

Credential mitigation in large scale organizations

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

Tobias Gabriel, SAP
Nikolas Krätzschmar, SAP
May 2020

PUBLIC



Tobias Gabriel

Developer Tools Team SAP

Internal GitHub Administration



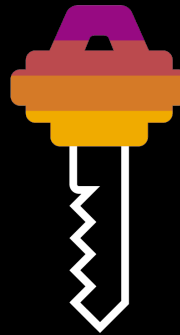
Nikolas Krätzschar

Master Student Computer Science – Heidelberg University

Working student at SAP Tools Team



>250 000
repositories



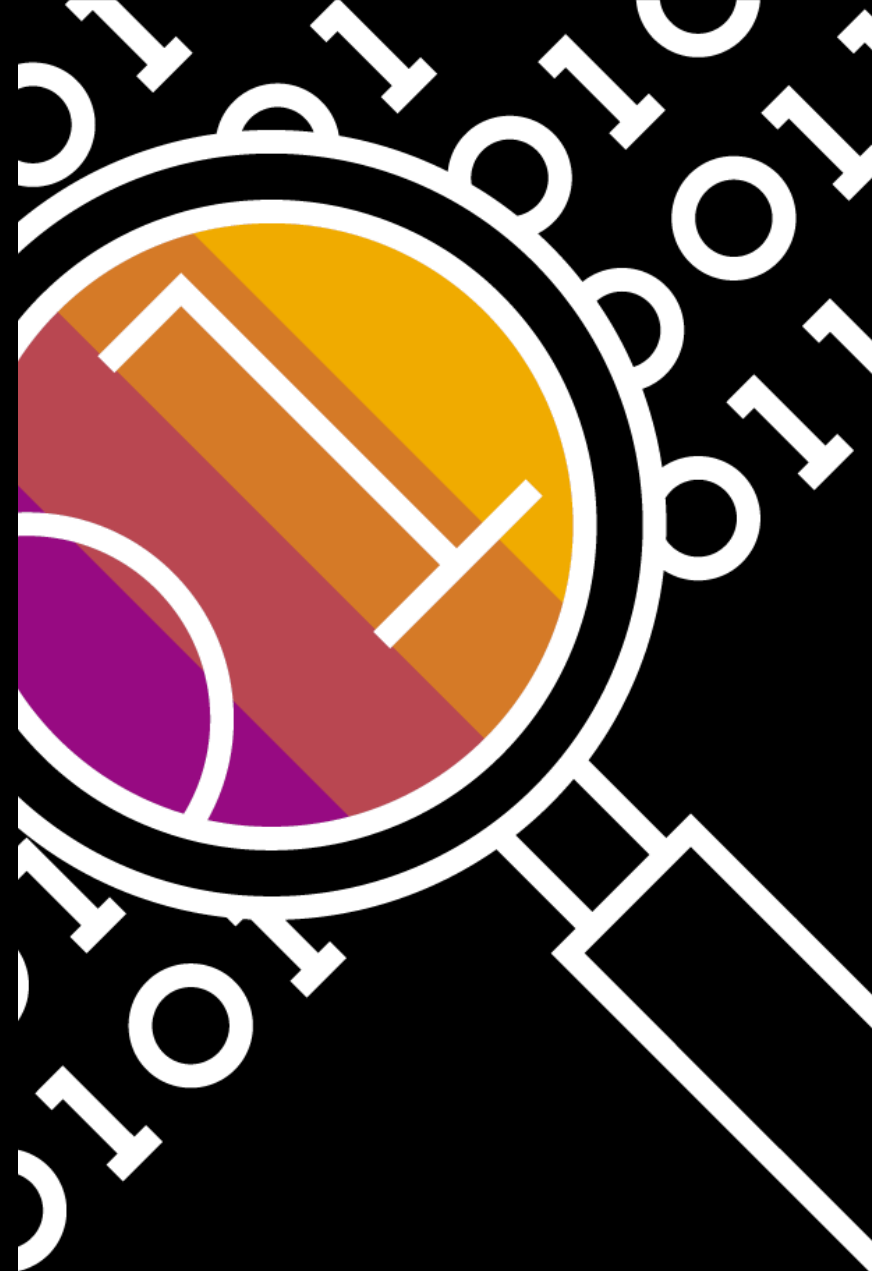
?
credentials



>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
```



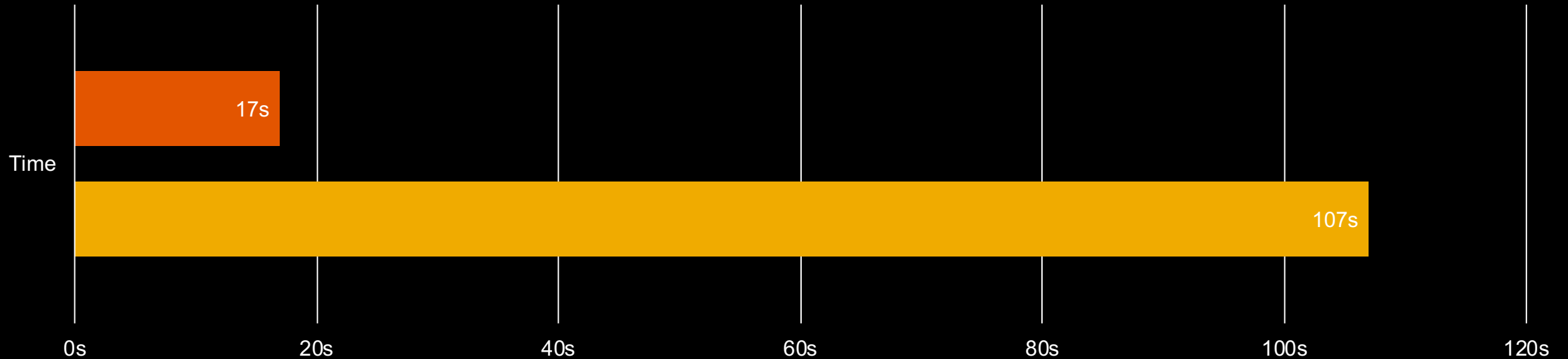
Scanning of Raw Content

PCRE grep

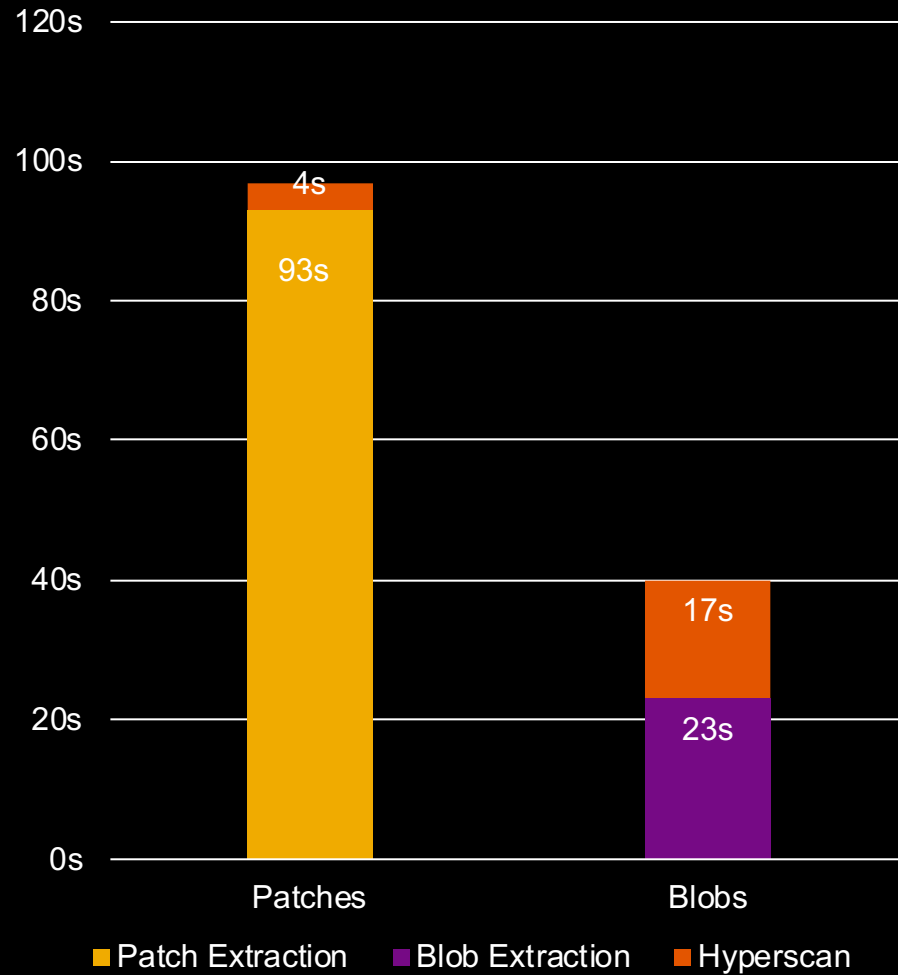
- multiline mode
- perl compatible regex

Hyperscan

- precompiled patterns
- optimized for CPU architecture

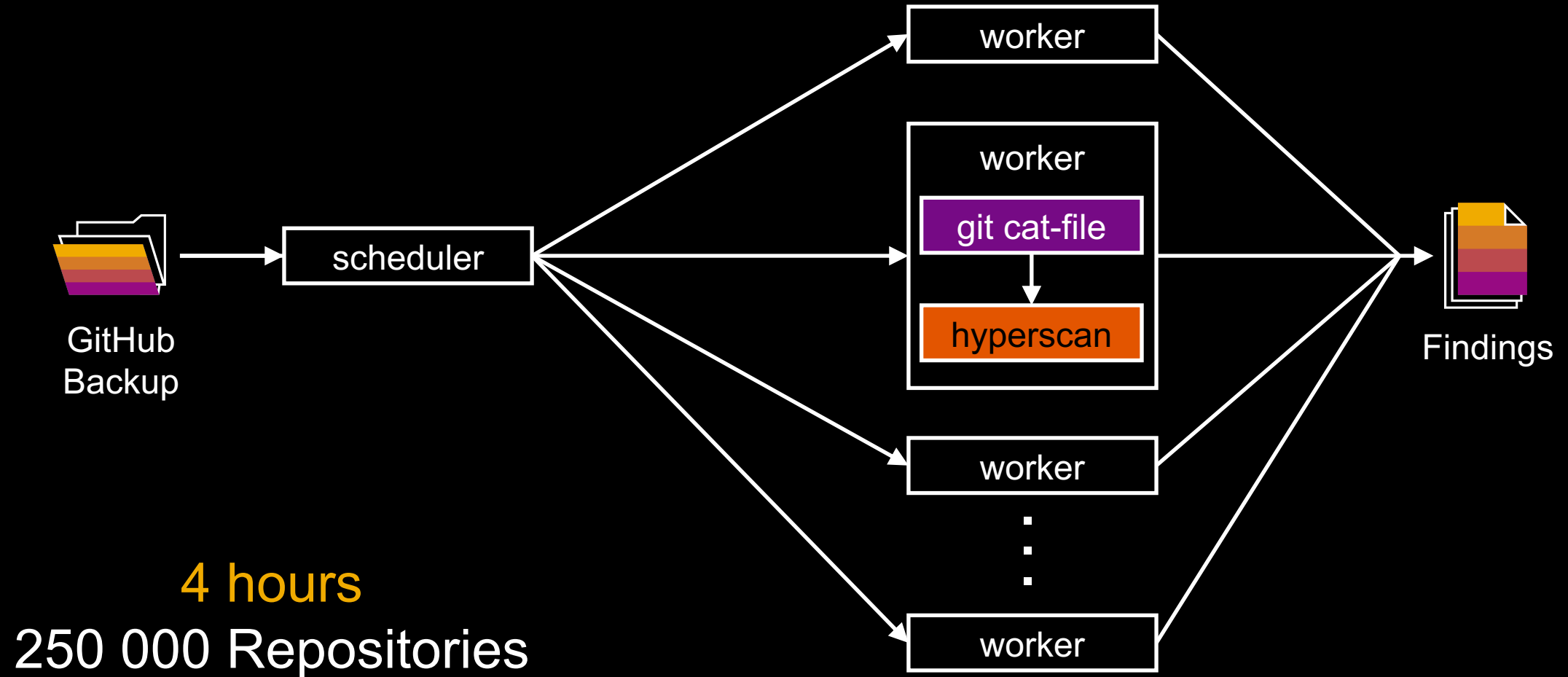


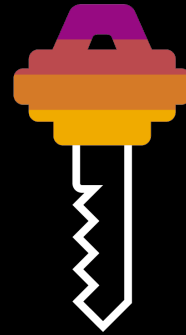
Building the Scanner



22s/100 Repos
Blob Extraction + Hyperscan
+ Blob Size Filter

Full Scanner Setup





At least 1 ;)

Service Secrets

Slack Webhooks

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

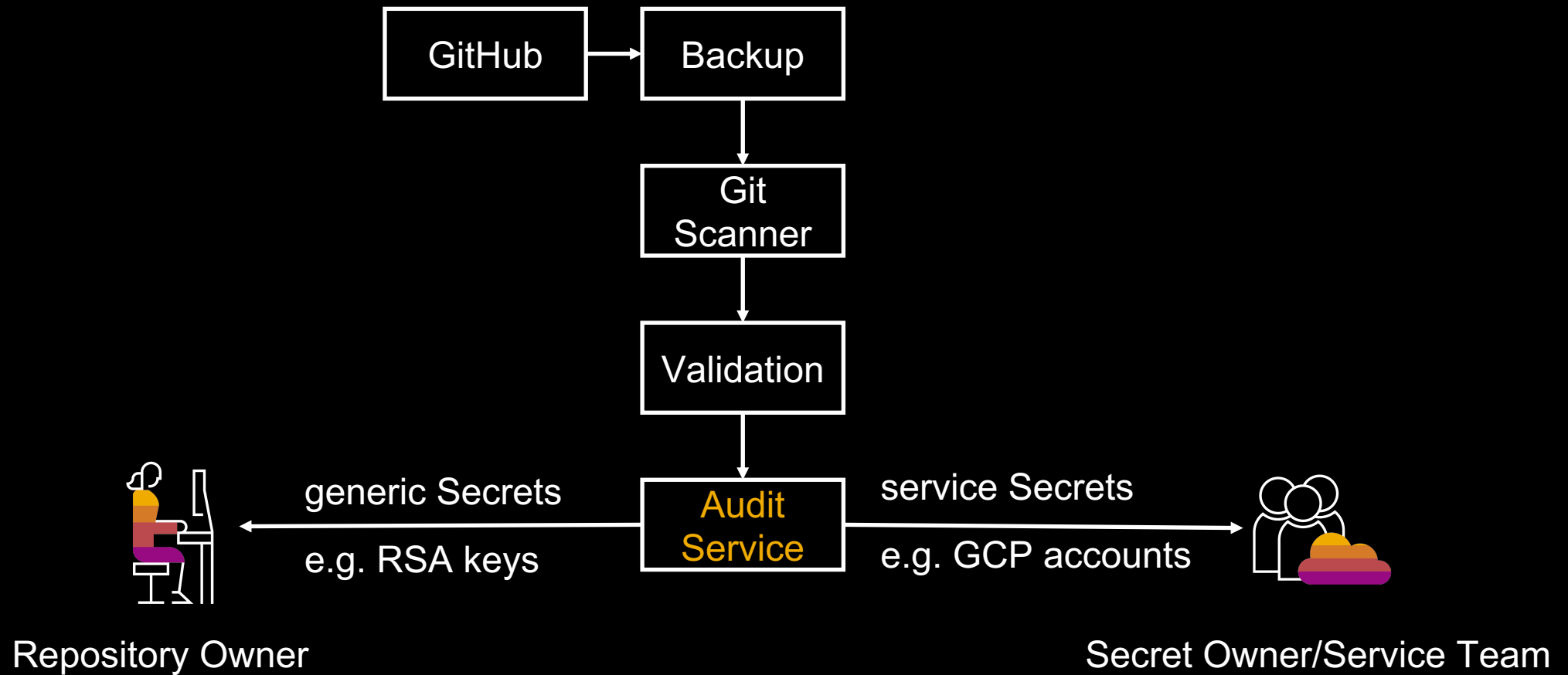
Active & Valid

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

Invalid

Majority Active & Valid

Architecture



Observations



Increasing
Accuracy



Mitigation
Guidance



Automatic
Validation

Thank you.

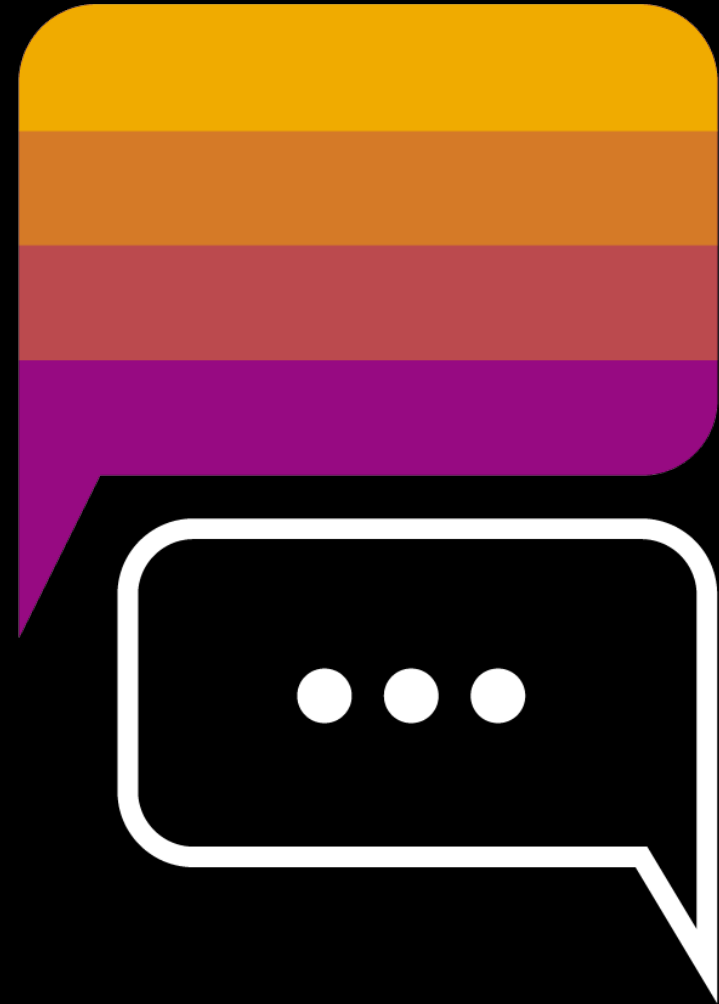
Contact information:

Tobias Gabriel

tobias.gabriel@sap.com

Nikolas Krätzschar

nikolas.kraetzschar@sap.com



Follow us



www.sap.com/contactsap

© 2020 SAP SE or an SAP affiliate company. All rights reserved.

No part of this publication may be reproduced or transmitted in any form or for any purpose without the express permission of SAP SE or an SAP affiliate company.

The information contained herein may be changed without prior notice. Some software products marketed by SAP SE and its distributors contain proprietary software components of other software vendors. National product specifications may vary.

These materials are provided by SAP SE or an SAP affiliate company for informational purposes only, without representation or warranty of any kind, and SAP or its affiliated companies shall not be liable for errors or omissions with respect to the materials. The only warranties for SAP or SAP affiliate company products and services are those that are set forth in the express warranty statements accompanying such products and services, if any. Nothing herein should be construed as constituting an additional warranty.

In particular, SAP SE or its affiliated companies have no obligation to pursue any course of business outlined in this document or any related presentation, or to develop or release any functionality mentioned therein. This document, or any related presentation, and SAP SE's or its affiliated companies' strategy and possible future developments, products, and/or platforms, directions, and functionality are all subject to change and may be changed by SAP SE or its affiliated companies at any time for any reason without notice. The information in this document is not a commitment, promise, or legal obligation to deliver any material, code, or functionality. All forward-looking statements are subject to various risks and uncertainties that could cause actual results to differ materially from expectations. Readers are cautioned not to place undue reliance on these forward-looking statements, and they should not be relied upon in making purchasing decisions.

SAP and other SAP products and services mentioned herein as well as their respective logos are trademarks or registered trademarks of SAP SE (or an SAP affiliate company) in Germany and other countries. All other product and service names mentioned are the trademarks of their respective companies.

See www.sap.com/copyright for additional trademark information and notices.