service Secrets

Slack Webhooks

https://hooks.slack.com/services/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

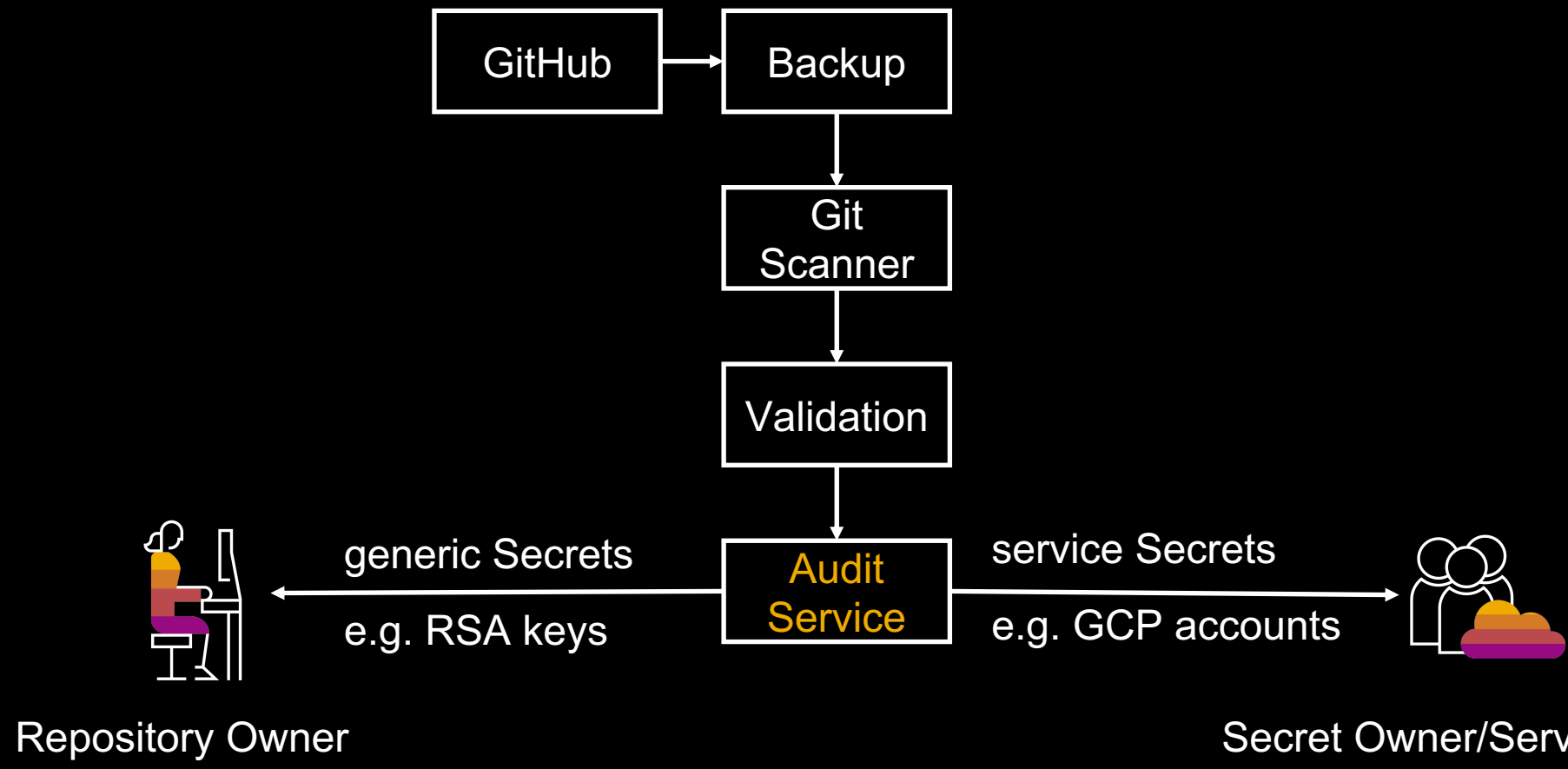
Active & Valid

https://hooks.slack.com/services/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

Invalid

Majority Active & Valid

Architecture



Observations

Increasing Accuracy

Mitigation Guidance

Automatic Validation

Thank you.

Contact information:

Tobias Gabriel
tobias.gabriel@sap.com

Nikolas Krätzschmar
nikolas.kraetzschmar@sap.com

Satellite Virtual 2020

THE BEST RUN SAP

Follow us

www.sap.com/contactsap

THE BEST RUN SAP®