// ROBERT PHILIPPS
@rophilipps

ist Software Engineer bei eBay im "Trust & Safety"-Team von eBay Kleinanzeigen.

BUG-BOUNTY-PROGRAMME

WILL THERE STILL BE ROBBERS EVEN IF YOU OFFER THEM JOBS AS LOCK PICKERS?

@Hackdwerg

https:// robert-philipps.com/tmp/bugbounty.pdf

Über mich

- Robert Philipps
- Software Engineer
- 

- Trust & Safety Team
- On-Hands Engineering

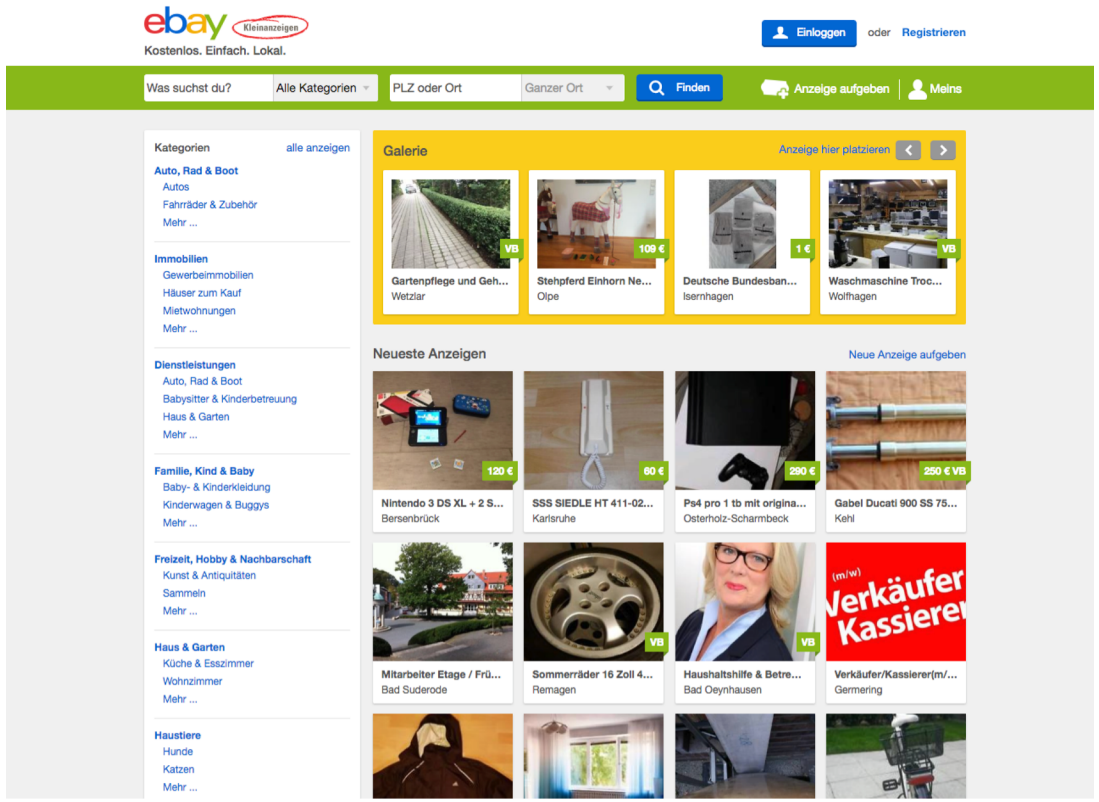
eBay Kleinzeigen

<u>Stats:</u>

- 30kk Anzeigen
- 52% 🇩🇪
- 40k requests /s

<u>Tech:</u>

- Docker, OpenStack, Kubernetes
- CI, CD



Konzernstruktur

Struktur des Vortrags

- Definition
- Notwendigkeitsanalyse
- Bestandteile
- Einbau in den Softwareentwicklungsprozess

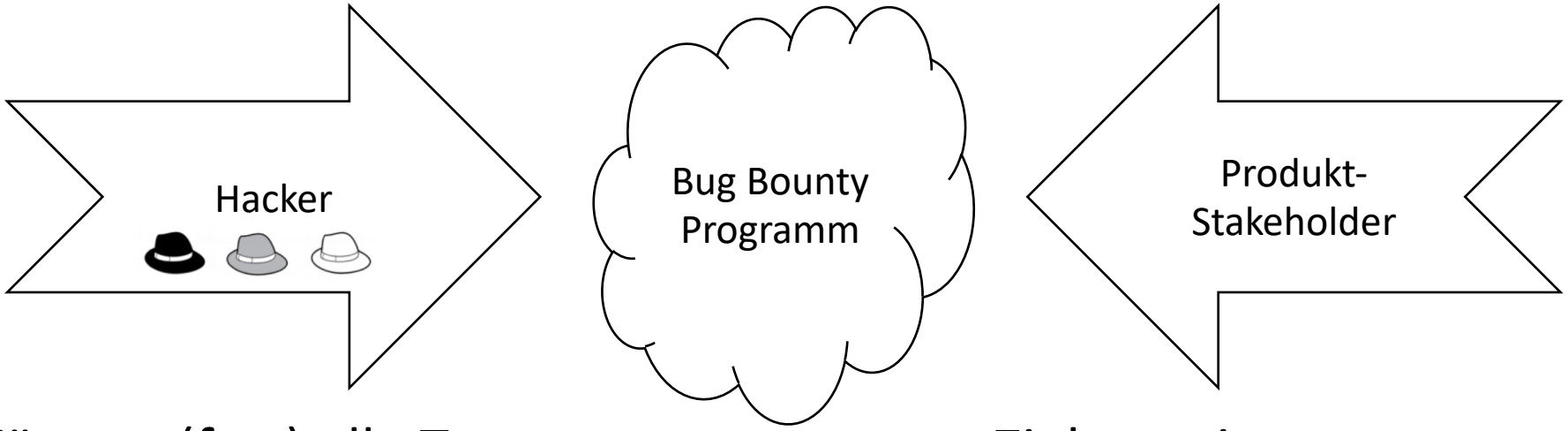
Bug-Bounty-Programm?

Bug-Bounty-Programm

Sicherheit Belohnung Organisierte Prozesse & klare Kommuikation

(Coordinated Vulnerability Disclosure)

Motivation



- Können (fast) alle Typen bedient werden
  - White-Hat
  - Black-Hat
- Sonst großes Risiko
- Wer hackt? Demografie

- Ziel: weniger Sicherheitslücken
- Potentielle Schwächung von SWE-Prozess
- Kostenersparnisse
- Marketing
- Employer-Branding

Rückblende

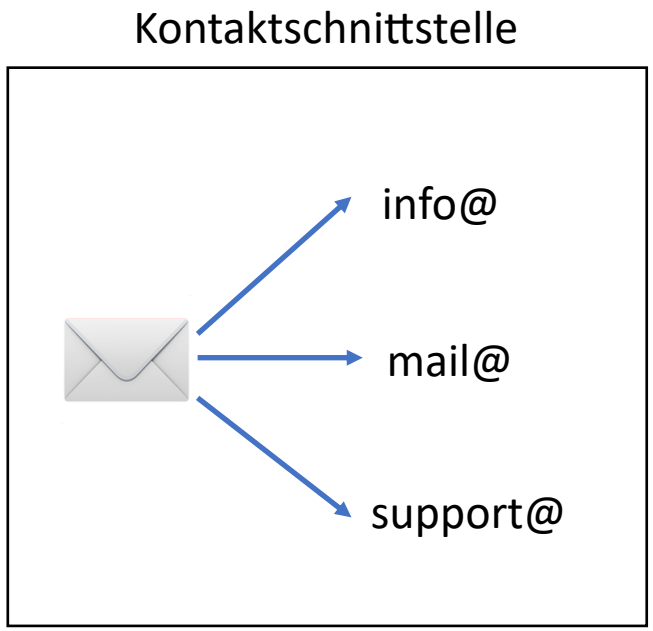
OpenBugBounty.org Portal
29. Mai 2016 um 23:03:06 MESZ
An: <info@ebay-kleinanzeigen.de>
Antwort an: <openbugbounty@xssposed.org>
ebay-kleinanzeigen.de Security Vulnerability Notification | Important

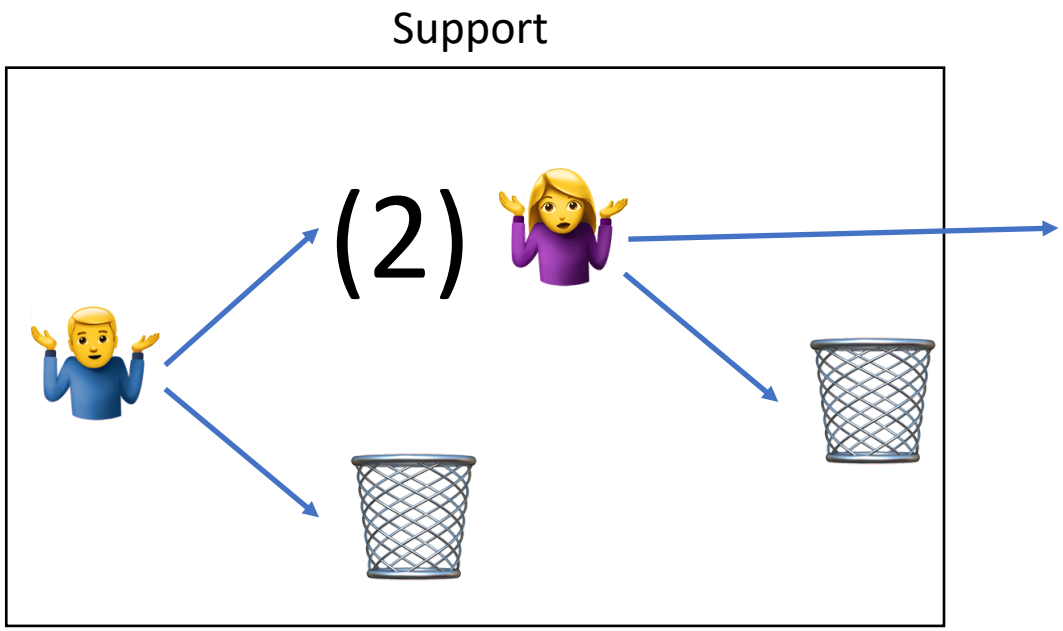
Dear Sirs,

A security researcher dim0k have reported a security vulnerability on your website:
https://www.openbugbounty.org/incidents/157014/

Es handelte sich hierbei um eine nicht persistente XSS-Injection, über die eBay Kleinanzeigen am 30.05.2016 gegen 18h informiert wurde. Knapp zwei Tage später, am 01.06.2016 um 10:41h, wurde der Fix zum Beheben der Vulnerability ins Produktivsystem eingespielt. Die Logs wiesen keine Ausnutzung dieser Lücke aus. Es kann also davon ausgegangen werden, dass keine Nutzer betroffen waren.

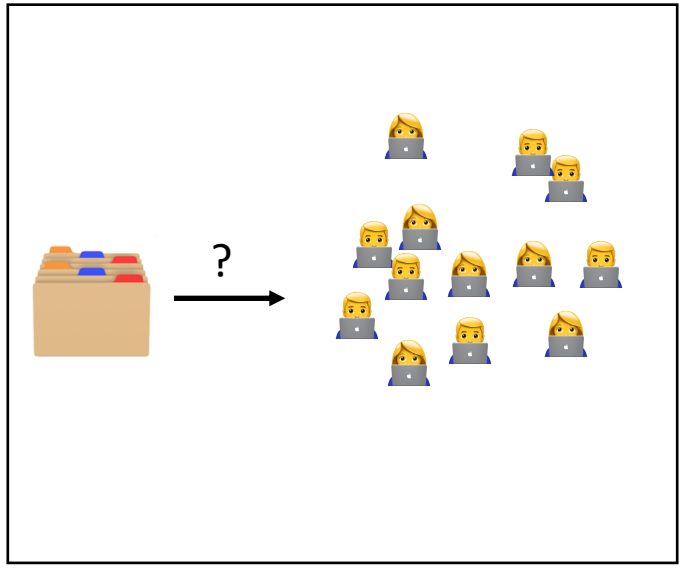
Rückblick



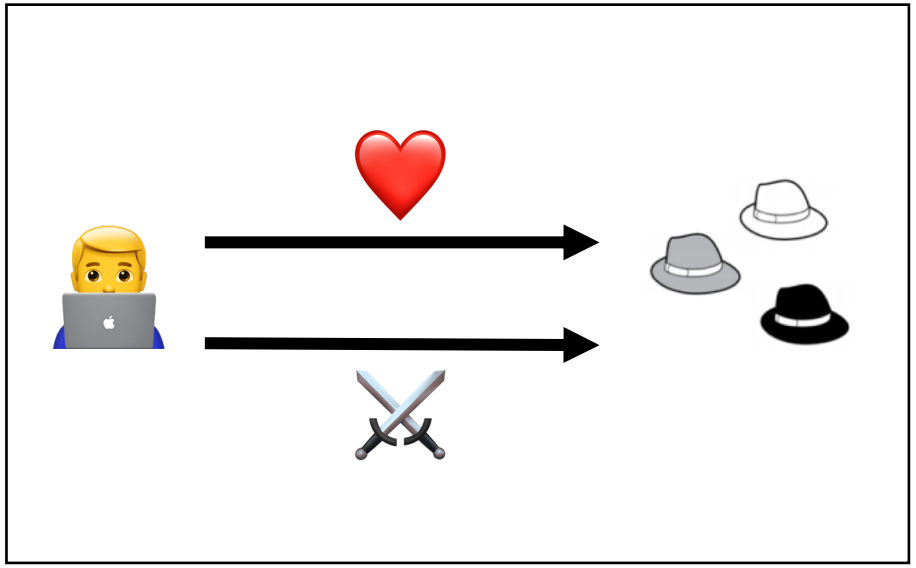


Rückblick 2

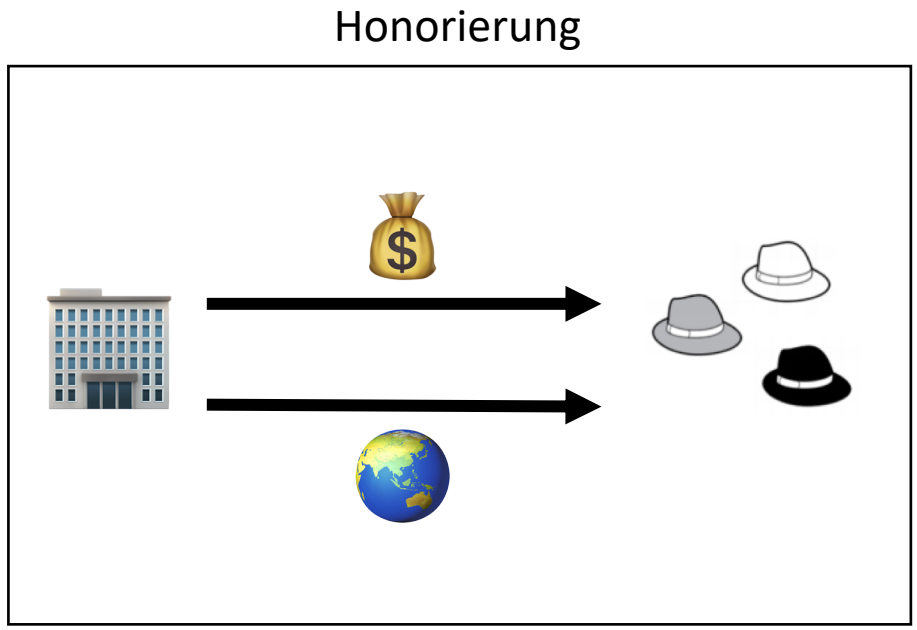
Zuständiger Entwickler & Prozess



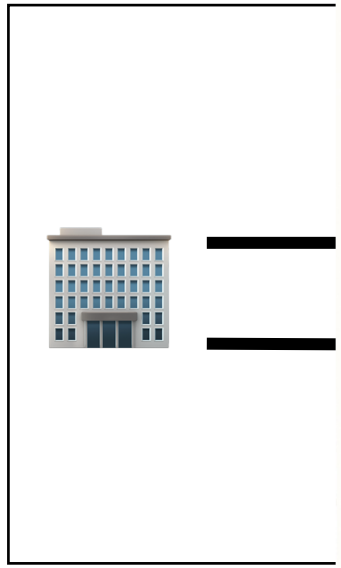
Kommunikation mit Hacker



Rückblick 3



Rückblick 3



ebay

Robert Philipps
rphilipps@ebay.com

eBay International AG
Albert-Einstein-Ring 2-6
14532 Berlin

Berlin, 30/06/2016

Dear Sir or Madam,

we have sent the following person:

Dmitry [redacted]

as a thank you for his help in fixing a security issue on ebay-kleinanzeigen.de the following goods:

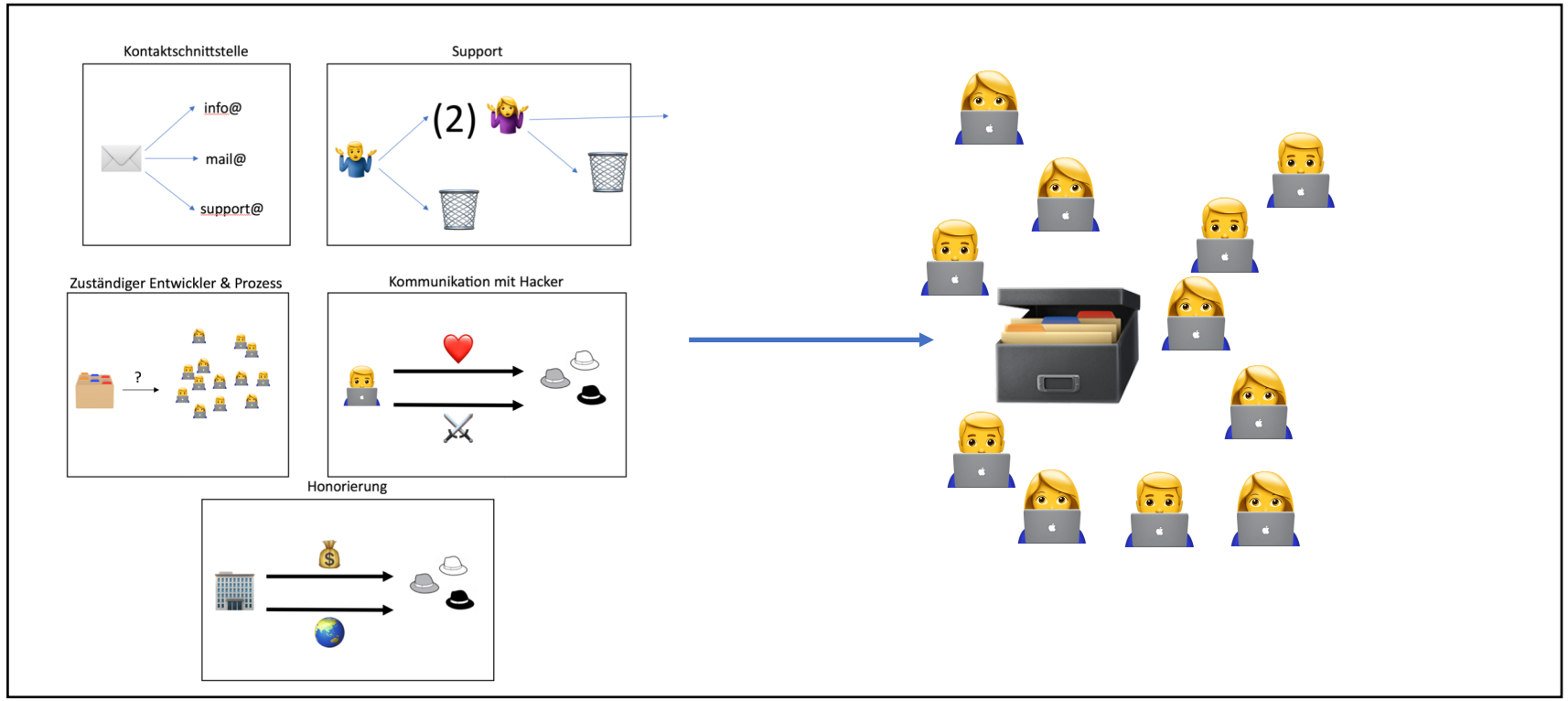
NAME	VALUE	COUNT	SUM
CUP	USD 2.00	2	USD 4.00
KEYCHAIN	USD 0.50	2	USD 1.00
PEN	USD 0.25	4	USD 1.00
BOOK	USD 3.00	2	USD 6.00
PORTABLE BATTERY	USD 5.00	1	USD 5.00
TABLE KICKER BALL	USD 0.50	2	USD 1.00
BICYCLE PROTECTION	USD 0.10	2	USD 0.20
T-SHIRT	USD 3.00	1	USD 3.00
TOTAL			USD 21.20

Best,

Robert Philipps

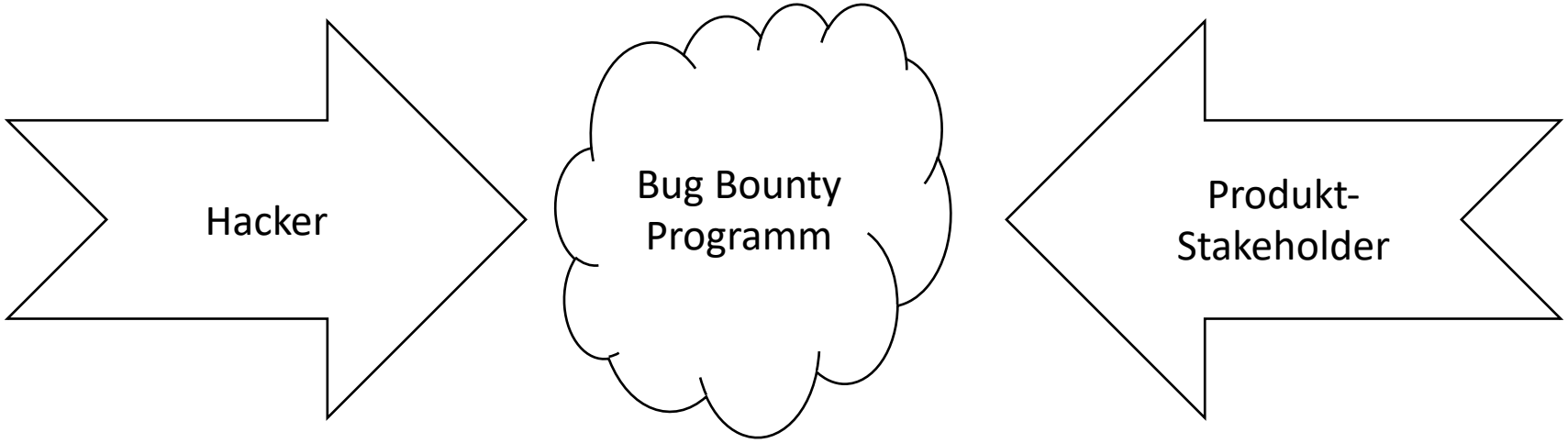
Rückblick 4

Prozess & Dokumentation



Zusammenfassung – Ohne BBP

- Sicherheitslücken werden gefunden
  - Keine Kontaktmöglichkeit
  - Kein geregelter Prozess
- Störung des Softwareentwicklungsprozesses
- Keine Möglichkeit für Entlohnungen



Bestandteile- einmalig

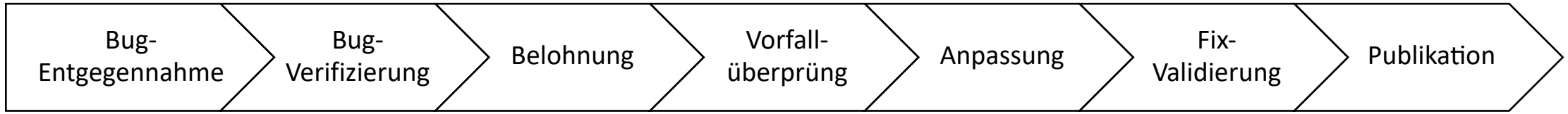
Kommunikation über Vorhandensein

- Auffindbarkeit
- Rahmenbedingungen
  - Scope
  - Payout

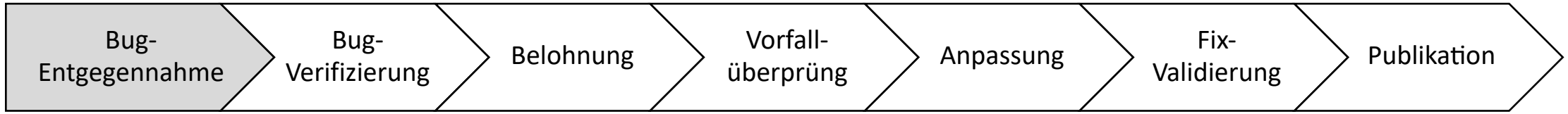
Schnittstelle für Kommunikation

- Bidirektional
- Schnelle Reaktion möglich machen
- Verschlüsselt

Bestandteile- wiederkehrend



Bestandteile- wiederkehrend



- Tatsächlich bezogen auf Sicherheit?
- Notwendige Angaben gemacht?

Google

Report a security vulnerability

If you have found a security bug in a Google product and want to report it to us, you've come to the right place. Please fill out the following form and we'll be in touch shortly. If this is a valid vulnerability report, it might also be eligible for a reward as part of our Vulnerability Reward Program. Thanks!

Problem description

Please describe the issue you wish to report.

- ○ I'm experiencing a security problem with my Google account.
- ○ I want to remove content on Google Search, Youtube, Blogger, or another service.
- ○ I have a privacy doubt or a privacy-related question about Google products and services.
- ◉ I found a security bug in Google "forgot password" feature.
- ○ I want to report a technical security bug in a Google product (SQLi, XSS, etc.).
- ○ I want to report a scam, malware, or other problems not listed above.

What is the security issue in forgot password feature you wish to report?

- ◉ I successfully hijacked a Google account, pretending to be an attacker.
- ○ Someone hijacked my Google account.

What is the type of issue that you exploited?

- ○ The questions Google asked me in the process are too easy to guess.
- ○ I was asked too few questions before getting access to an account.
- ◉ I was let in to the account, while my answers to questions were incorrect.
- ○ Restoring the access to an account was otherwise easy.

It turns out people make mistakes, even when recovering their own accounts. Sometimes, when multiple other signals in the recovery process tell us you're the actual owner, we might turn a blind eye to an invalid response. It isn't the case for the attacker though.

We use multiple signals when deciding whether to allow an access to an account. To keep your account secure, we cannot speak about many of them, but rest assured the real attacker would experience the the process very differently than the original account owner.

Was the account previously used on the same browser/computer/IP address that was used to attack?

- ◉ No
- ○ Yes

This initially looks like a bug. However, most of the security reports about the 'forget password' feature we receive turn out to be invalid, so please read about the known issues with account recovery first.

For this kind of security report it's important we got the details right and can reproduce the issue. If the bug you've found works consistently time after time, please report the vulnerability and we'll be in touch shortly. Thanks a lot!

Google

Report a security vulnerability

If you have found a security bug in a Google product and want to report it to us, you've come to the right place. P
shortly. If this is a valid vulnerability report, it might also be eligible for a reward as part of our Vulnerability Rewar

Problem description

Please describe the issue you wish to report.

- ○ I'm experiencing a security problem with my Google account.
- ○ I want to remove content on Google Search, Youtube, Blogger, or another service.
- ○ I have a privacy doubt or a privacy-related question about Google products and services.
- ◉ I found a security bug in Google "forgot password" feature.
- ○ I want to report a technical security bug in a Google product (SQLi, XSS, etc.).
- ○ I want to report a scam, malware, or other problems not listed above.

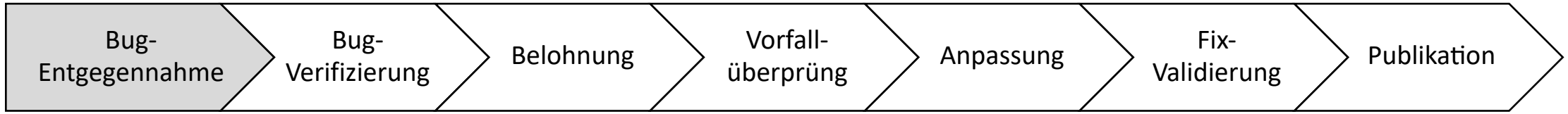
What is the security issue in forgot password feature you wish to report?

- ○ I successfully hijacked a Google account, pretending to be an attacker.
- ◉ Someone hijacked my Google account.

We're sorry to hear that. To recover access to your account, please continue here and select the 'My account has

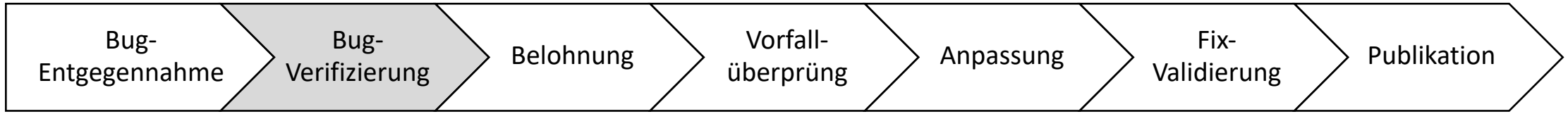
Google · About Google · Privacy & Terms

Bestandteile- wiederkehrend



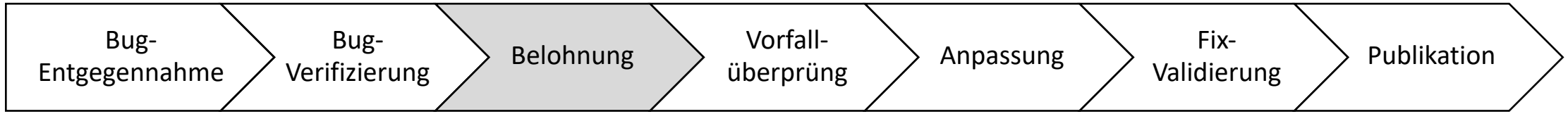
- Tatsächlich bezogen auf Sicherheit?
- Notwendige Angaben gemacht?

Bestandteile - wiederkehrend



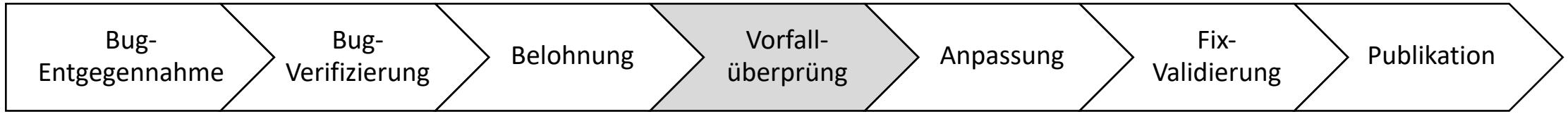
- Bug vorhanden?
- In relevantem System?
- Duplikat?

Bestandteile - wiederkehrend



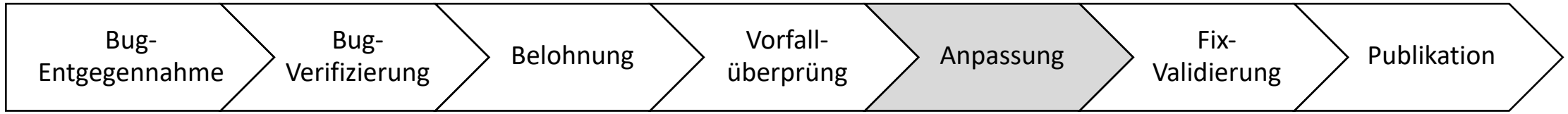
- Spätestens am Ende
- Belohnung?
  - Komplexer Prozess
- Merchandise?

Bestandteile - wiederkehrend



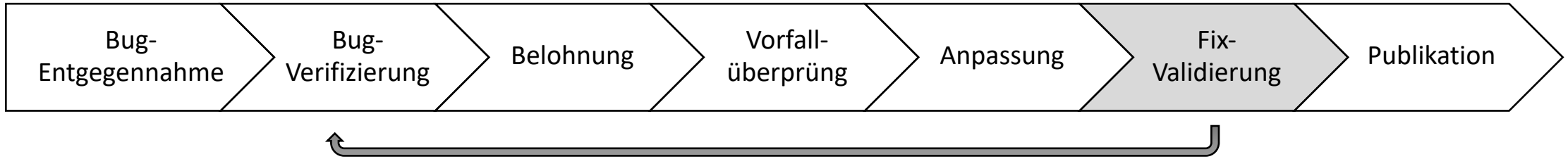
- Wurde Bug ausgenutzt?
- In welchem Ausmaß?

Bestandteile - wiederkehrend



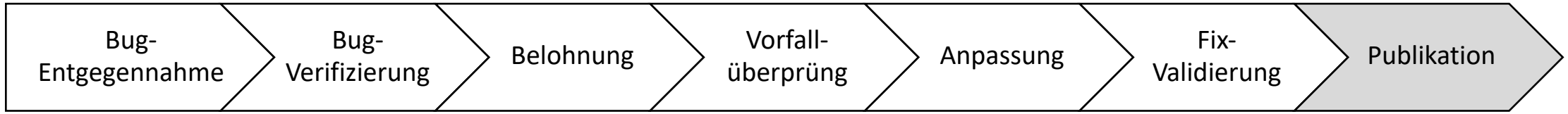
- Integration in regulären Softwareentwicklungsprozess
- Sprint / Aufgabe / Kaskade
- Möglichkeit weitere Fehler zu entdecken

Bestandteile - wiederkehrend



- Bug behoben?

Bestandteile - wiederkehrend



- User aus Gefahr?
- PR-Effekt

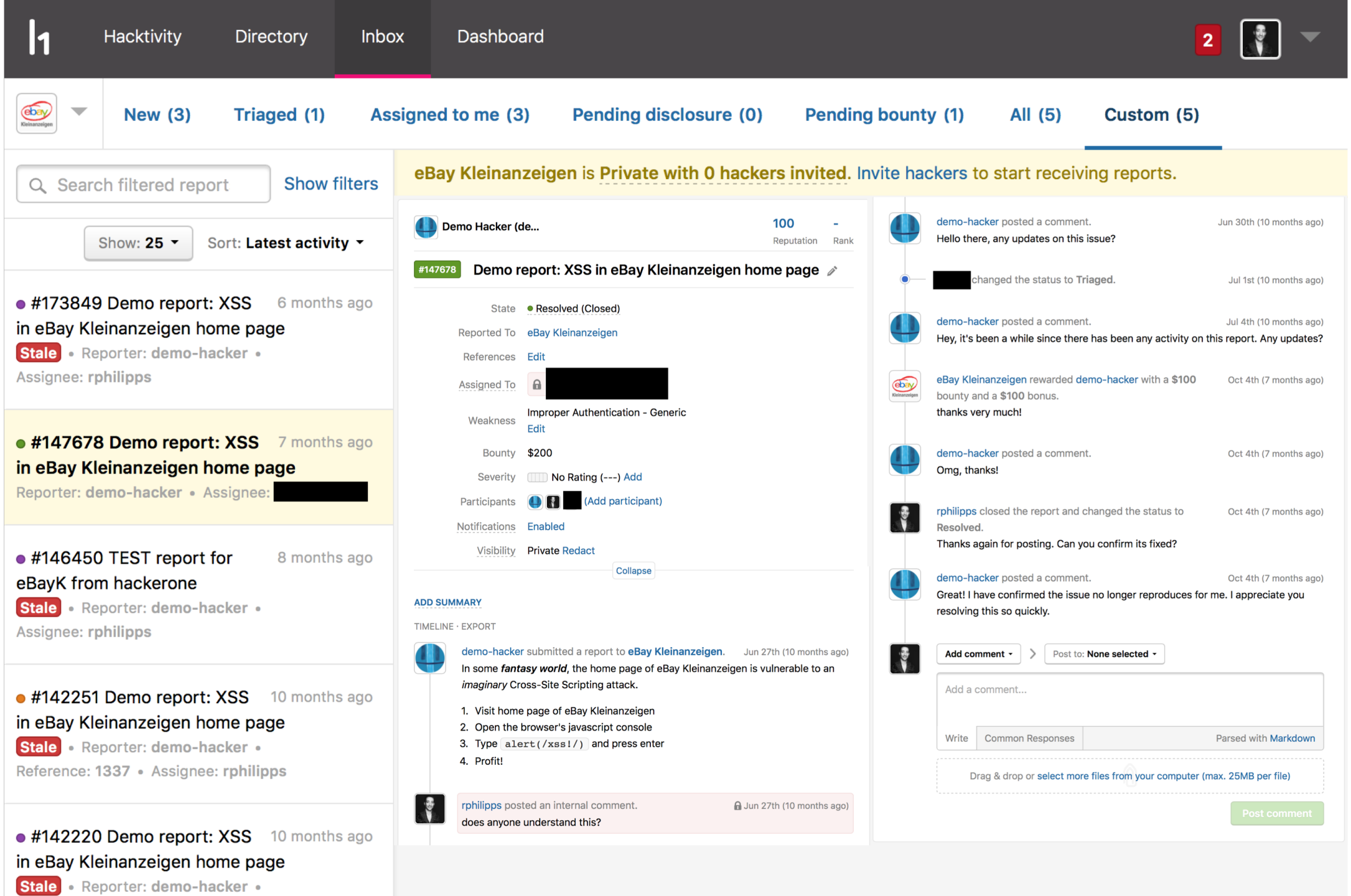
Selber machen vs. Extern

- Markt wächst kontinuierlich
- Große Hilfe
- Grundsätzliches Problem

hackerone

zerocopter

bugcrowd


Hacktivity
Directory
Inbox
Dashboard
2
New (3)
Triaged (1)
Assigned to me (3)
Pending disclosure (0)
Pending bounty (1)
All (5)
Custom (5)
Search filtered report
Show filters
Show: 25
Sort: Latest activity
#173849 Demo report: XSS in eBay Kleinanzeigen home page
6 months ago
Stale • Reporter: demo-hacker •
Assignee: rphilipps
#147678 Demo report: XSS in eBay Kleinanzeigen home page
7 months ago
Reporter: demo-hacker • Assignee: [redacted]
#146450 TEST report for eBayK from hackerone
8 months ago
Stale • Reporter: demo-hacker •
Assignee: rphilipps
#142251 Demo report: XSS in eBay Kleinanzeigen home page
10 months ago
Stale • Reporter: demo-hacker •
Reference: 1337 • Assignee: rphilipps
#142220 Demo report: XSS in eBay Kleinanzeigen home page
10 months ago
Stale • Reporter: demo-hacker •
eBay Kleinanzeigen is Private with 0 hackers invited. Invite hackers to start receiving reports.
Demo Hacker (de...
100
Reputation
-
Rank
#147678
Demo report: XSS in eBay Kleinanzeigen home page
State
Resolved (Closed)
Reported To
eBay Kleinanzeigen
References
Edit
Assigned To
[redacted]
Weakness
Improper Authentication - Generic
Edit
Bounty
$200
Severity
No Rating (---) Add
Participants
(Add participant)
Notifications
Enabled
Visibility
Private Redact
Collapse
ADD SUMMARY
TIMELINE · EXPORT
demo-hacker submitted a report to eBay Kleinanzeigen.
Jun 27th (10 months ago)
In some fantasy world, the home page of eBay Kleinanzeigen is vulnerable to an imaginary Cross-Site Scripting attack.
1. Visit home page of eBay Kleinanzeigen
2. Open the browser's javascript console
3. Type alert(/xss!/) and press enter
4. Profit!
rphilipps posted an internal comment.
Jun 27th (10 months ago)
does anyone understand this?
demo-hacker posted a comment.
Jun 30th (10 months ago)
Hello there, any updates on this issue?
[redacted] changed the status to Triaged.
Jul 1st (10 months ago)
demo-hacker posted a comment.
Jul 4th (10 months ago)
Hey, it's been a while since there has been any activity on this report. Any updates?
eBay Kleinanzeigen rewarded demo-hacker with a $100 bounty and a $100 bonus.
Oct 4th (7 months ago)
thanks very much!
demo-hacker posted a comment.
Oct 4th (7 months ago)
Omg, thanks!
rphilipps closed the report and changed the status to Resolved.
Oct 4th (7 months ago)
Thanks again for posting. Can you confirm its fixed?
demo-hacker posted a comment.
Oct 4th (7 months ago)
Great! I have confirmed the issue no longer reproduces for me. I appreciate you resolving this so quickly.
Add comment
Post to: None selected
Add a comment...
Write
Common Responses
Parsed with Markdown
Drag & drop or select more files from your computer (max. 25MB per file)
Post comment

Wer kann was? Personengruppen

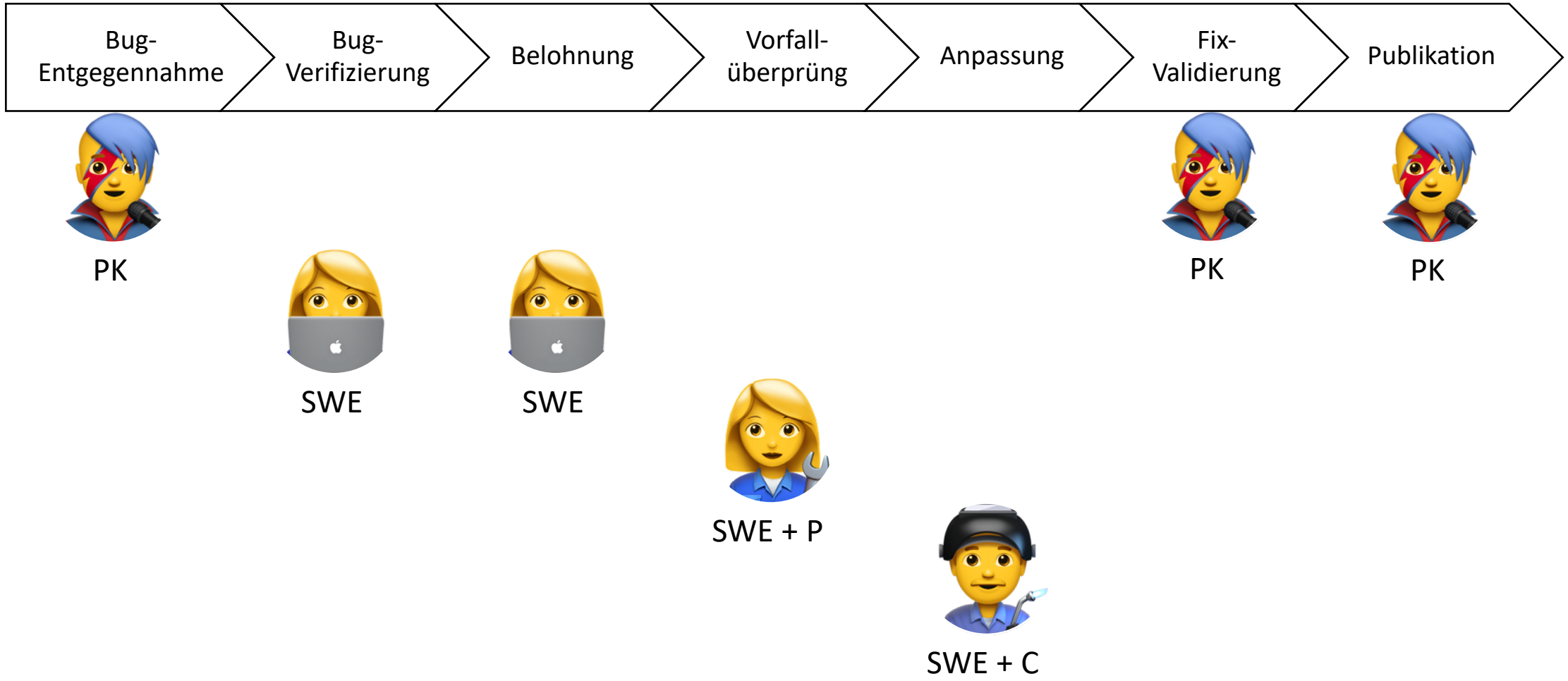
Personen mit Kommunikationskompetenz

Softwareentwickler

SWE mit Zugang zu PROD

SWE mit Zugang zum Code

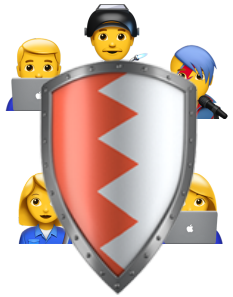
Kompetenzmatrix



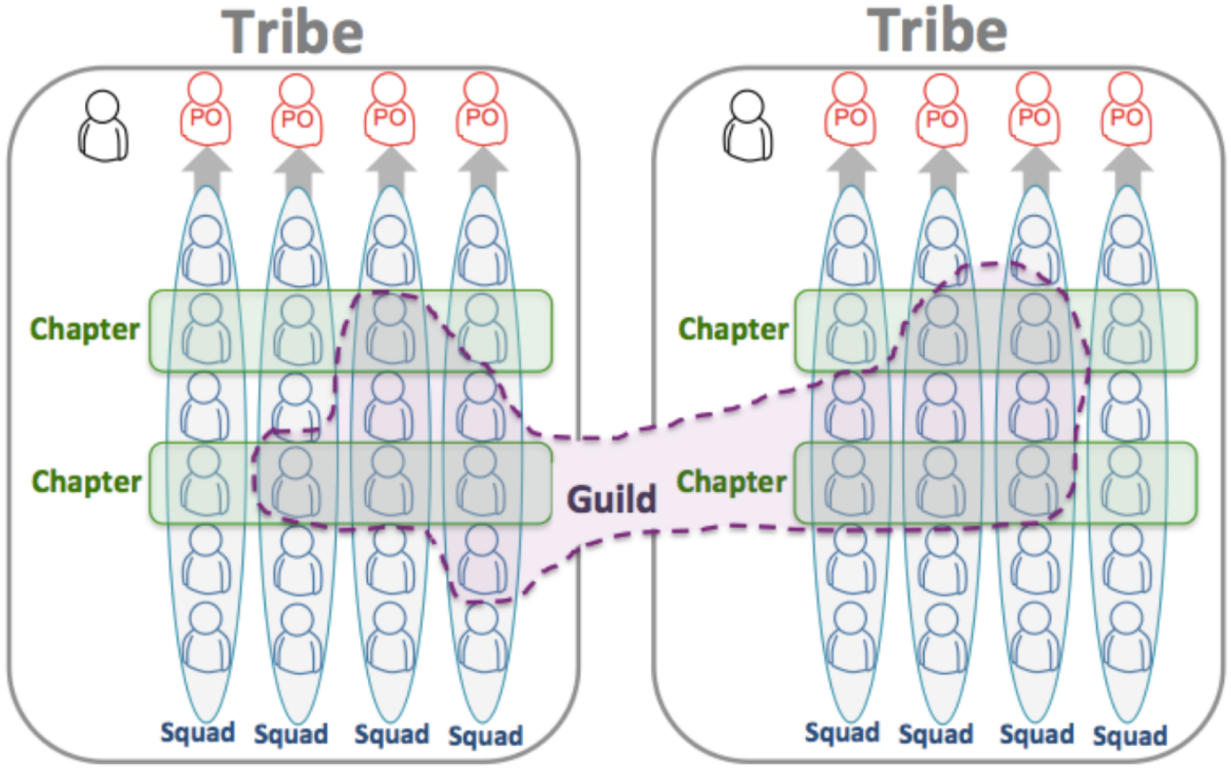
eBay Kleinanzeigen

Konzernstruktur
- InfoSec

Guild-Konzept (Spotify)



Henrik Kniberg & Anders Ivarsson
Oct 2012



eBay Kleinanzeigen

We are Germanys biggest classifieds proposition and part of the eBay Classifieds Group and eBay Inc.

www.ebay-kleinanzeigen.de • @ebay_ka • Launched on July 2nd, 2018

Rewards

P1 (8 to 10)	P2 (7 to <8)	P3 (5 to <7)	P4 (1 to <5)
$1,000	$400	$250	$100

We reward vulnerabilities based on the Common Vulnerability Scoring System (CVSS v3). You can calculate the score of a possible vulnerability with this easy calculator.

eBay Kleinanzeigen will determine in its discretion whether a reward should be granted and the amount of the reward.

Policy

Preamble

eBay Kleinanzeigen (eBayK) is excited to be working with the hacker community in our inaugural bug bounty program. As such, we are starting small, and once we prove the value to our internal team and management, we will be expanding the program to include additional scope and increase our bounty amounts. We thank you for helping us as we ease into running a bug bounty program.

Responsible Disclosure Program

At eBay Kleinanzeigen we take user safety and the security of our services very serious. We recognize the important role that security researchers and our community play in keeping our services and users safe. We have adopted the responsible disclosure program described here to encourage everyone reporting security vulnerabilities. To recognize your efforts we offer bounty for reporting certain qualifying security vulnerabilities. Please review the following rules before you report a vulnerability. By participating in this program, you agree to be bound to these rules.

In Scope

- Please use the latest mobile app versions.
- For old browsers or browser versions eBay Kleinanzeigen might not accept and thus not fix the vulnerability based on its discretion.

Response Efficiency

6 hrs
Average time to first response

9 days
Average time to bounty

about 1 month
Average time to resolution

94% of reports
Meet response standards

Based on last 90 days

Program Statistics

$11,700
Total bounties paid

$100 - $150
Average bounty range

$300 - $2,000
Top bounty range

47
Reports resolved

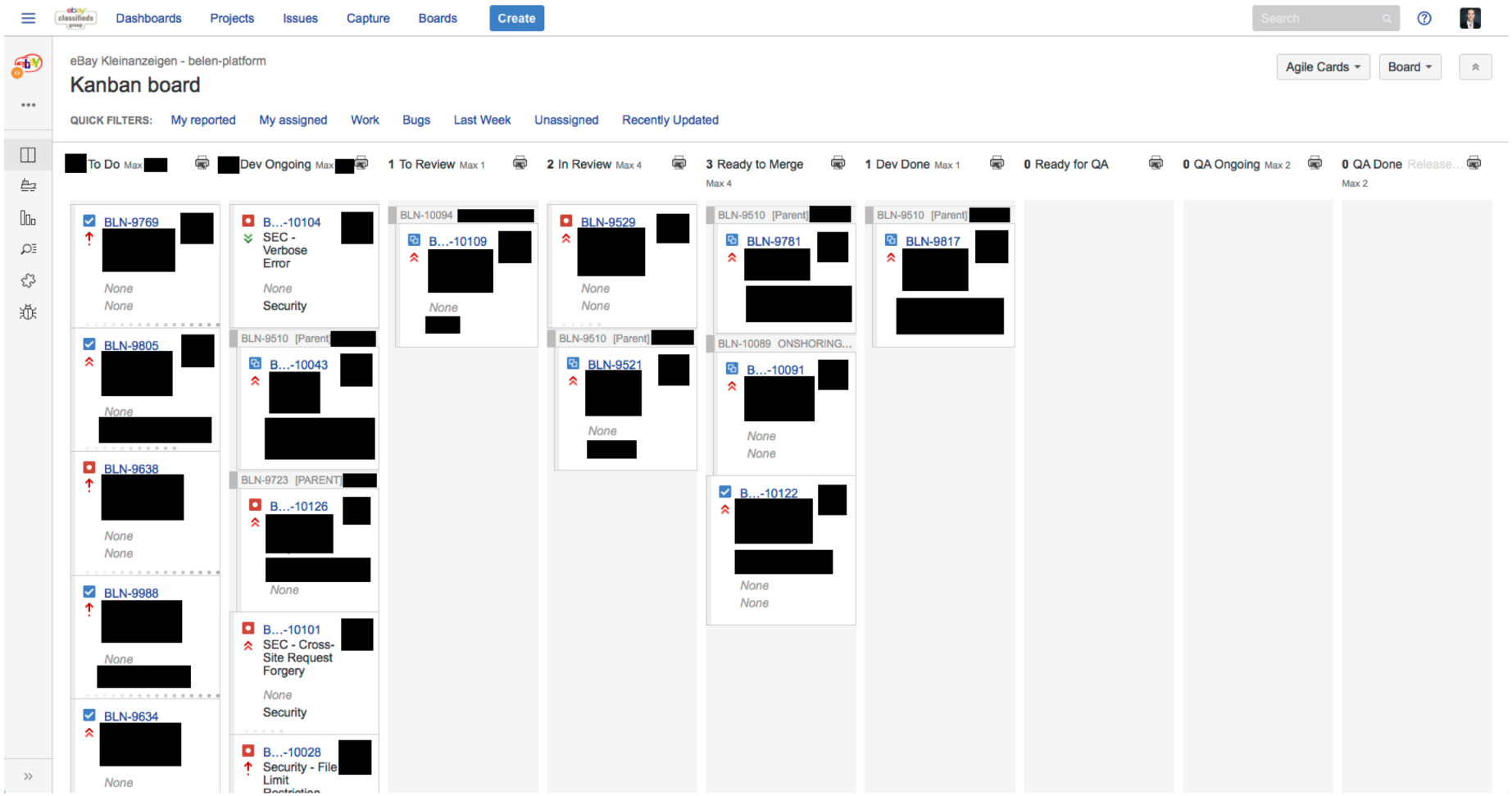
44
Hackers thanked

Top hackers

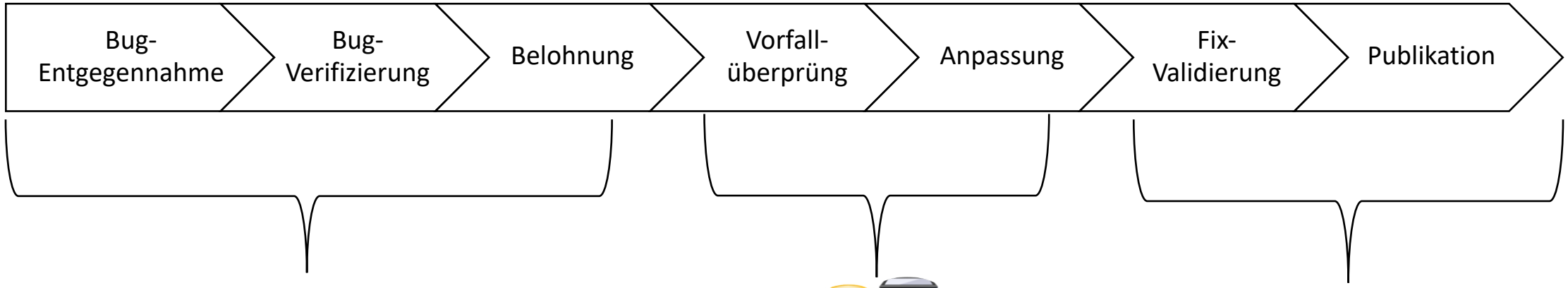

gerben_javado
Reputation:239

cyber-guard
Reputation:141

Zero Security Bug Policy

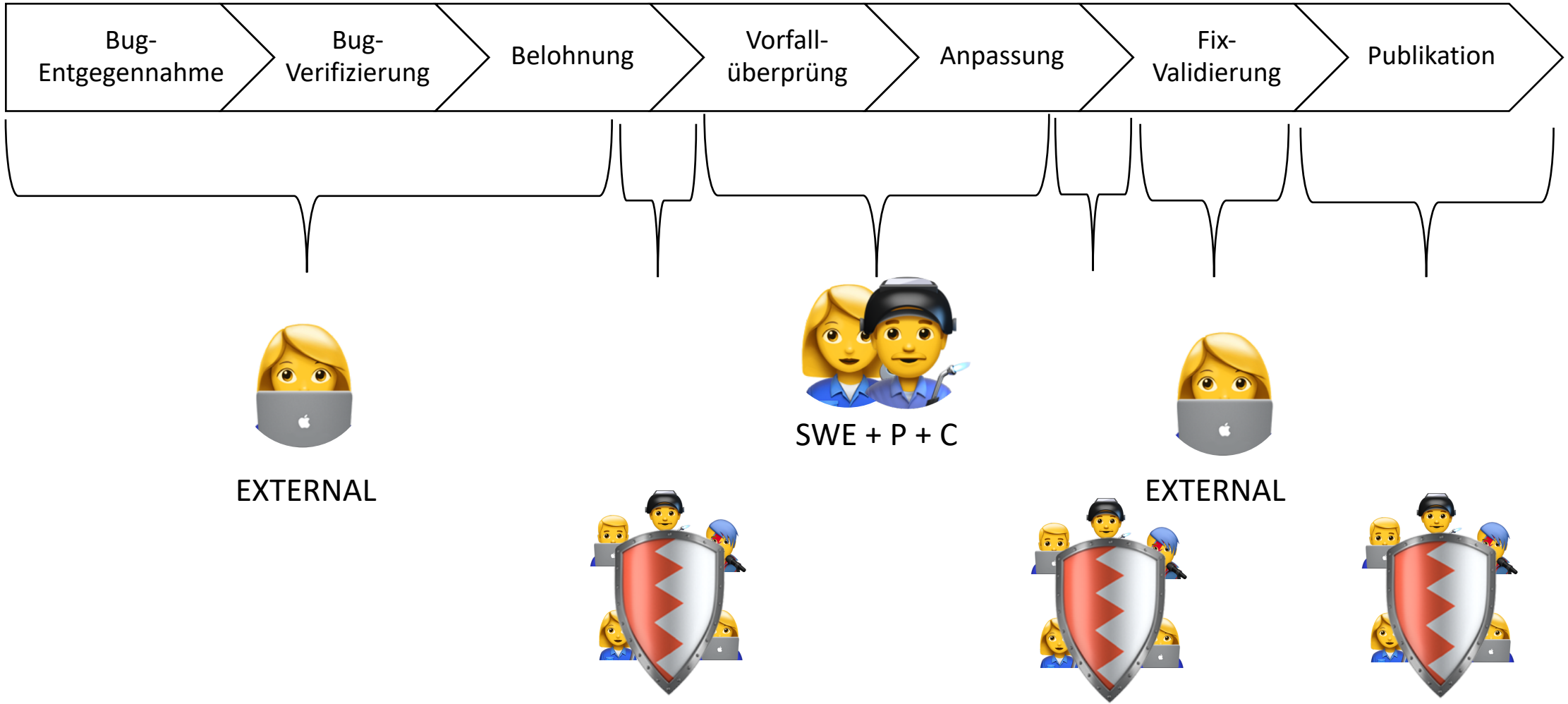


Kompetenzmatrix eBayK

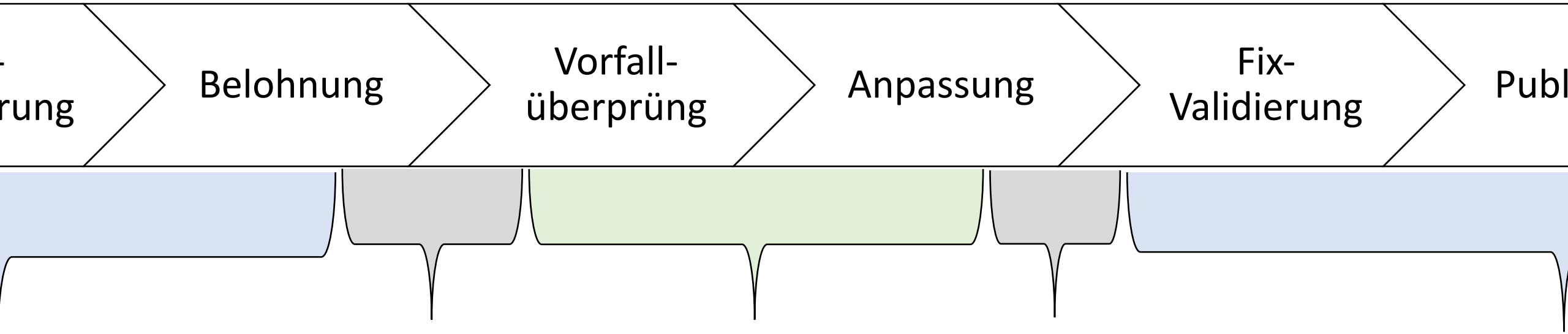


SWE + P + C

Kompetenzmatrix eBayK

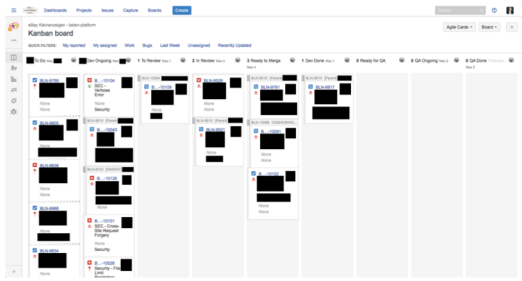


Kompetenzmatrix eBayK



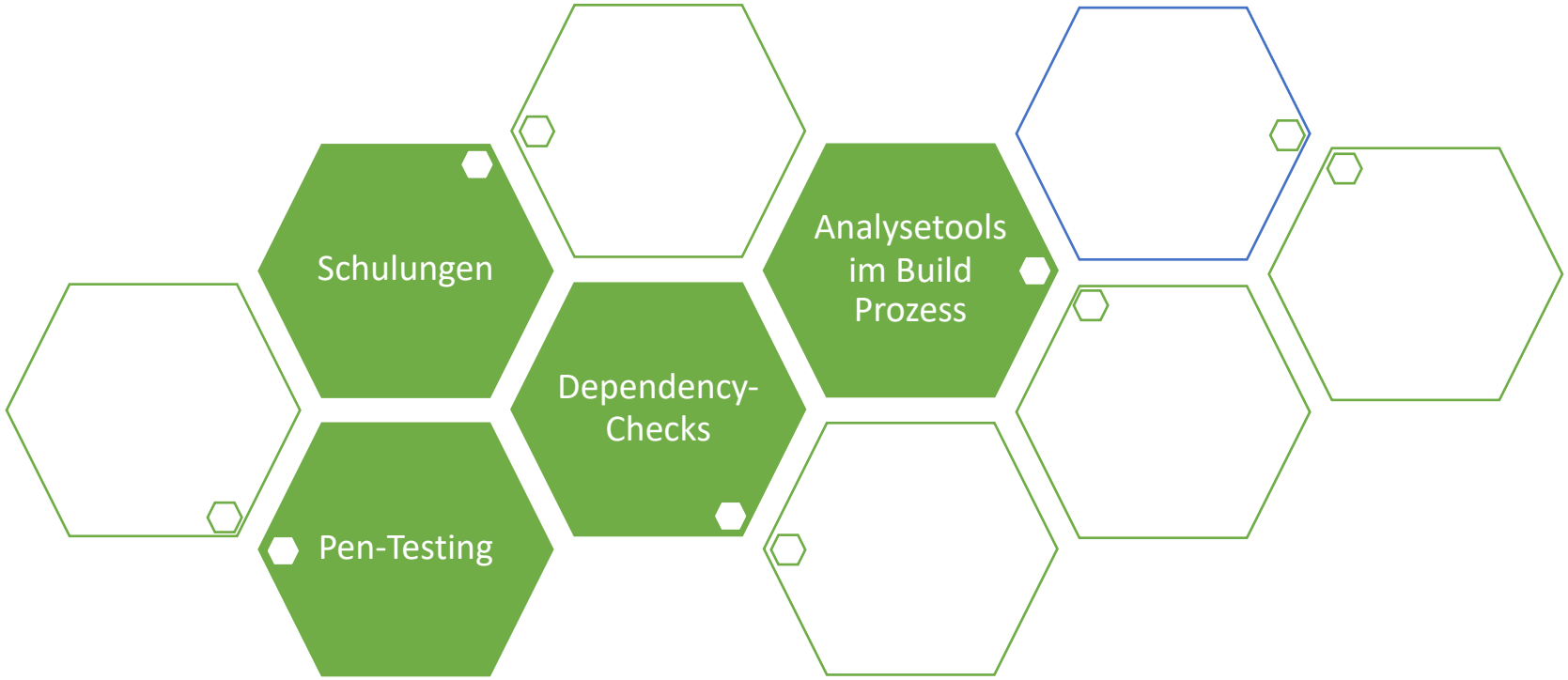
- Überprüfung
  - CVSS
  - Bounty

- Konfliktklärung
- Integration in int. System

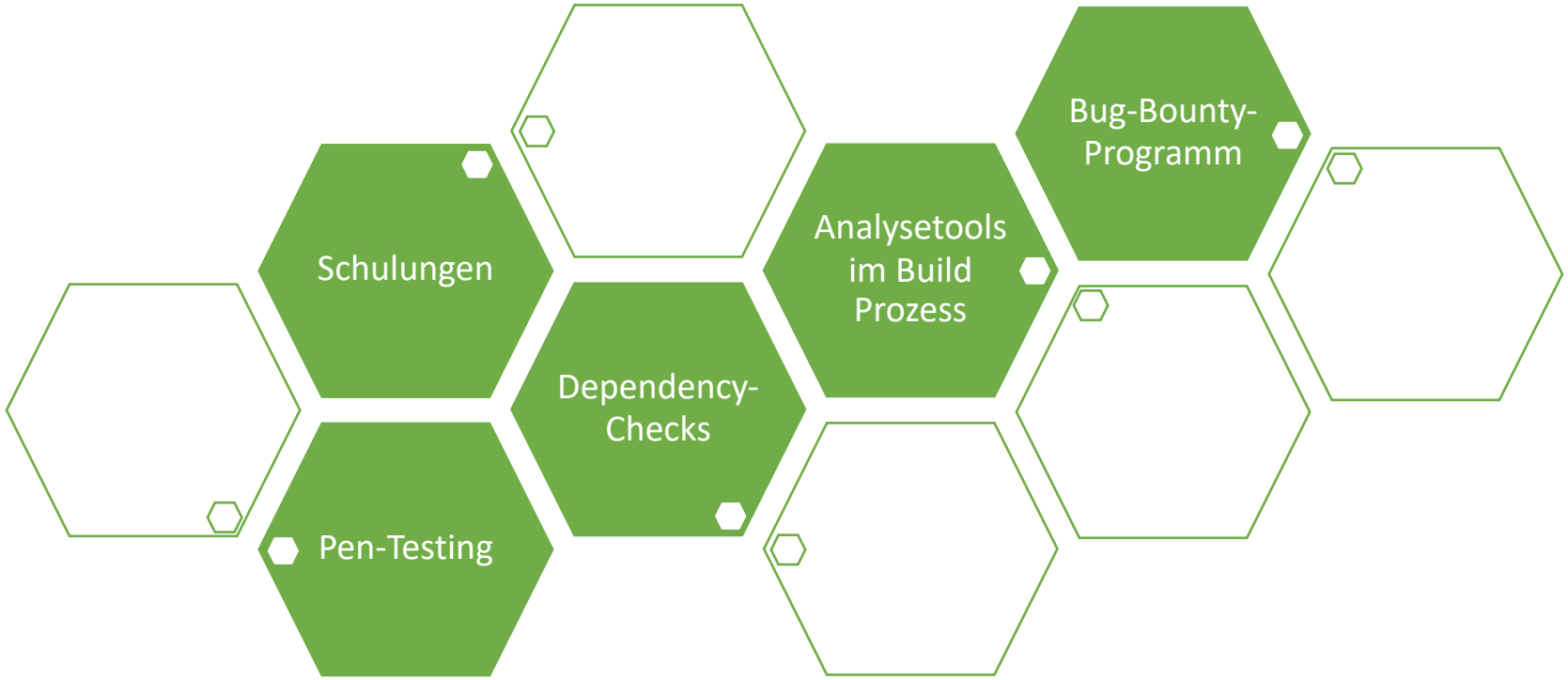


- Benachrichtigung das (vmtl.) gefixt an externes System

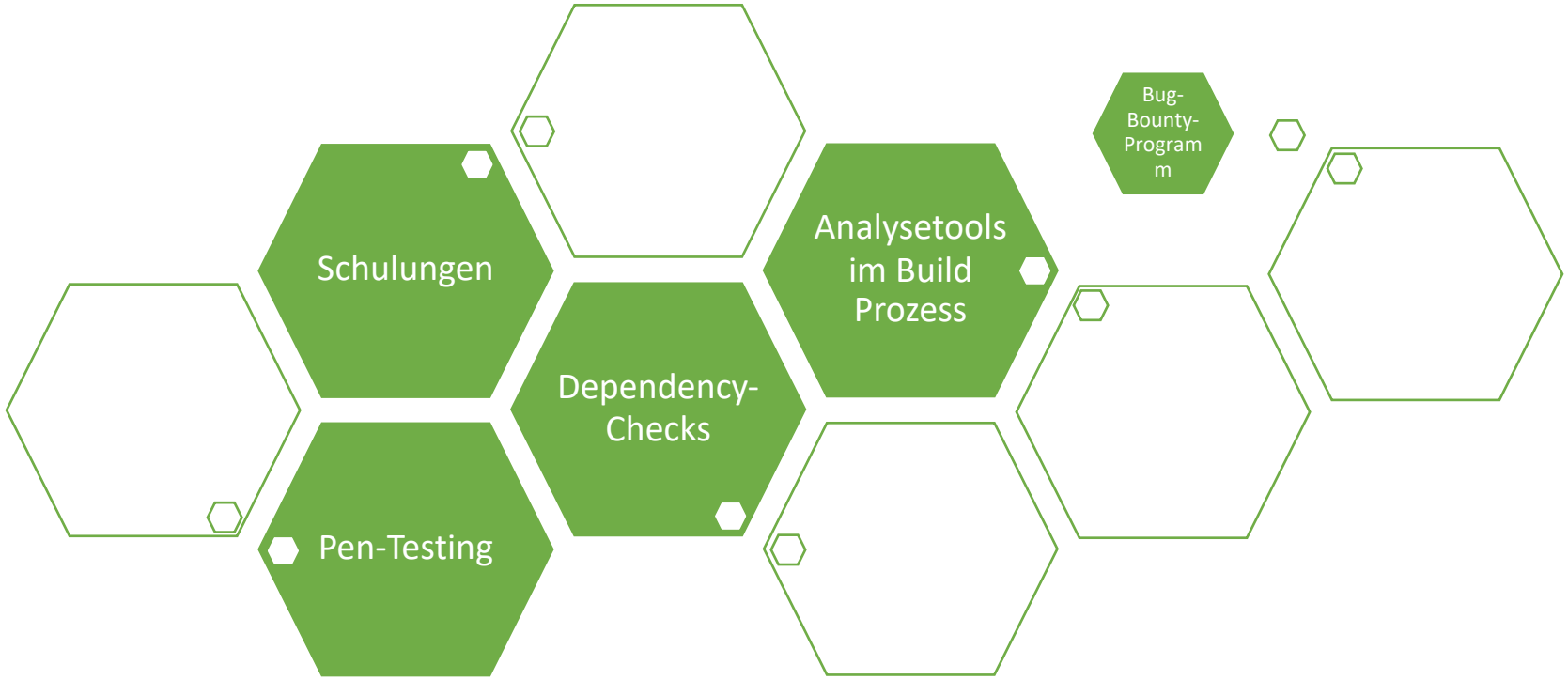
Rolle in Security Landschaft



Rolle in Security Landschaft



Rolle in Security Landschaft



Zusammenfassung & Fazit

- Personen finden Lücken
  - Können sie aber nicht melden
- Natürlicher Teil des Softwareentwicklungsprozesses
  - Bereicherung
  - Kein Unterschied zu Rest
- Kein Garant für Sicherheit
- Immer mehr Firmen bauen Bug-Bounty-Programme ein
  - Zukünftig vmtl. „Pflicht“

Getting Started

- Mit externer Hilfe „einfach“ integrierbar
- Bestandteile => Checkliste

hackerone
zerocopter
bugcrowd

Fragen, Kritik, Anregungen

https:// robert-philipps.com

/tmp/bugbounty.pdf

Robert Philipps

rphilipps@ebay.com
mail@robert-philipps.com

@rophilipps

The CERT® Guide to
Coordinated Vulnerability Disclosure

ISO 29147