



SAP Bug Bounty Program for SAP S/4HANA

Patrick Boch, Product Manager SAP S/4HANA Security, SAP SE

Ravishankar Sahadevan, Global Lead S/4HANA Bug Bounty & COO S/4HANA Security, SAP SE

July 21st, 2022

PUBLIC

Disclaimer

The information in this presentation is confidential and proprietary to SAP and may not be disclosed without the permission of SAP. Except for your obligation to protect confidential information, this presentation is not subject to your license agreement or any other service or subscription agreement with SAP. SAP has no obligation to pursue any course of business outlined in this presentation or any related document, or to develop or release any functionality mentioned therein.

This presentation, or any related document and SAP's strategy and possible future developments, products and or platforms directions and functionality are all subject to change and may be changed by SAP at any time for any reason without notice. The information in this presentation is not a commitment, promise or legal obligation to deliver any material, code or functionality. This presentation is provided without a warranty of any kind, either express or implied, including but not limited to, the implied warranties of merchantability, fitness for a particular purpose, or non-infringement. This presentation is for informational purposes and may not be incorporated into a contract. SAP assumes no responsibility for errors or omissions in this presentation, except if such damages were caused by SAP's intentional or gross negligence.

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, which speak only as of their dates, and they should not be relied upon in making purchasing decisions.

Agenda

The Security of SAP S/4HANA

What is Bug Bounty?

Why Bug Bounty?

Where to report security issues to SAP?

Bug Bounty @S/4HANA

The Security of SAP S/4HANA



Confidence in SAP S/4HANA Security through a holistic approach

Security is integrated into SAP Company Processes



Secure Cloud Software Development



Leading Security and DPP Products & Features



Secure Operations & Landscape Architecture



Security Products

- Risk based approach aligned to ISO 27034
- Threat modelling
- Code scans
- Data Protection & Privacy assessment (DPCE)
- Internal & external security assessment
- Continuous security fixes and enhancements
- SAP S/4HANA Bug Bounty Program
- Digitally signed code
- Security validation

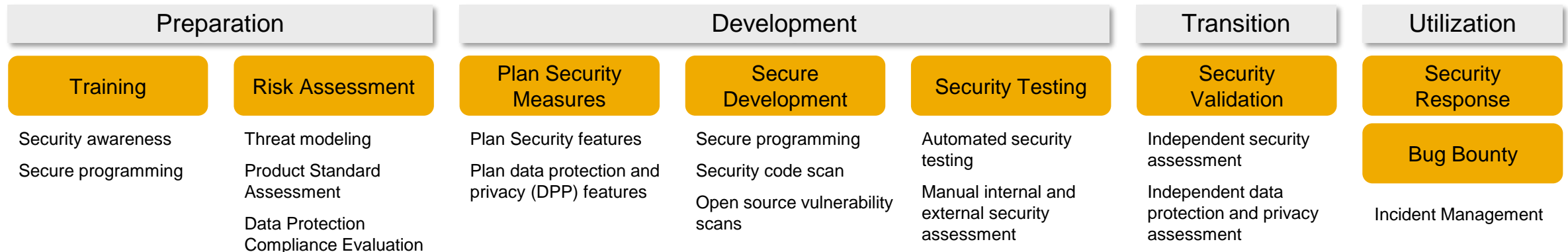
SAP Secure Software Development and Operations Lifecycle

From Risk Assessment to Security Validation

The Secure Software Development and Operations Lifecycle is the framework at SAP to develop software that fulfills both Security and Data Protection & Privacy requirements.

SAP follows a risk-based approach to efficiently achieve security within economic boundaries:

- Product teams first identify security risks by conducting security risk assessments
- Performing security activities to embed security in the product and verify its effectiveness for the identified risks

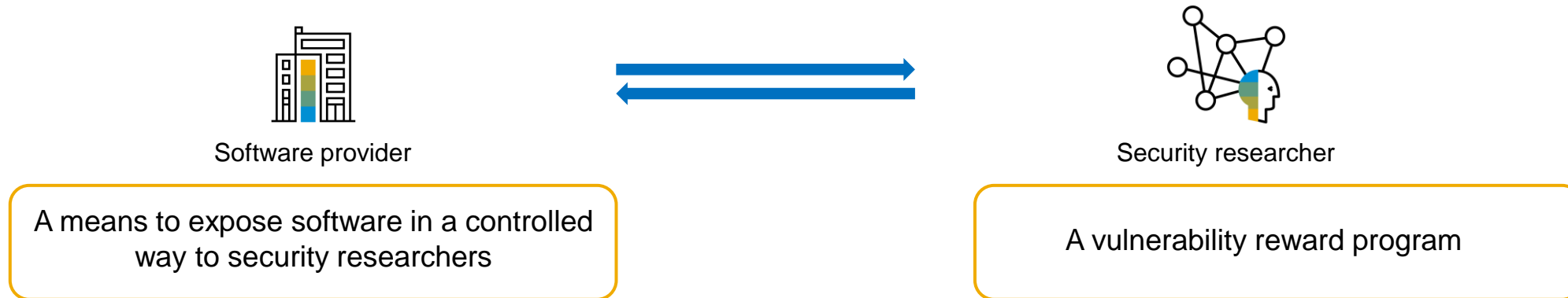


Common denominator: Product standard security as knowledge base across all phases

What is Bug Bounty?

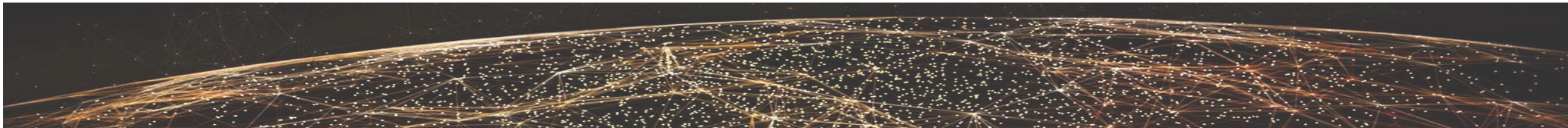


Bug bounty history and basics



”Crowdsourced Penetration Testing”-
Ethical hackers are rewarded for finding vulnerabilities

- Strict rules for what is in scope and what is out
- Responsible disclosure of findings
- Rewards (bounties) are paid according to criticality of the finding based on CVSS ([Common Vulnerability Scoring System](#))



Why Bug Bounty?





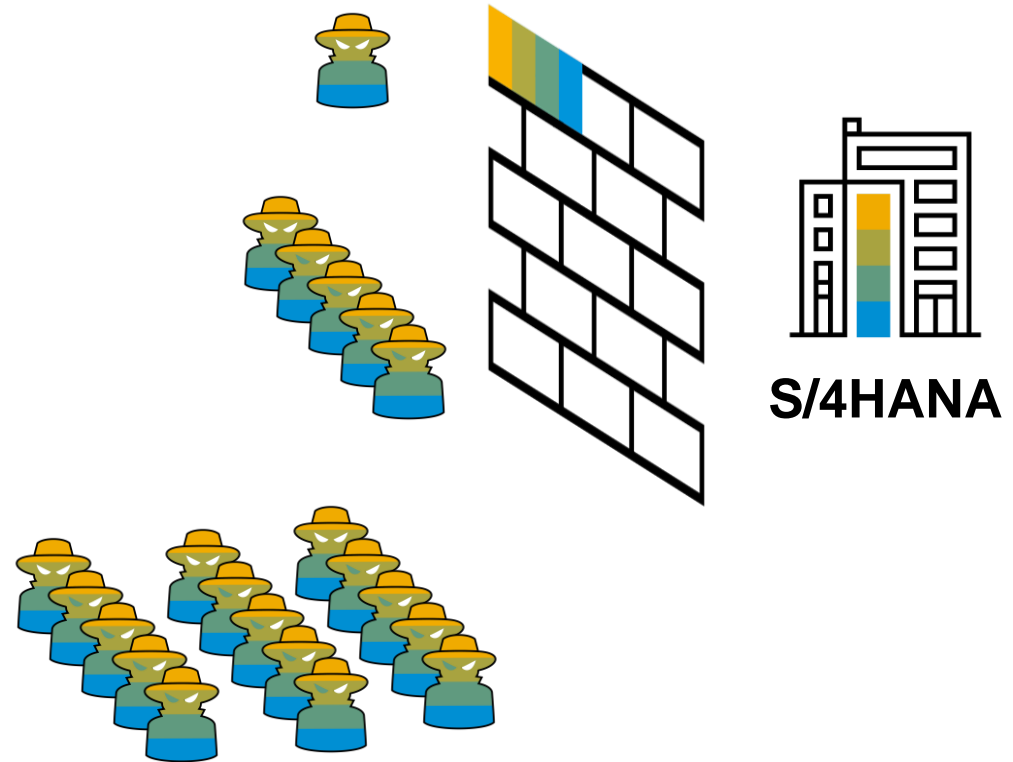


Offensive Security Testing

Penetration Tests

Hacking Simulations (Red Team)

Bug Bounty



SAP's journey to bug bounty program

2016

Public “Hall of Fame” for security researchers submitting vulnerabilities to SAP Secure Inbox

2017 - 2021

Set up and continuous evolution of bug bounty programs at SAP

2022 onwards

General availability of bug bounty programs for all interested applications at SAP

- One of the main sources for vulnerability findings beside general vulnerability reports and customer disclosures
- 75% true positive rate
- 17% of disclosures rated with CVSS higher than 7.0
- Reward range between \$100 and \$4000 to submissions with CVSS scores between 2.9 and 9.6
- Average payout **\$983** per vulnerability
- Findings range from simple vulnerabilities to design flaws



Bug Bounty vs Conventional Security Testing

Bug Bounty

- After product release
- Defined scope (in / out of scope definition)
- Ongoing
- As many testers as you like
- Regular scope extensions
- Private and public programs
 - Private:** Invited hackers only
 - Public:** All hackers who are registered with the bug bounty platform service provider

Conventional security testing

- During the development lifecycle of a product
- Narrow scope
- One time activity at a set point in time with limited pen testers

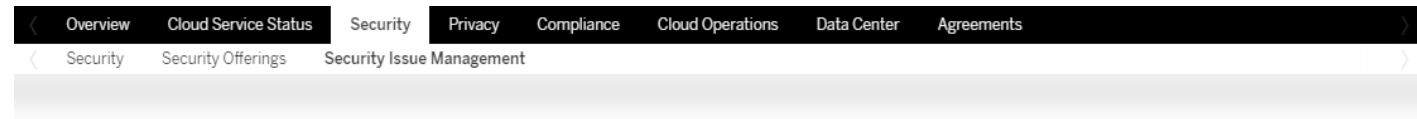
Bug Bounty in the Secure Software Development and Operations Lifecycle



Where to report security issues to SAP?



Product Security Findings



Report a Security Issue

SAP is committed to identifying and addressing security issues that affect our software and cloud solutions. We are continuously working on improving our security processes. To report a potential security issue, choose from the options below.



SAP customers

Report a customer security issue by using the SAP ONE Support Launchpad to find a solution and get real-time support from an expert.

[View the launchpad](#)



Security researchers

Inform the SAP Security Response Team of a security issue by completing and submitting the security vulnerability form.

[Access the form](#)

Note: Include the following details in the report, as applicable, so that we can better analyze the nature and scope of the security issue: issue category, affected product version with support package and patch level, necessary pre/post-conditions for the exploit to work, description with proof of concept or exploit code, and impact of the issue if exploited.

<https://www.sap.com/about/trust-center/security/incident-management.html>

[Get the public PGP key](#)

[Learn more about disclosure guidelines](#)

SAP Security Patch Day and Researcher Acknowledgement

[Products](#)[Industries](#)[Services and Support](#)[Learning](#)[Community](#)[Partner](#)[About](#)[Try & Buy](#)

SAP Security Patch Day



Fix vulnerabilities discovered in SAP products

Review notes from our monthly SAP Security Patch Day to learn about vulnerabilities discovered in SAP products and apply patches to protect your SAP landscape.

[Read the SAP Security Patch Day blog](#) >



Join us in acknowledging our security researchers

Learn about the security researchers who help us identify and solve security vulnerabilities, so we can help maintain the security and safety of our customers and partners.

[See the list of security researchers](#) >

Contact us

SAP Trust Center – Security – Security Issue Management

Bug Bounty @ S/4HANA



SAP S/4HANA Bug Bounty Program – Overview

Goal



To establish an **external security verification platform** for **S/4HANA** to **financially incentivize** responsible disclosure by external security researchers and **leverage** synergy of **crowdsourced security testing**

Collaboration



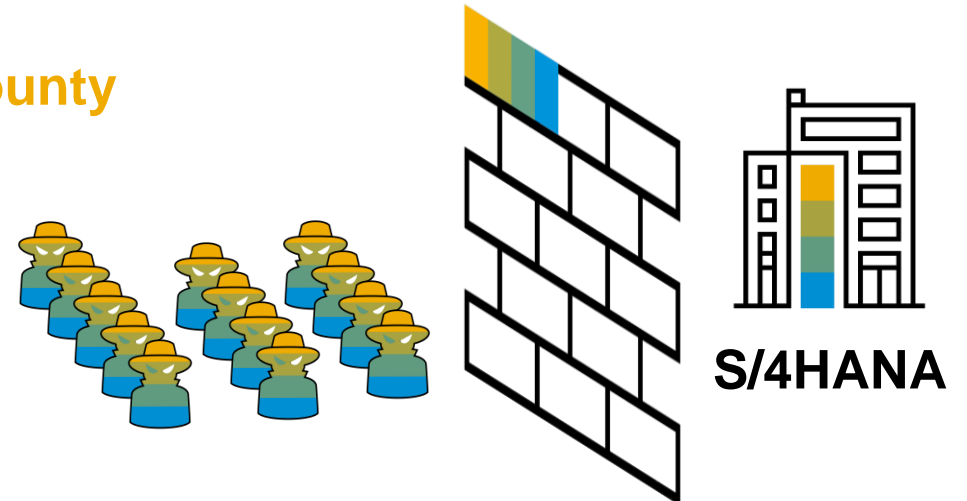
Launched through **SGS Bug Bounty Service** and
Operated by **BugBounty Platform Provider**

Advantage



Continuous external security verification **post General Availability (GA)** of S/4HANA with **high external visibility**. Reported findings **improve the security of S/4HANA (On Premise & Cloud)**

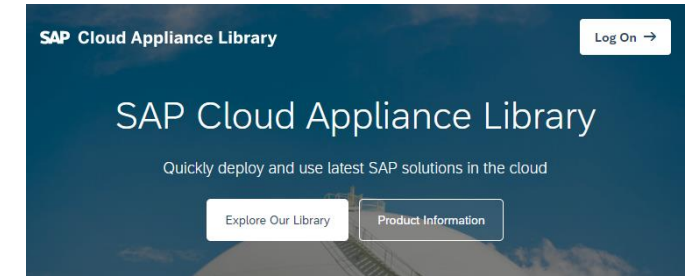
Bug Bounty



SAP S/4HANA Bug Bounty Program – Focus On-Premise

Systems

- S/4HANA On-Premise is used based on the Fully Activated Appliance from SAP Cloud Appliance Library (CAL), e.g.
<https://cal.sap.com/catalog#/solutions/a0b63a18-0fd3-4d88-bbb9-4f02c13dc343>



Scope

- First release in 2019
 - S/4HANA On-Premise 1809 FPS01 with activated functional scope: SAP Finance
- Second release in 2020
 - S/4HANA On-Premise 1909 FPS02 with activated functional scope: SAP Finance and SAP Transport Mgmt
- Current release in 2022
 - S/4HANA On-Premise 2020 FPS01 with activated functional scope: SAP Finance, SAP Transport Mgmt, Logistics & Sales and Distribution

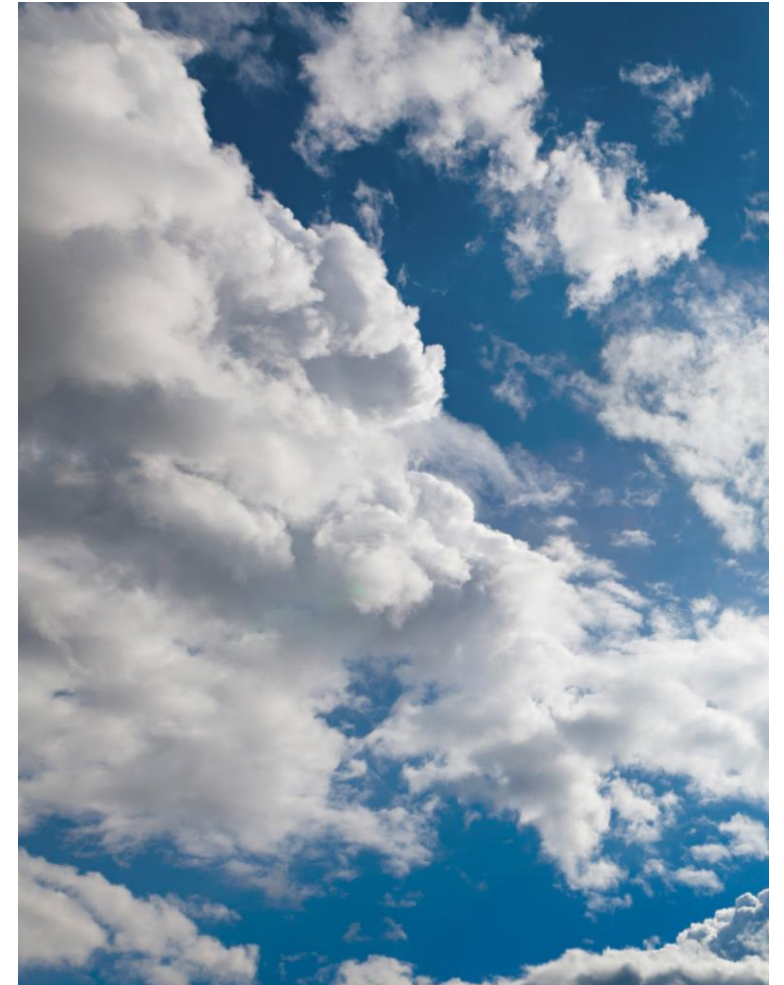
SAP S/4HANA Bug Bounty Program – Focus Cloud

Systems

- S/4HANA Cloud is an isolated tenant in the production landscape based on the S/4HANA Cloud Starter Edition

Scope

- First release in 2022 (S/4HANA Cloud 2202) with selected scope in certain areas
 - Accounts Payable
 - General Ledger
 - Master Data
 - Post Goods Movement



SAP S/4HANA Bug Bounty Program – Highlights & Challenges

Highlights



- High value findings (P1 & P2)

42

Total
submissions

\$

~1900

Average reward

400+

Security
researchers

72%

True
positive rate

Standard Reward Ranges

- P1| \$(4000-5000)
- P2| \$(2000-3500)
- P3 |\$(1500-700)
- P4| \$(500-250)

Promotional Reward Ranges (Live-S/4H OP)

- P1| \$(6000-8000)
- P2| \$(4000-5000)
- P3 |\$(1000-2000)
- P4| \$(350-600)

Challenges



- **Tailored** Application scope
- **Test-Data** for the applications
- **Managing / Verifying hardening** for every layer (Application, Platform, DB, OS, IaaS)
- **Compliance** to SAP Global Security checklist
- Regular **Maintenance & Monitoring**
- **Budget** for Bug Bounty
- Managing **continuous traction**
- **Sustaining** the Bug Bounty program
- **Running a bounty service** for S/4HANA On-Premise

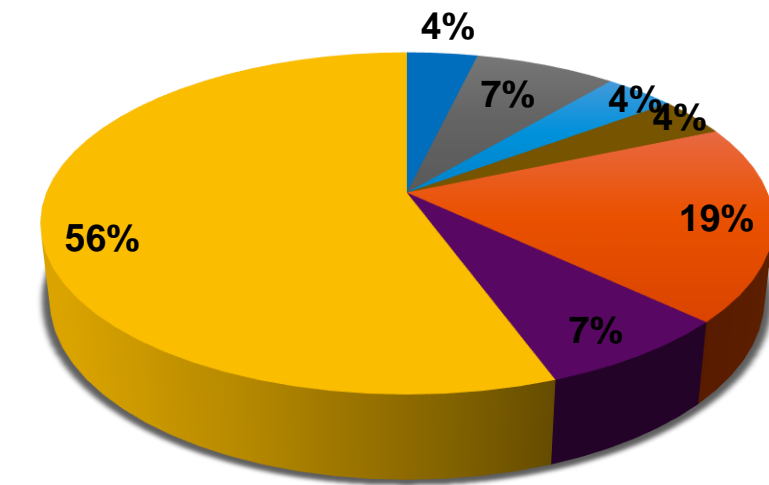
SAP S/4HANA Bug Bounty Program – Learnings & Vulnerability Overview

Learnings



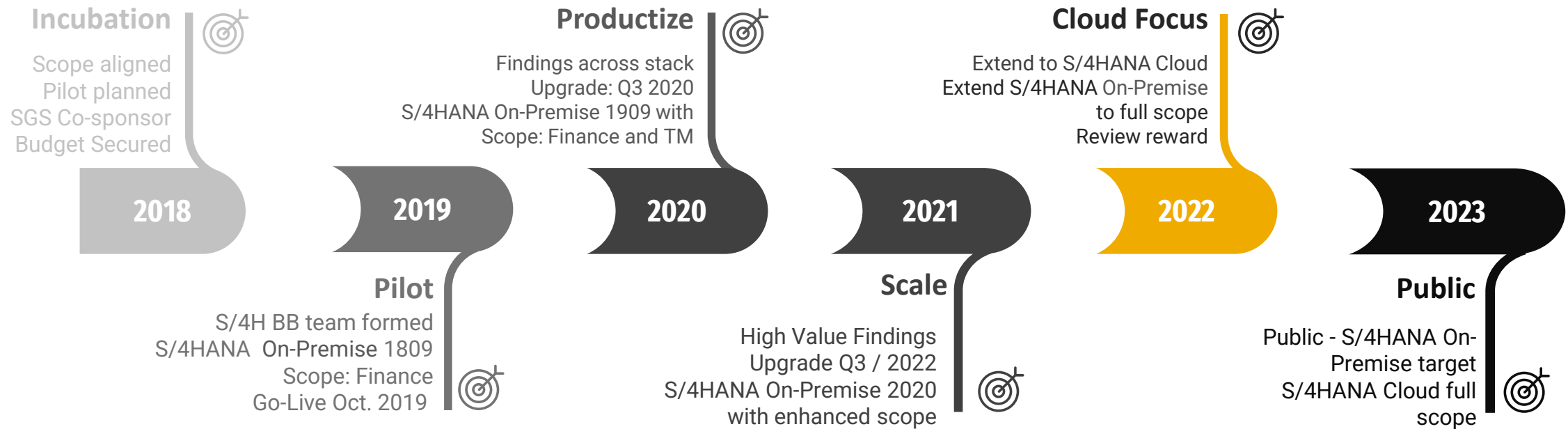
- **Start with small scope** & plan for full scope enablement via roadmap
- **Invest in application knowledge**
- Managing **continuous traction** via onboarding researches, scope, enhancements, reward structure
- **High True positive** rates of findings
- Researches provide **new vulnerability patterns / ideas**

Vulnerability Analysis



- | | |
|-------------------------------|--------------------------|
| ■ Denial of Service | ■ Information Disclosure |
| ■ Missing Authorization Check | ■ Missing XML Validation |
| ■ Other | ■ URL Redirection |
| ■ Cross Site Scripting | |

SAP S/4HANA Bug Bounty Program – Roadmap



Thank you.

Contact information:

Patrick Boch

Product Management, S/4HANA Security

E-mail: patrick.boch@sap.com

Ravishankar Sahadevan

Global Lead S/4HANA Bug Bounty & COO

S/4HANA Security

E-mail: ravishankar.sahadevan@sap.com

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.