

A long-exposure photograph of a city at night, showing light trails from cars and buildings in shades of blue, orange, and yellow.

Development rush vs. security

Speed and security don't mix well? We beg to differ.

Fabian Sölker, Tobias Pahlings, SAP
December, 2022

PUBLIC

Agenda

Mentimeter

Current Situation

- German “Rückholprogramm”

Other Applications

- Approach
- Architecture
- Threat Modeling

Secure Development Lifecycle

Key Learnings

What is needed for a secure product?



Repatriation Application

“Rückholprogramm”



Back home in the cloud



15th March



Back home in the cloud

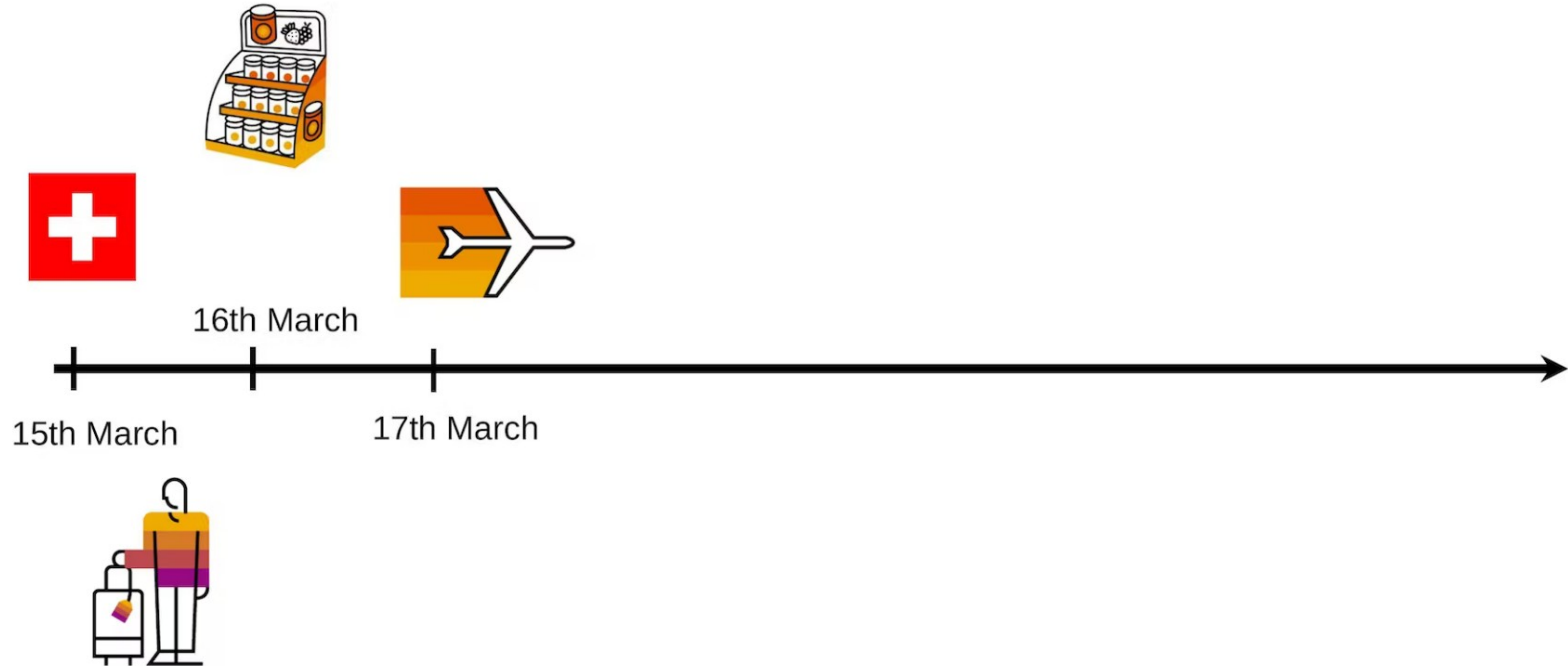


16th March

15th March



Back home in the cloud



Elektronische Erfassung von Deutschen im Ausland

- > Login
- > Registrierung
- > Aktivierung
- > Passwort vergessen

Login

E-Mail:

Passwort:

Login

Herzlich Willkommen auf der Startseite der Elektronischen Erfassung von Deutschen im Ausland (Elefand) !

Im Folgenden werden Sie durch die Schritte der Elektronischen Erfassung von Deutschen im Ausland (Elefand) geleitet.

Zur Erfassung Ihrer Daten in Elefand ist eine einmalige **Registrierung** nötig. Geben Sie dazu bitte Ihre E-Mailadresse sowie ein freigeschaltetes Passwort ein. Anschließend wird Ihnen per E-Mail ein Link zur **Aktivierung** Ihres Zugangs zugeschickt. Klicken Sie auf den in der E-Mail enthaltenen Link und geben Sie Ihr Passwort erneut ein, um den Registrierungsvorgang abzuschließen.

Nach der Aktivierung Ihres Zugangs erfolgt die **Erfassung Ihrer Daten**. Geben Sie dazu die Daten zu Ihrer Person, Ihrem Aufenthalt, der Sie begleitenden Personen und Kontaktpersonen in Deutschland in die dafür vorgesehenen Felder ein. Später können Sie durch **Login** jederzeit auf Ihre Daten zugreifen, um Änderungen oder Anpassungen vorzunehmen.

In der rechten Spalte finden Sie eine Bedienungsanleitung, die Ihnen die einzelnen Schritte erläutert. Bitte lesen Sie diese sorgfältig durch.

Hilfe

Bitte geben Sie zum Login Ihre E-Mailadresse und Ihr Passwort ein.

Achten Sie dabei auf Groß- und Kleinschreibung!

Falls Sie sich zum ersten Mal einloggen möchten, müssen Sie sich zuvor einmalig registrieren. Klicken Sie dazu auf **Registrierung**.

Hinweis

Eine effektive konsularische Hilfe und Unterstützung durch deutsche Auslandsvertretungen im Notfall setzt voraus, dass Namen, Aufenthaltsorte und Erreichbarkeiten von Deutschen im Ausland und ggf. auch den im Ernstfall zu kontaktierenden Personen im Inland bekannt sind.

Die deutschen Auslandsvertretungen führen dazu anhand Ihrer Eingaben Krisenvorsorgelisten der in ihrem Amtsbezirk ansässigen Deutschen und ihrer Familienangehörigen. Grundlage dafür ist § 6 Abs. 3 Konsulargesetz. Die Möglichkeit der Registrierung zur Einbeziehung in Maßnahmen der Krisenvorsorge und -reaktion besteht darüber hinaus auch für kurzzeitige Auslandsaufenthalte.

Elektronische Erfassung von Deutschen im Ausland

- > Login
- > Registrierung
- > Aktivierung
- > Passwort vergessen

Login

E-Mail:

Passwort:

Login

Hilfe

Bitte geben Sie zum Login Ihre E-Mailadresse und Ihr Passwort ein.

Achten Sie dabei auf Groß- und Kleinschreibung!

Falls Sie sich zum ersten Mal einloggen möchten, müssen Sie sich zuvor einmalig registrieren. Klicken Sie dazu auf [Registrierung](#).

Hinweis

Eine effektive konsularische Hilfe und

Herzlich Willkommen auf der Startseite der Elektronischen Erfassung von Deutschen im Ausland (Elefand) !

Im Folgenden werden Sie durch die Schritte der Elektronischen Erfassung von Deutschen im Ausland (Elefand) geleitet.

Zur Erfassung Ihrer Daten in Elefand ist eine einmalige **Registrierung** nötig. Geben Sie dazu bitte Ihre E-Mailadresse sowie ein freigeschaltetes Passwort ein. Anschließend wird Ihnen per E-Mail ein Link zur **Aktivierung** Ihres Zugangs zugeschickt. Klicken Sie auf den in der E-Mail enthaltenen Link und geben Sie Ihr Passwort erneut ein, um den Registrierungsvorgang abzuschließen.

Nach der Aktivierung Ihres Zugangs erfolgt die **Erfassung Ihrer Daten**. Geben Sie dazu die Daten zu Ihrer Person, Ihrem Aufenthalt, der Sie begleitenden Personen und Kontaktpersonen in Deutschland in die dafür vorgesehenen Felder ein. Später können Sie durch **Login** jederzeit auf Ihre Daten zugreifen, um Änderungen oder Anpassungen vorzunehmen.

In der rechten Spalte finden Sie eine Bedienungsanleitung, die Ihnen die einzelnen Schritte erläutert. Bitte lesen Sie diese sorgfältig durch.



Diese Webseite ist nicht verfügbar.

Neu laden

SAP

4:00 pm

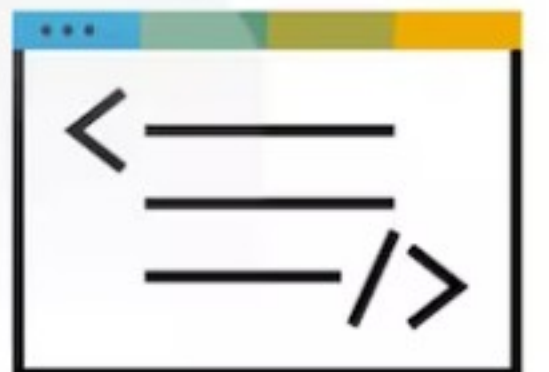


7:00 pm



Auswärtiges Amt

7:30 pm





This domain name has been registered with Gandi.net

View the WHOIS data for rueckholprogramm.de to see the domain's public registration information.

1:44 am



Want your own domain name?

Learn more about the domain name extensions we manage

Find a domain name similar to rueckholprogramm.de

10:00 am



Auswärtiges Amt

COVID-19 Rückholprogramm

Anmelden

E-Mail oder Benutzername

Kennwort

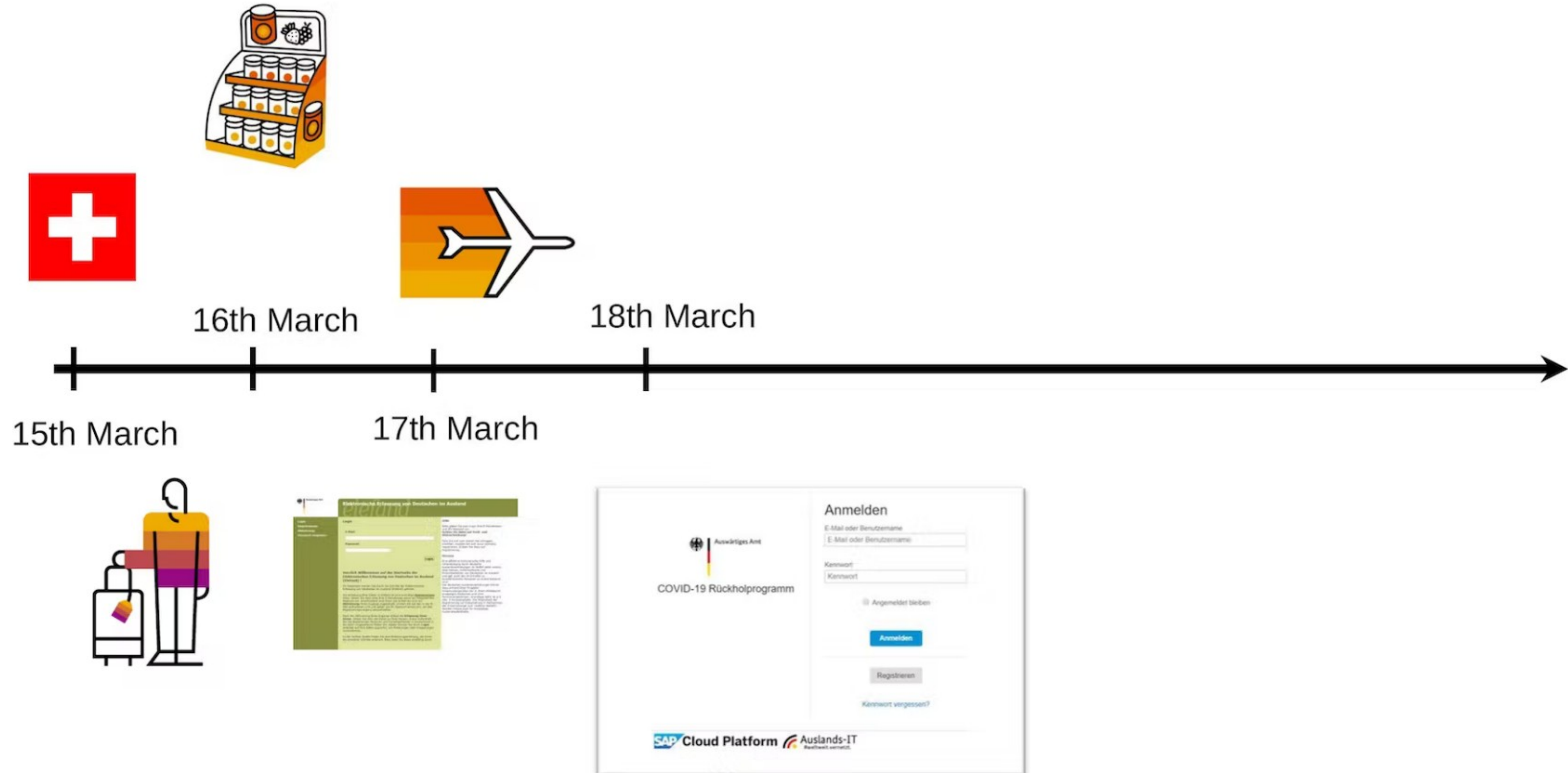
☐ Angemeldet bleiben

Anmelden

Registrieren

[Kennwort vergessen?](#)

Back home in the cloud





Auswärtiges Amt  @AuswaertigesAmt · Mar 19

#Rückholprogramm: In den Ländern, aus denen Rückholflüge der Bundesregierung stattfinden, sollten Sie sich jetzt über [rueckholprogramm.de](https://www.rueckholprogramm.de) melden! Für welche Länder derzeit Flüge geplant sind, erfahren Sie hier: diplo.de/rueckholaktion #COVID19 @AA_SicherReisen



99

145

233



SAP

2:30 pm



marvin @MarvinMoloczec · Mar 20

Falls noch jmd nicht mitbekommen hat: Es gibt eine neue Webseite für die Registrierung zum **#Rückholprogramm**
Diese funktioniert sogar



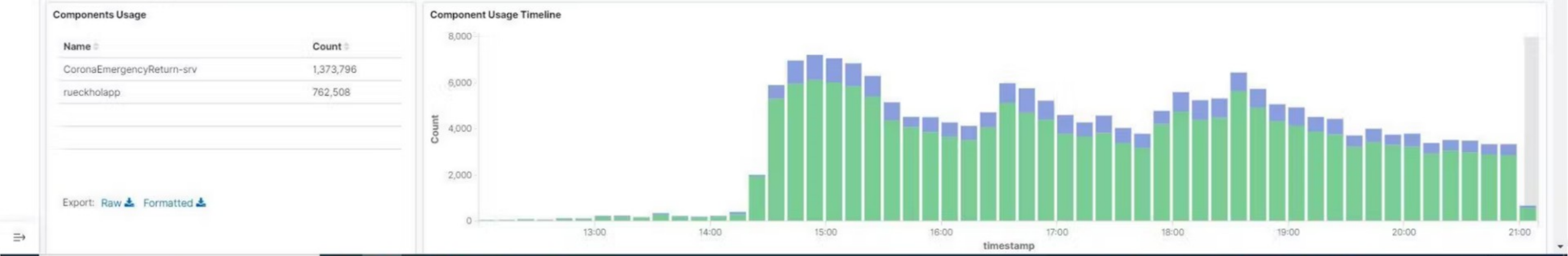
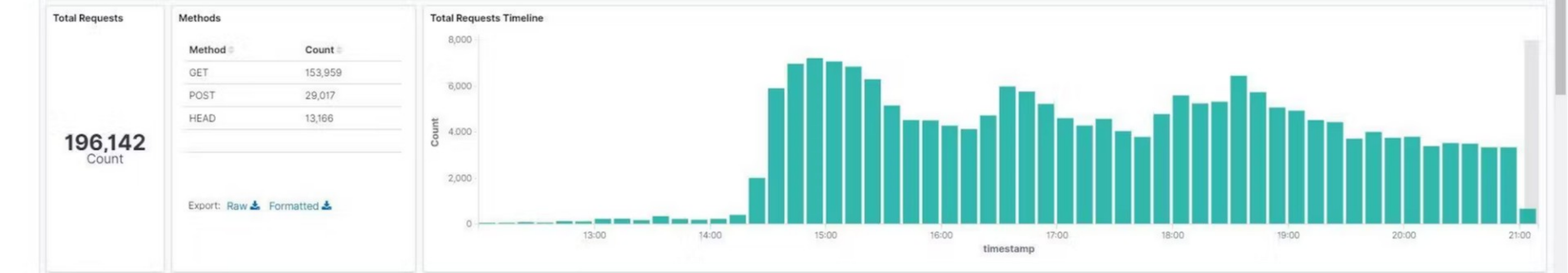
Auswärtiges Amt  @AuswaertigesAmt · Mar 19

#Rückholprogramm: In den Ländern, aus denen Rückholflüge der Bundesregierung stattfinden, sollten Sie sich jetzt über [rueckholprogramm.de](https://www.rueckholprogramm.de) melden! Für welche Länder derzeit Flüge geplant sind, erfahren Sie hier: diplo.de/rueckholaktion #COVID19 @AA_SicherReisen



2

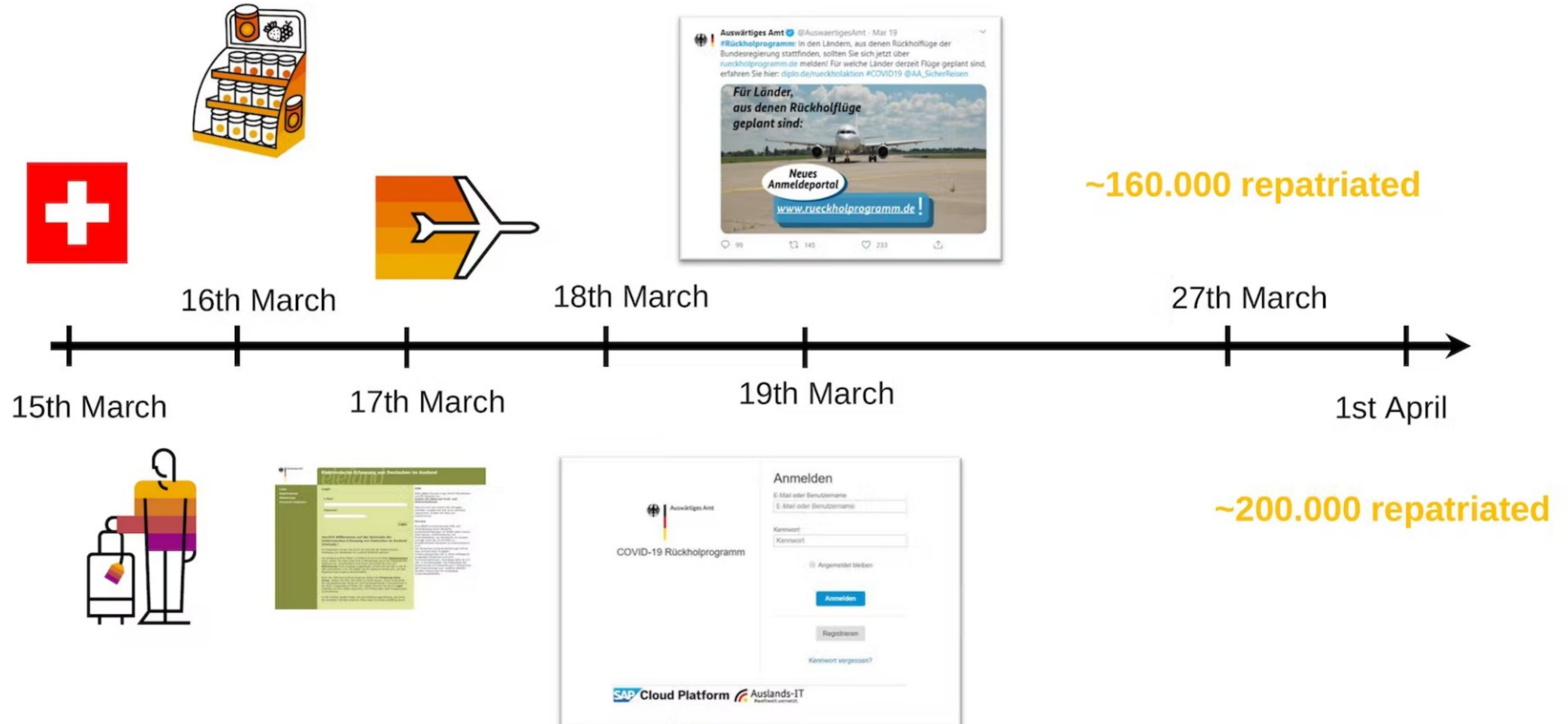




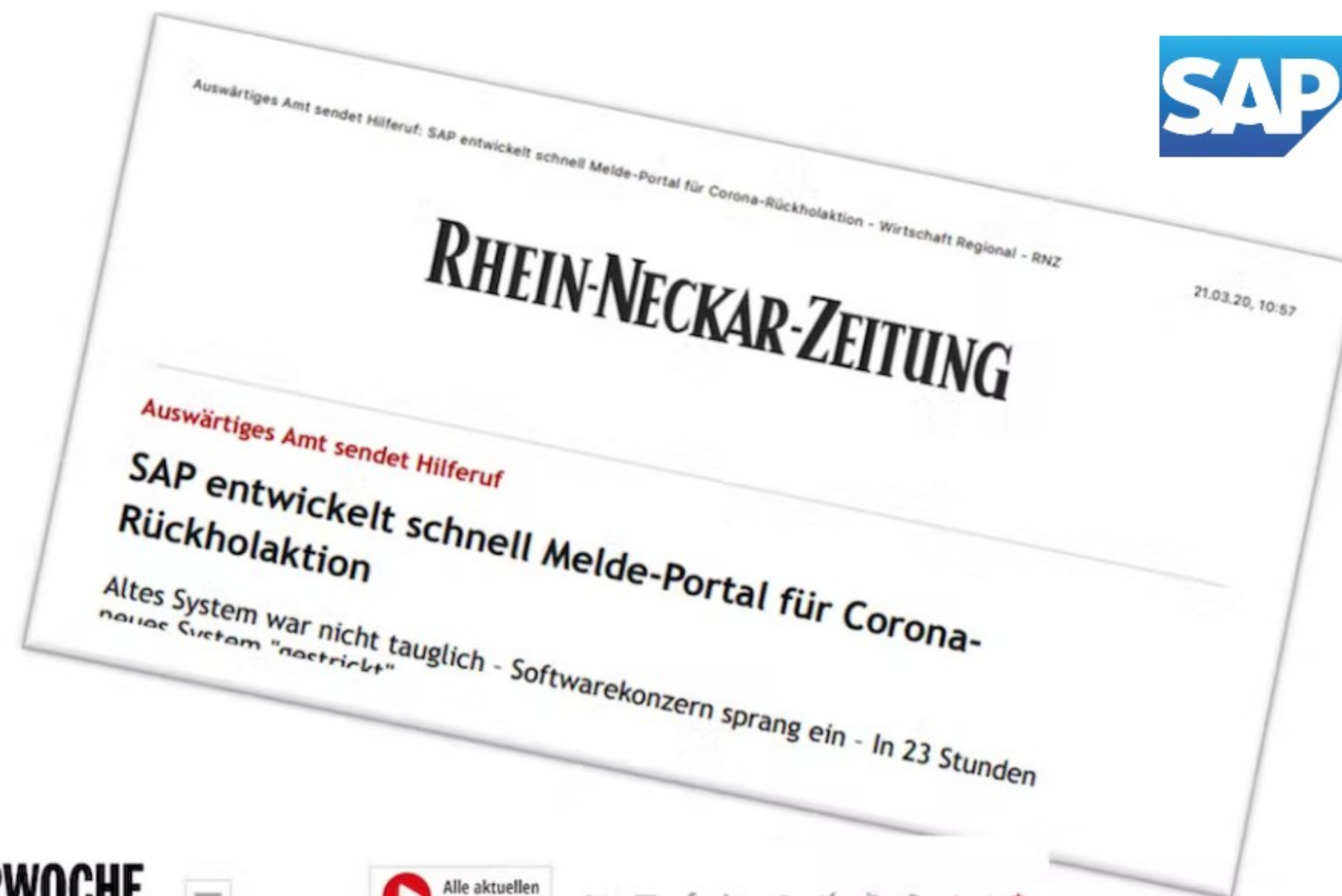
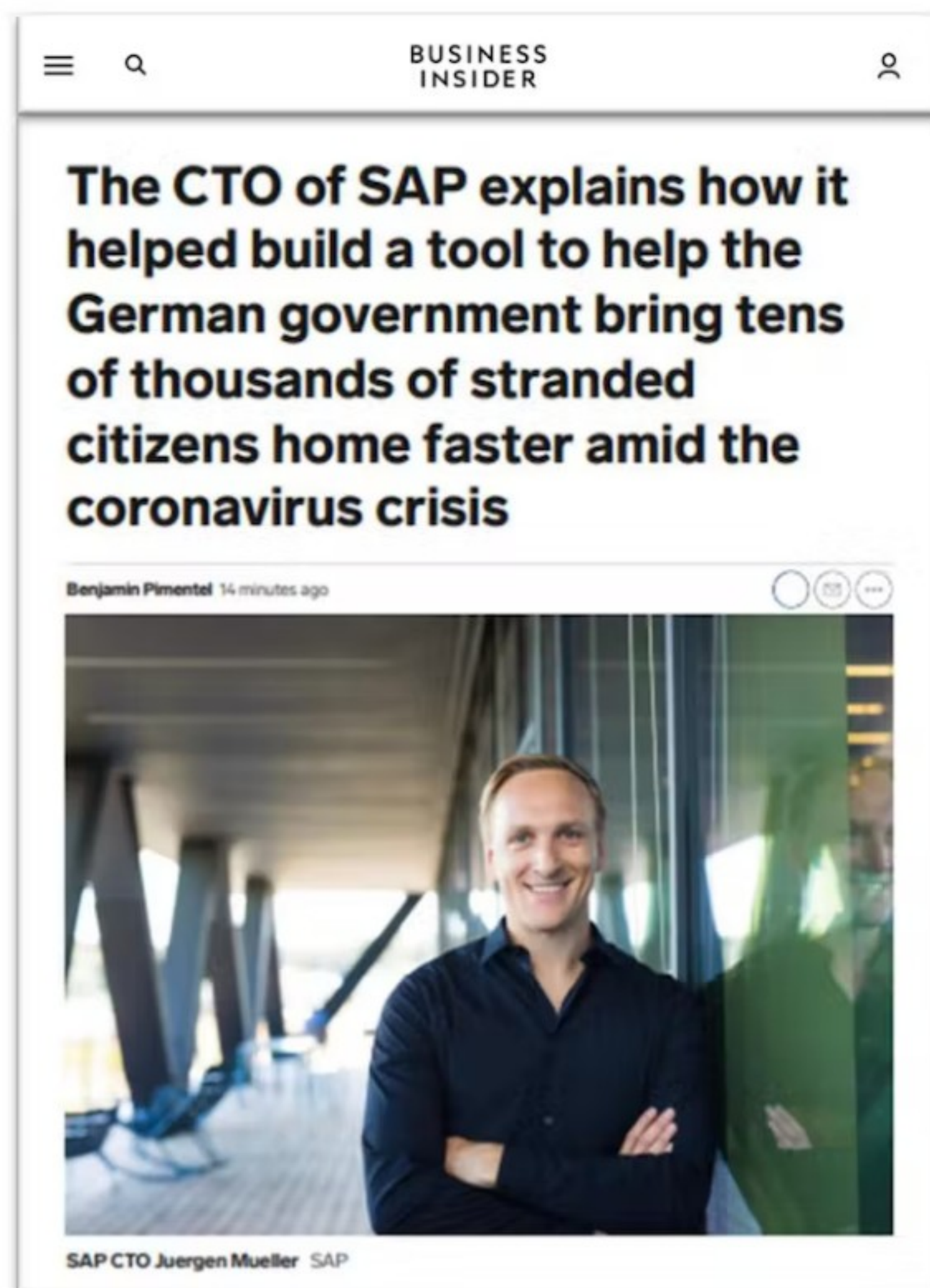
Back home in the cloud



Back home in the cloud



From the Press



Other Applications



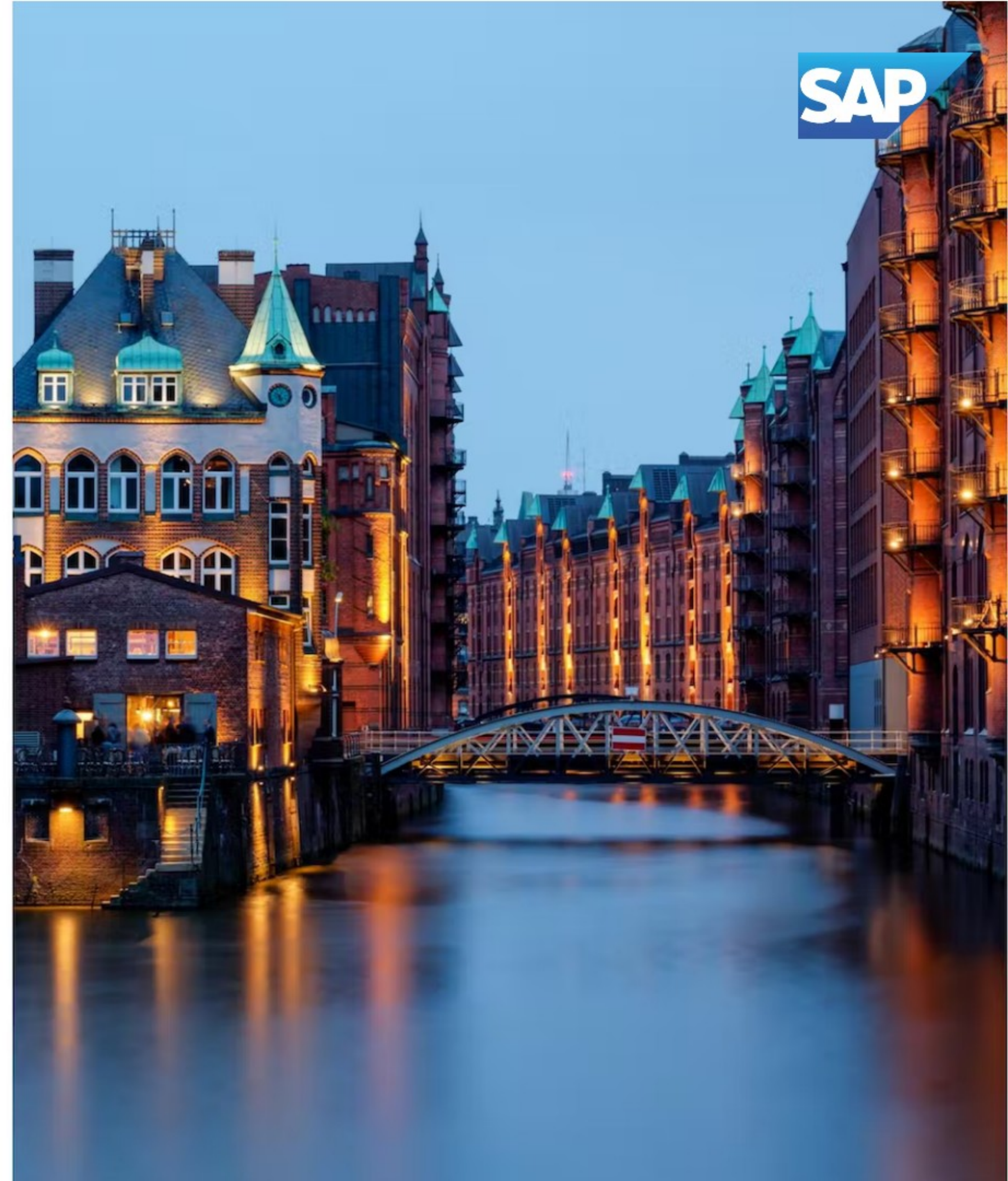
SAP Emergency Aid Request App

Background

- Corona Emergency Aid of the Hanseatic City of Hamburg: supports entities in need with up to 30,000 € per applicant.
- Over 100,000 applications for immediate aid were expected.

Solution

- Easy access via computer/mobile - stable performance even under high load.
- Customized development based on SAP Business Technology Platform and SAP HANA technology.
- Platform compliant with local legal requirements, GDPR and security standards
- Plausibility checks resulting in very low rate of requests requiring manual effort





Application needs to be ready quickly

- Goal of IFB Hamburg: go live on Monday, first payouts triggered Tuesday
- Application integration with SAP backend systems cannot be done in the “traditional way” due to time constraints → different infrastructure and app approach required



Application must be scalable & secure

- IFB Hamburg was expecting up to 100.000+ applicants in need of support to avoid bankruptcy and serious damage to their businesses.



Personal data needs to be collected & stored safely

- GDPR rules and local regulations must be obeyed. Security is of the utmost importance to avoid breaches as happened in Berlin¹

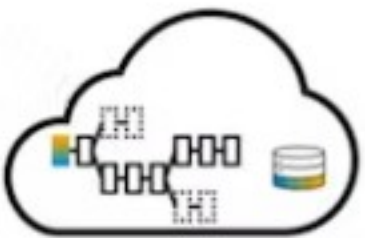
¹ <https://www.heise.de/newsticker/meldung/Corona-Soforthilfe-Datenpanne-bei-der-Investitionsbank-Berlin-4693603.html> (German)

SAP Business Technology Platform: fast, flexible & secure



Fast SAP Product Customization

- An expert team working through the weekend and nights delivered the app architecture, development and implementation within 3 days



SAP BTP as flexible technology layer

- Platform as a Service (PaaS) run and operated by SAP.
- Services and technologies used are adjusted to the demands of the customer.



High security standards ensure protection of sensitive data

- SAP Platform is compliant with GDPR, SOC2 and C5 Cloud Computing Compliance Criteria Catalogue.



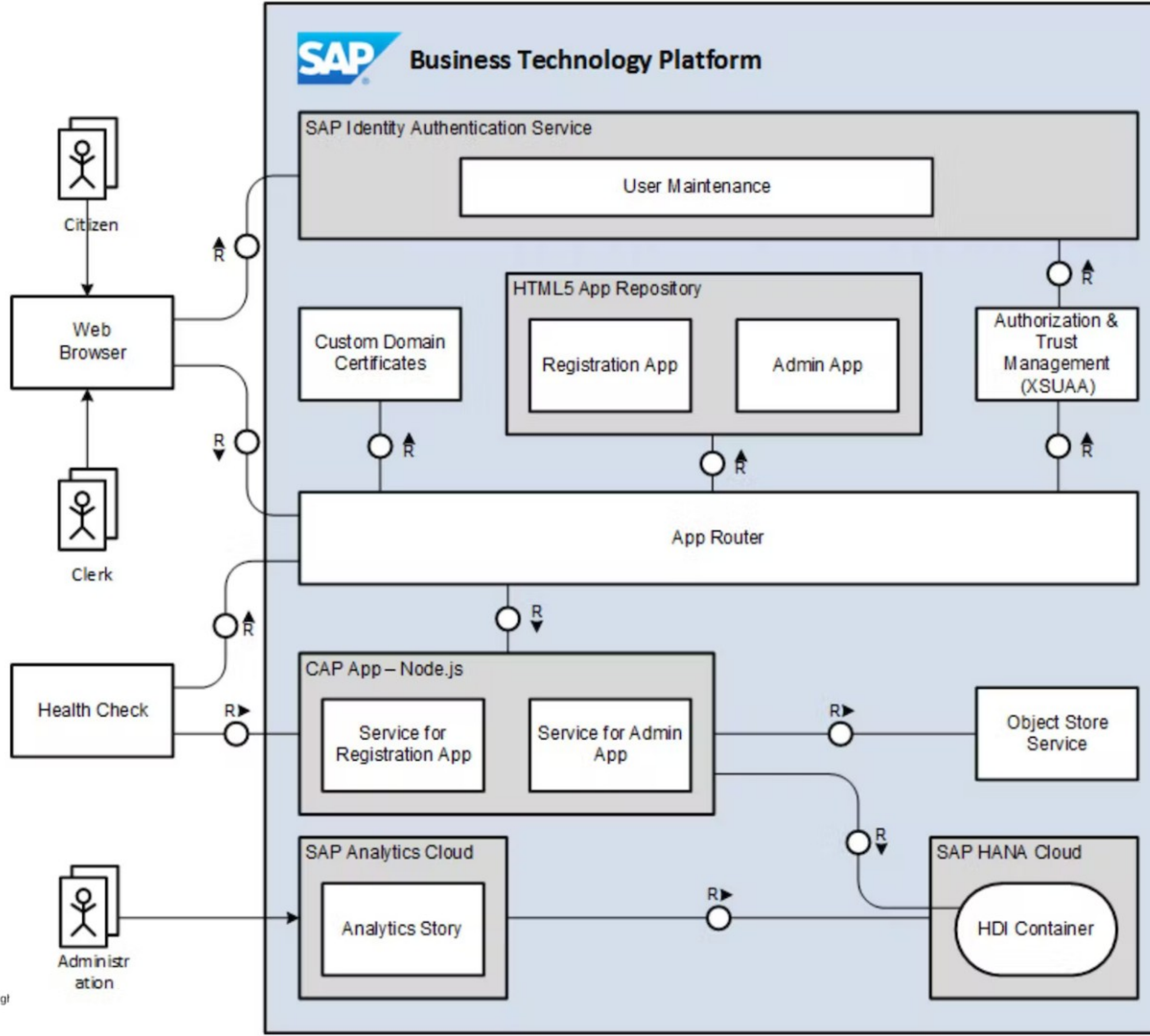
Highlight 1 (as of 01.04.)

- 65k+ registrations
- Over 50k+ applications
- 200.000 request per hour at peak
- 16.000 same-time user at peak
- <1% queries



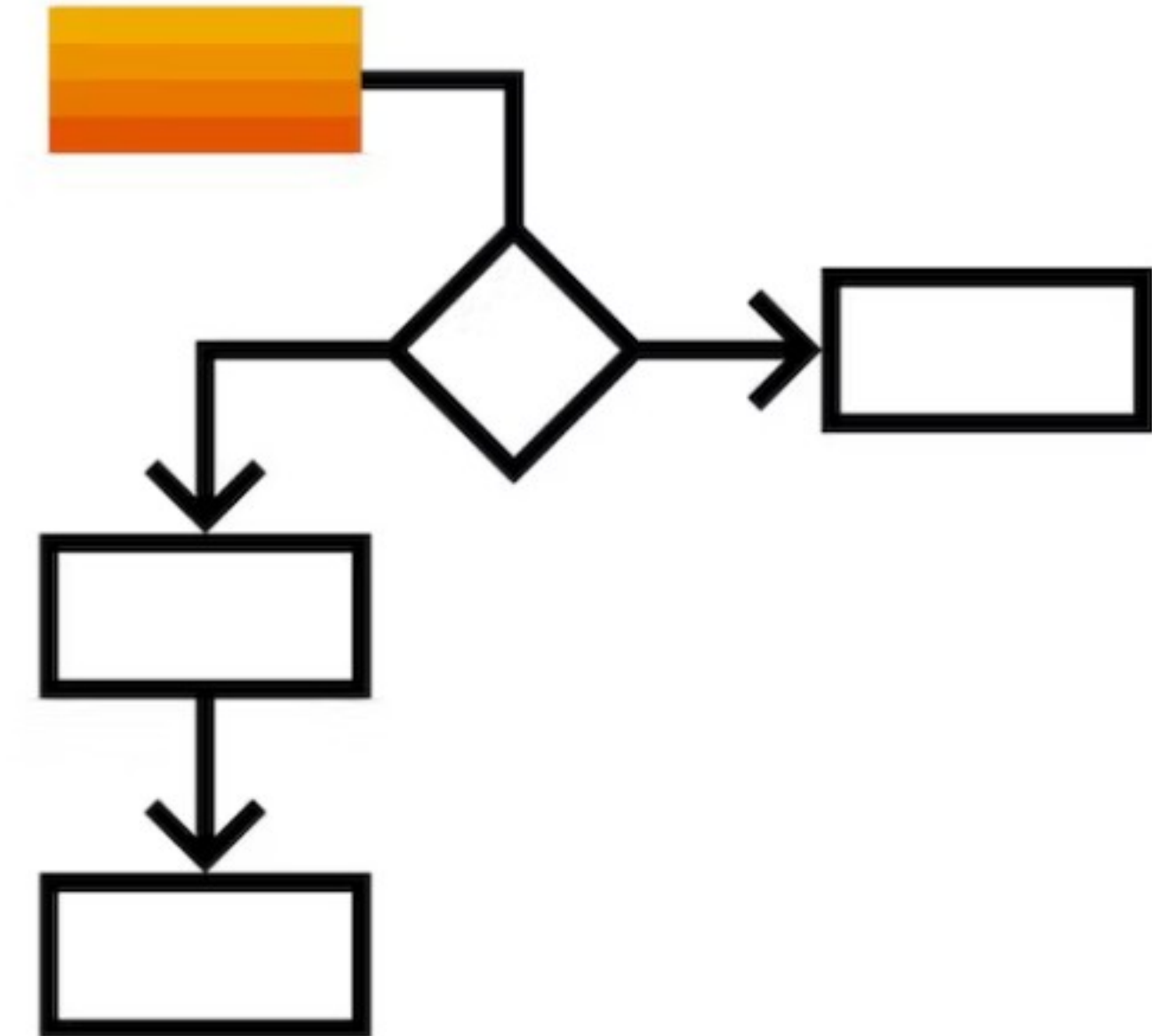
Highlight 2

- go live after 3 days
- 100+ person days delivered
- financial aid payout at go live day
- Over 330 Mio Euros support paid

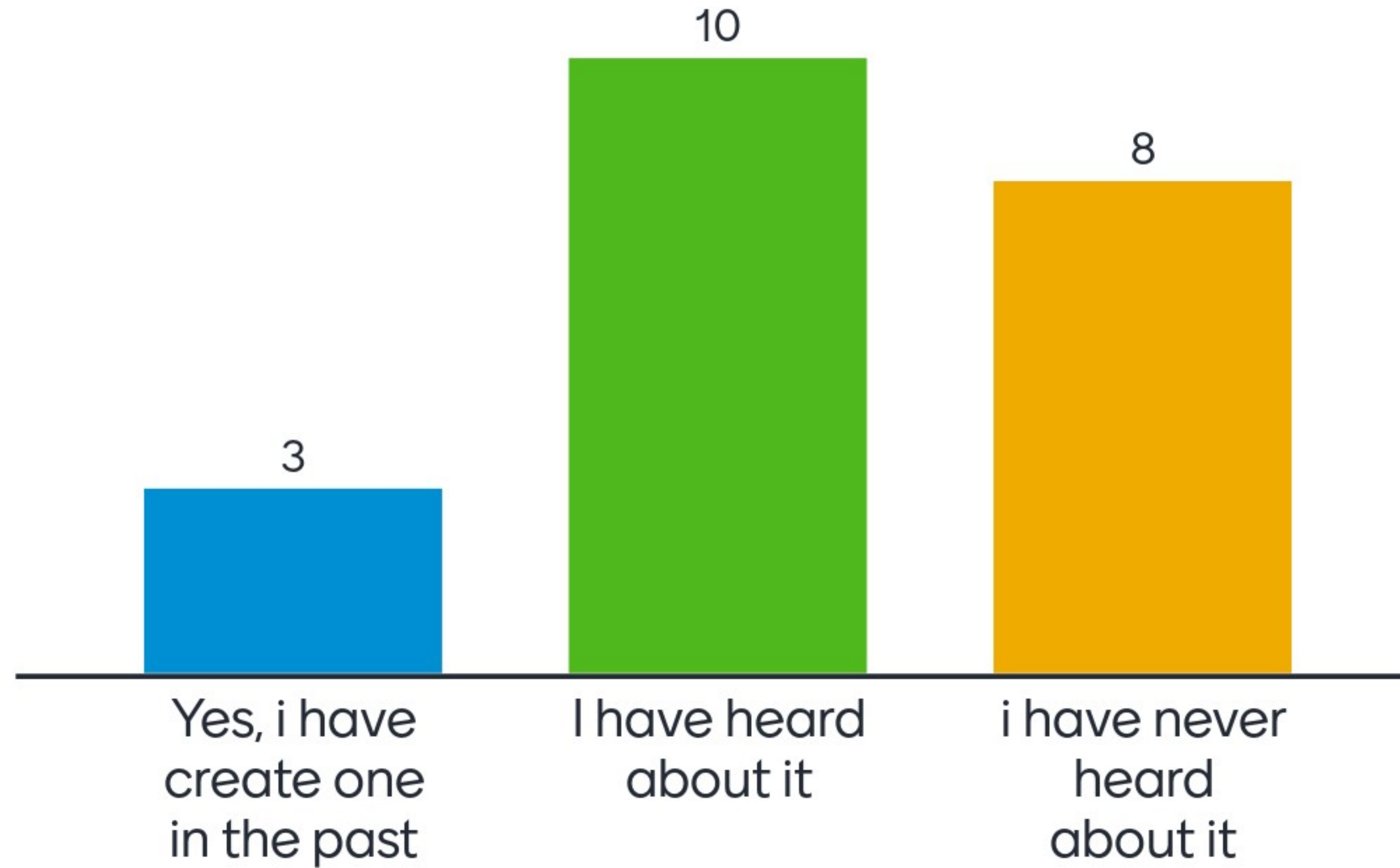


Threat Modeling

- Need for a methodology at the heart of development that help the teams to secure their products at design time.
- Security risks shall be known early in the development cycle so that proper mitigation and verification can be planned.
- Bring the correct Security Requirements, prioritized onto the Product Backlog
- Provide means for targeted testing and selection of test methodologies



Have you used Threat Modeling before



Basic terms – Microsoft STRIDE

Spoofing: Impersonating something or someone else

Tampering: Modifying data or code

Repudiation: Claiming to have not performed an action

Information Disclosure: Exposing information to illegitimate requesters

Denial of Service: Deny or illegitimately reduce service offering to users

Elevation of Privilege: Illegitimately, gain additional privileges / capabilities

Source “Microsoft: [The STRIDE Threat Model](#)”

Authentication

Integrity

Non-repudiation

Confidentiality

Availability

Authorization

Threats

**Security
Properties**

Threat Modeling - Risk Evaluation

$$\text{Risk} = \text{Impact} * \text{Ease of Attack}$$

Ease of attack = Advanced
Impact = Moderate

Risk = Medium Risk

Impact						
	Severe	medium	high	critical	critical	critical
	Significant	medium	medium	high	critical	high
	Moderate	low	medium	medium	high	medium
	Minor	low	low	medium	medium	low
		Very complex	Complex	Advanced	Easy	Regulation
How easy is the attack?						

Threat Modeling - Example



Spooxing

Tampering

Repudiation

Information Disclosure

Denial of Service

Elevation of Privilege

Authentication via Username / Password

Potential Issuers:

- Passwords leak
- Passwords can be guessed
- Password can be “cracked” by brute-force

Question: Would you consider using / trying it in the future?



Diese Slides wird duch eine Menti Umfrage ausgewechselt

Secure Software Development Lifecycle



Secure Software Development Lifecycle (S2DL)



Preparation



Development



Transition

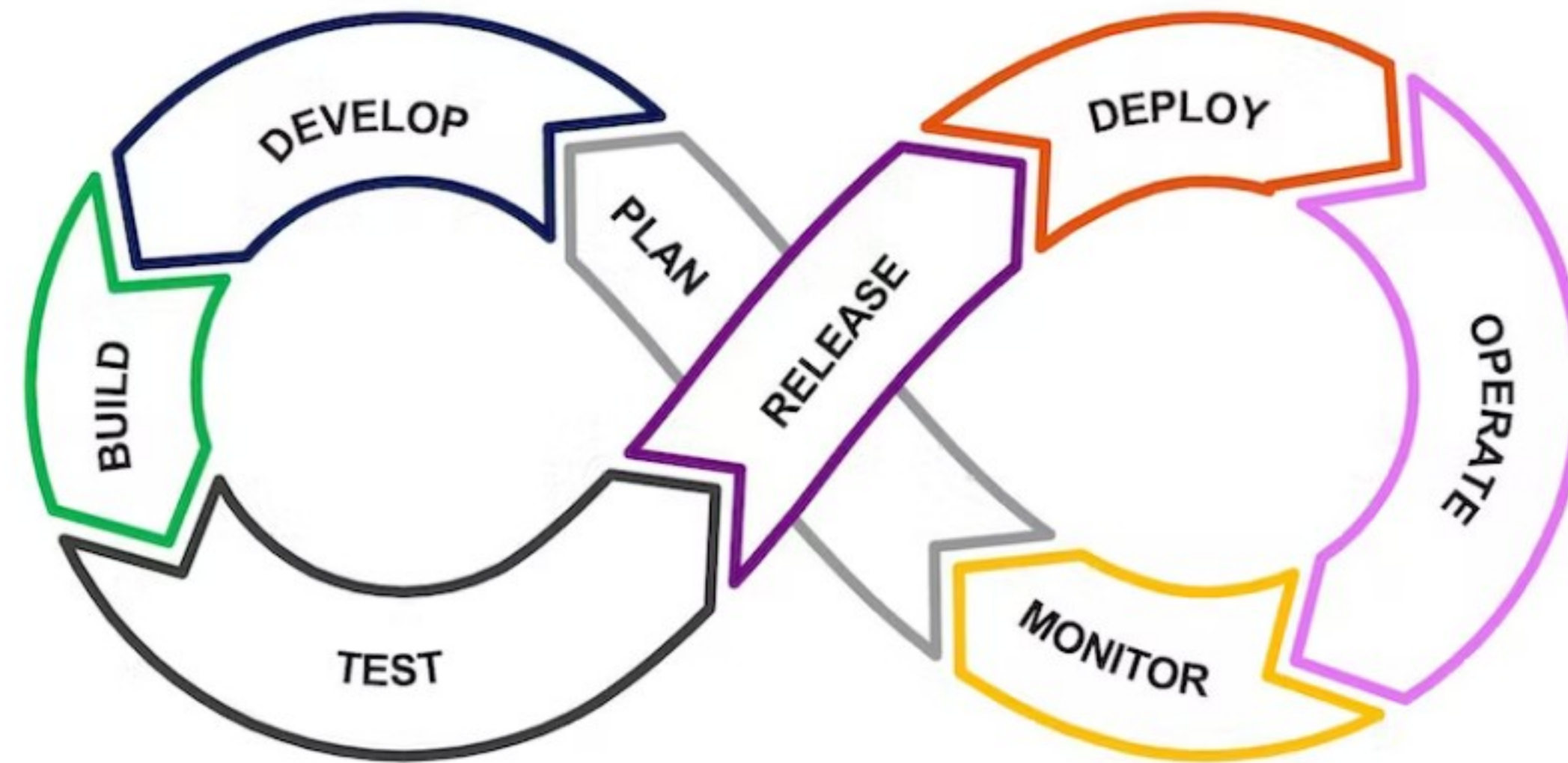


Utilization

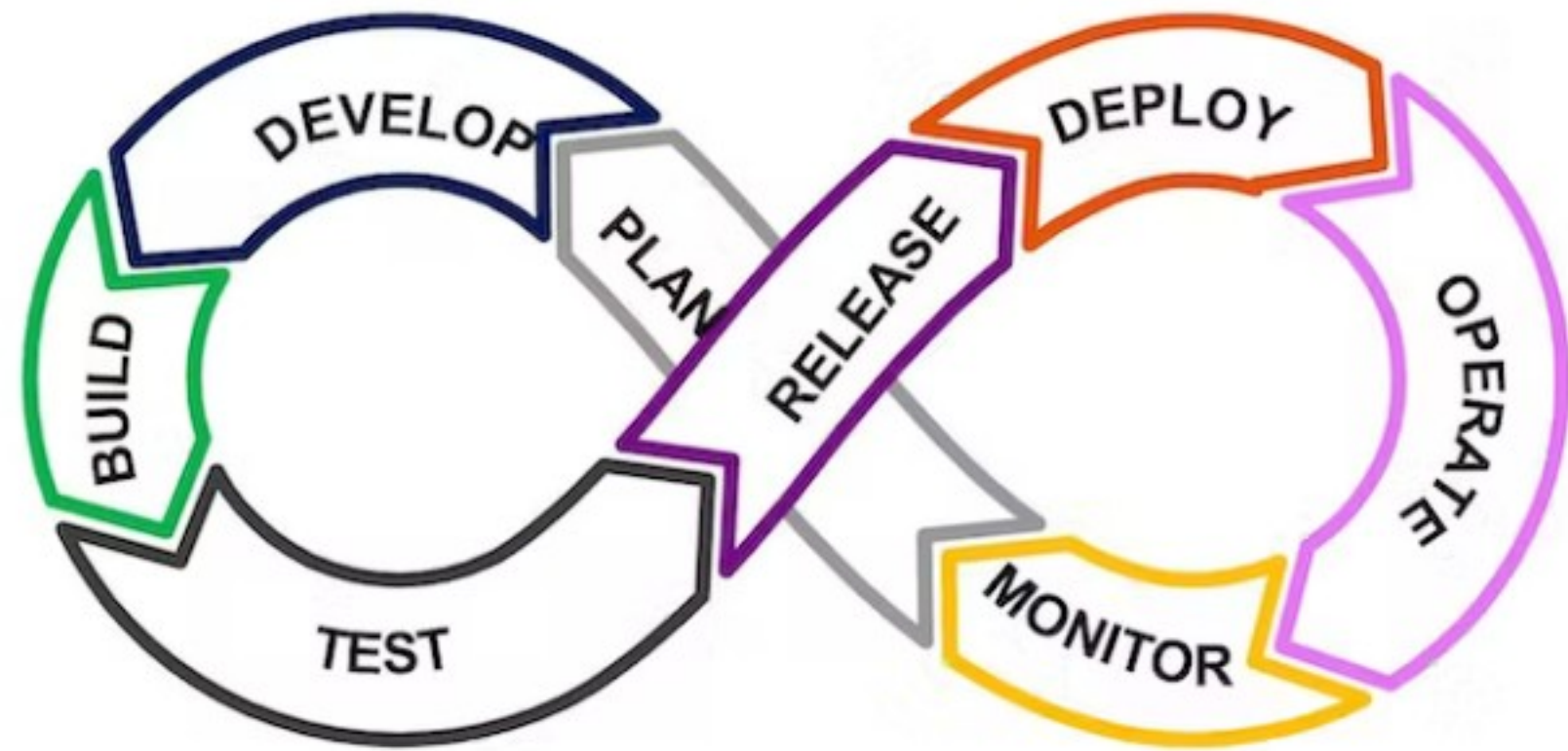


Security Awareness	Threat Modeling	Plan Security Features	Secure Programming	Manual Testing	Security Assessment	Incident Management
Secure Programming	DPP Evaluation	Plan DPP Features	Static Code Scans	Dynamic Testing	DPP Assessment	
Data Protection and Privacy	Product Standard Assessment	Plan Incident Response	OSS Vuln. Scans	Penetration Testing		
Security Testing			Unit Tests			
...			Code Reviews			

Secure Software Development and Operations Lifecycle (S2DOL)



Secure Software Development and Operations Lifecycle (S2DOL)



PLAN	DEVELOP	BUILD	TEST	RELEASE	DEPLOY	OPERATE	MONITOR
Training							
Product Standard Security							
Tools / Pipeline / Repository Security							
Threat Modelling*		Unit Tests	Manual Tests	Sec. Validation	Rel./Feat. Mgt.	Patch and Vuln. Mgt.	
DPCE			Pentest	Rel. Decision		Bus. Cont. Mgt.	Monitoring**
Security and DPP plan*			Account Mgt.	Incident/Breach Mgt.			
Network Architecture			Secure Backup Mgt.	Bug Bounty Progs.			
	Coding Guidelines		Cloud Asset Mgt.				
	Code Reviews						
	SAST		DAST				
OS3 Strategy	OS3/3rd Party Scans and Lifecycle Mgt.						

Lessons **Learned**



Key Learnings



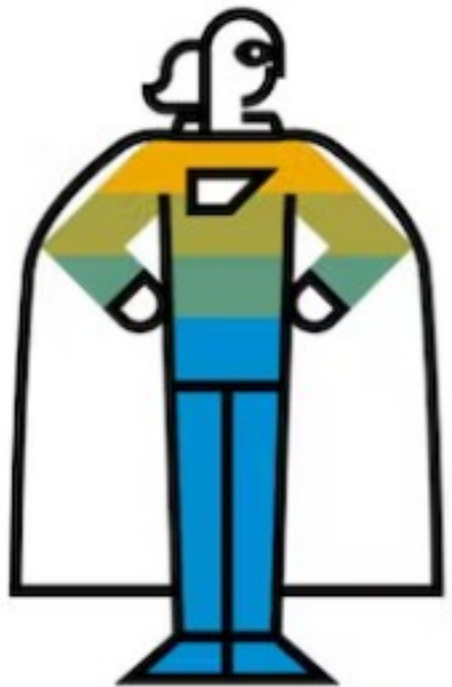
Testing



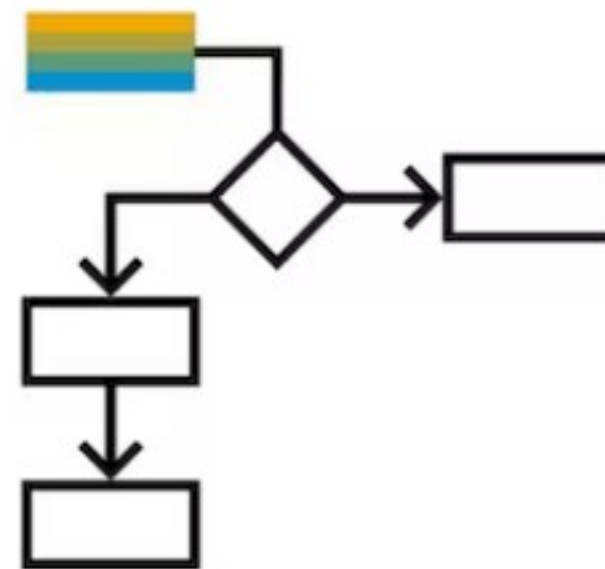
Requirements Management



Commitment



Experienced and Empowered Team



Threat Modelling



Breaks

References

- [The Secure Software Development Lifecycle at SAP](#)
- [The STRIDE Threat Model](#)



Questions?



4 questions
0 upvotes

Thank you.

Contact information:

Fabian Sölker
BTP Consultant

Tobias Pahlings
Security Consultant



Follow us



www.sap.com/contactsap

© 2022 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/trademark for additional trademark information and notices.