Camilla Lundahl, Head of IT security

Motives, strategies and efforts to implement a bug bounty program

AVANZA

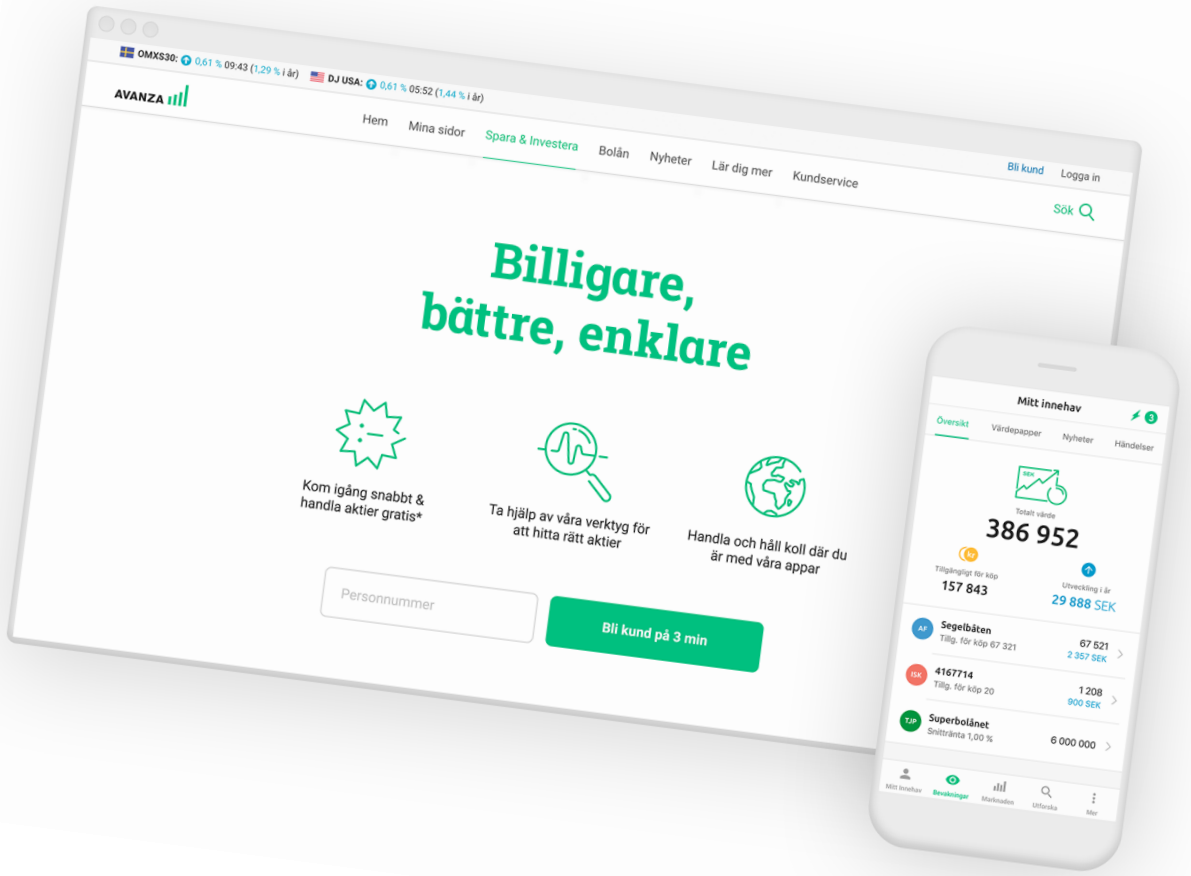
Sweden's most satisfied customers within savings for eight years in a row according to Swedish Quality Index

- **Sweden’s leading platform for savings and investments**
- **Uncompromising customer focus – more to you, less to the bank**
- **Vision to create a better future for millions of people**

AVANZA

Avanza

- Founded 1999
- 400 employees
- 130 in IT
  - 70% developers, agile teams
  - Release updates every 5th day
- More than 800 000 customers
- 3.8% market share in Sweden
- Listed on Nasdaq Stockholm
- 100% digital



AVANZA

Camilla Lundahl

REPORTER

"I've found a security vulnerability!

I want money, fame and/or the vulnerability fixed NOW!"

(In 90 days...!)

RECIEVER

...but how will the receiver respond most likely?

(if they don´t know anything about ethical hacking)

AVANZA

WHY
Responsible disclosure and Bug Bounty Program

Avanza

- Threat landscape
- Development speed
- Resolve issues faster
- Goodwill – proactive in IT sec

→ Hacker = Customer!

Ethical hacker

- Black | Grey | White hat hacker
- Build a better world
- Make a living | Make extra money
- Gamification (fun, family, fame)
- Education

AVANZA

HOW
Get management commitment

- CIO
- CRO
- CEO

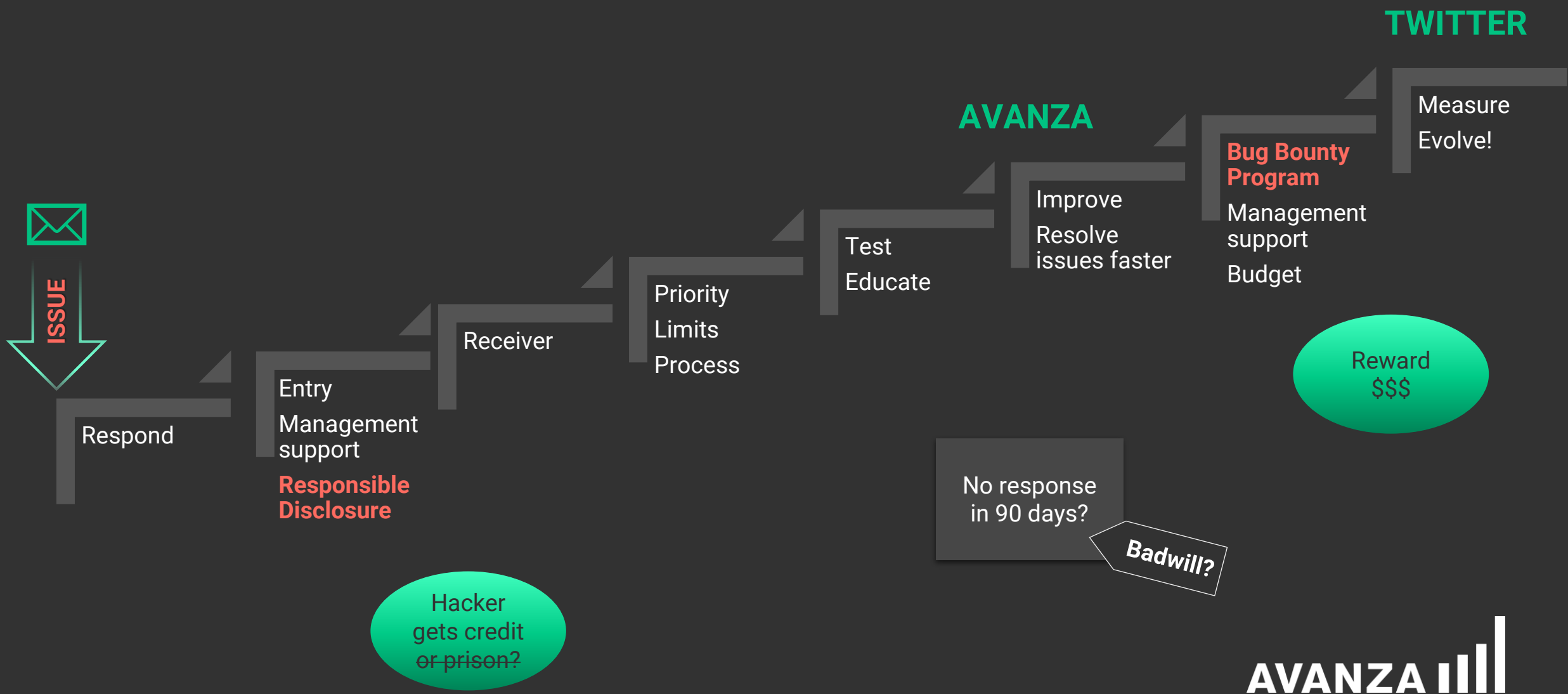
→ **Culture!**

RISK:
Collaborate with hackers?

Implementing a bug bounty program?

AVANZA

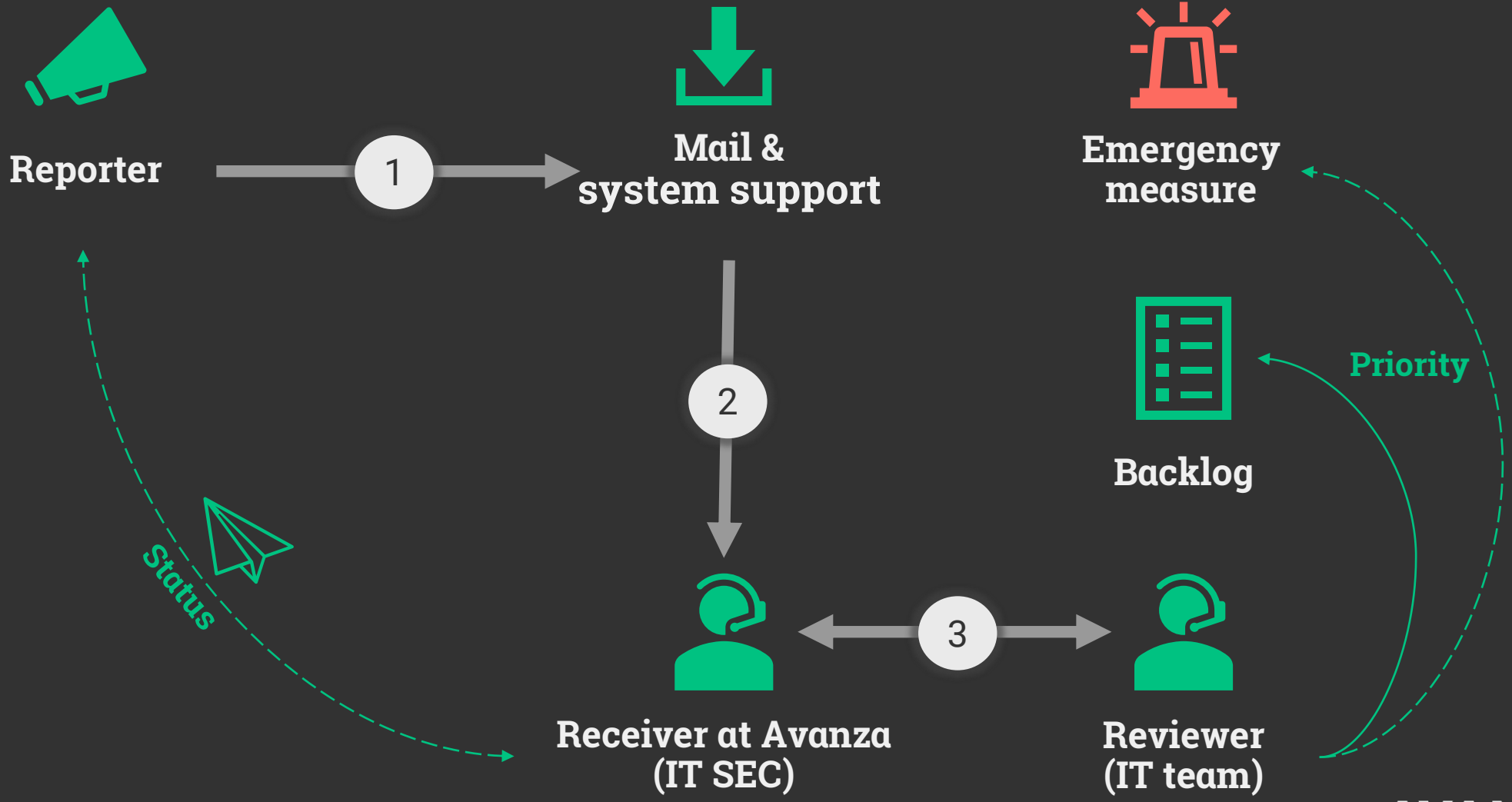
HOW TO BUILD A BUG BOUNTY PROGRAM



AVANZA

Camilla Lundahl

A SPECIFIC ISSUE



AVANZA

Camilla Lundahl

REPORTER-HACKER

The choice of contact path can be crucial for continued good cooperation

Customer impact

Your intention

Damage of company trust and reputation

AVANZA

Camilla Lundahl

RESPONSIBLE DISCLOSURE

On your website

How to report a security vulnerability

Rapportera en teknisk säkerhetsbrist

Vi på Avanza värdesätter våra kunders trygghet och säkerhet när de utför affärer genom våra tjänster. IT-säkerhetsarbetet är en kontinuerlig process som genomsyrar hela vår verksamhet. Som ett led i målsättningen att bli Sveriges säkraste bank vill vi därför gärna bli uppmärksamma på eventuella IT-säkerhetsbrister som ni som kunder stöter på.

Vilka brister kan rapporteras?

- Webbapplikationsbrister
- Brister i affärslogik
- Felkonfigurationer
- Möjliga infrastrukturbrister

Vi ser gärna att ni undviker att rapportera brister som inte har en direkt påverkan på IT-säkerheten, exempelvis möjliga feltolkningar eller stavningsfel i texter.

Hur skickar man in en rapport?

Rapporten skickas per email till securityreport@avanza.se, helst levereras denna krypterad med PGP. Vår publika nyckel finns att hämta här.

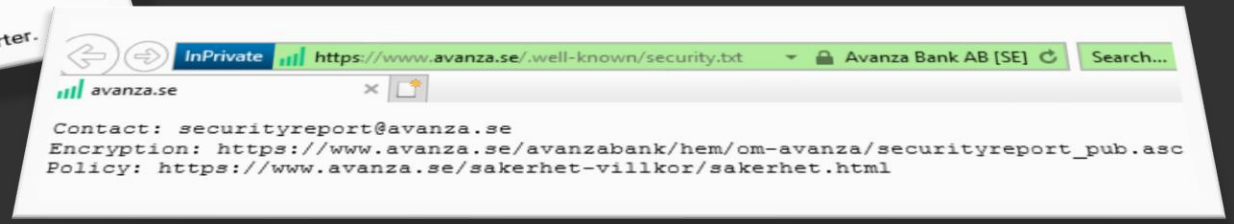
Vad bör rapporten innehålla?

- Övergripande beskrivning av bristen
- Steg-för-steg exempel hur bristen utnyttjas
- Eventuella skärmdumpar
- Kontaktuppgifter

Riktlinjer och regler

Följande regler och riktlinjer ser vi gärna att du följer om du upptäckt en brist:

- Utnyttja inte bristen för att komma åt information du inte har behörighet till.
- Radera inte data i system.
- Orsaka inte avbrott i tjänsten (Denial-of-Service).
- Offentliggör eller diskutera inte bristen med andra parter.



Security.txt

Find information about how to report a security vulnerability

COMPANY

Explain how you want information delivered

Your company provides straightforward guidelines for submitting security vulnerabilities to your organization.

AVANZA

Camilla Lundahl

NEXT STEP – LEARN MORE

Bug Bounty Programs

- Twitter, Airbnb
- Facebook

Platforms

- HackerOne
- Bugcrowd

AVANZA

Camilla Lundahl, Head of IT security

TOGETHER
we create better and safer services, and contribute to a more robust society

AVANZA