

The SURF logo is a white speech bubble with the word "SURF" in black capital letters. The background of the slide is a photograph of a man with a beard and red hair, wearing a green hoodie, sitting at a desk and looking at a laptop. The laptop has several stickers on it, including "HP", "NGINX", and "Compass". The man is surrounded by other people in a workshop or conference setting, with colorful vertical light bars in the background.

SURF

Making Yourself Vulnerable to Become Less Vulnerable

Joost Gadellaa

TNC 2025, June 11 Lightning Talks: First Strike

| The Problem

We need to continuously manage our attack surface

- Vulnerability scanning → Limited
- Pentesting → Expensive



| Our Solution

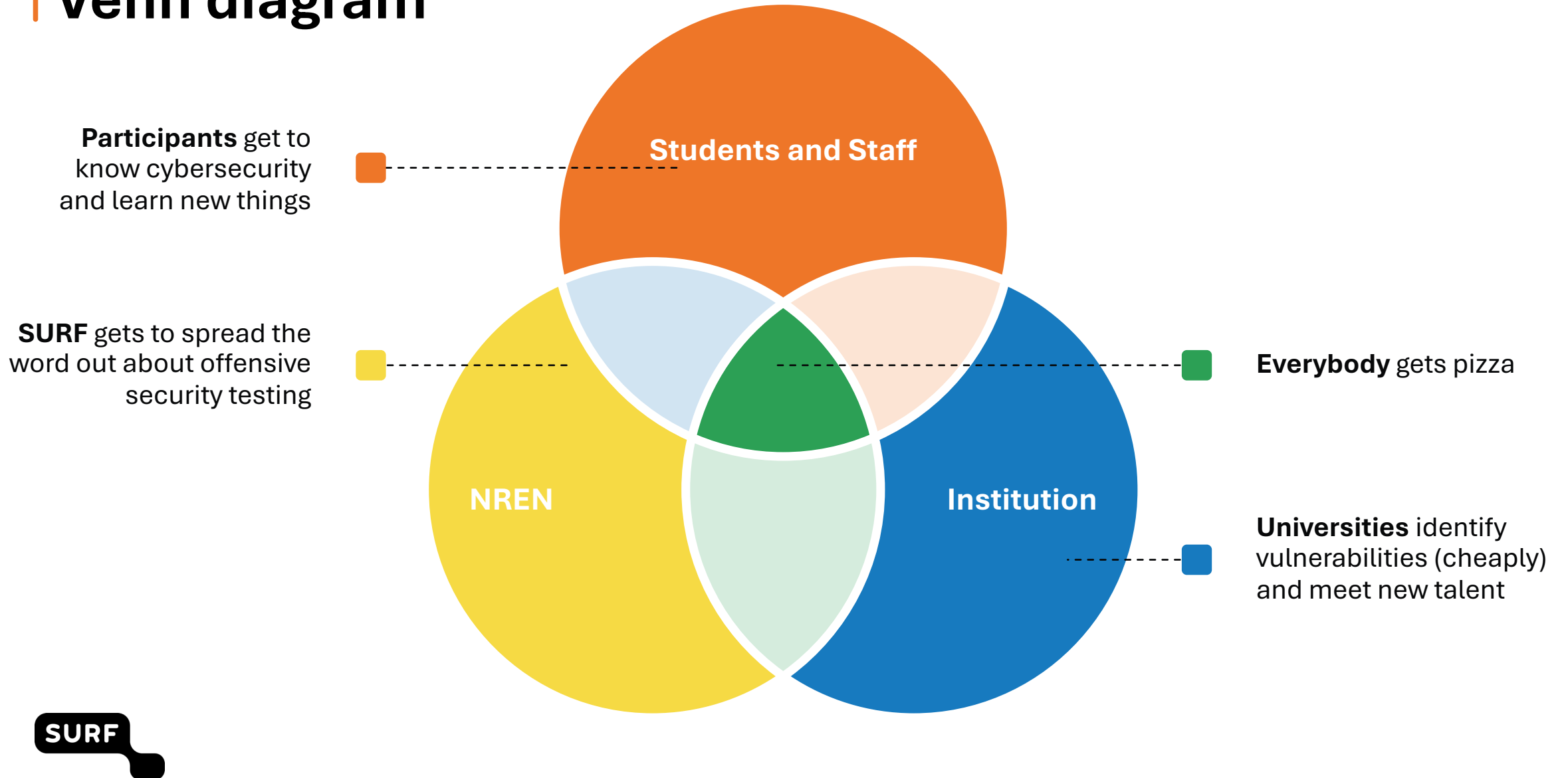
- Invite your favourite troublemakers:

Students and IT staff!

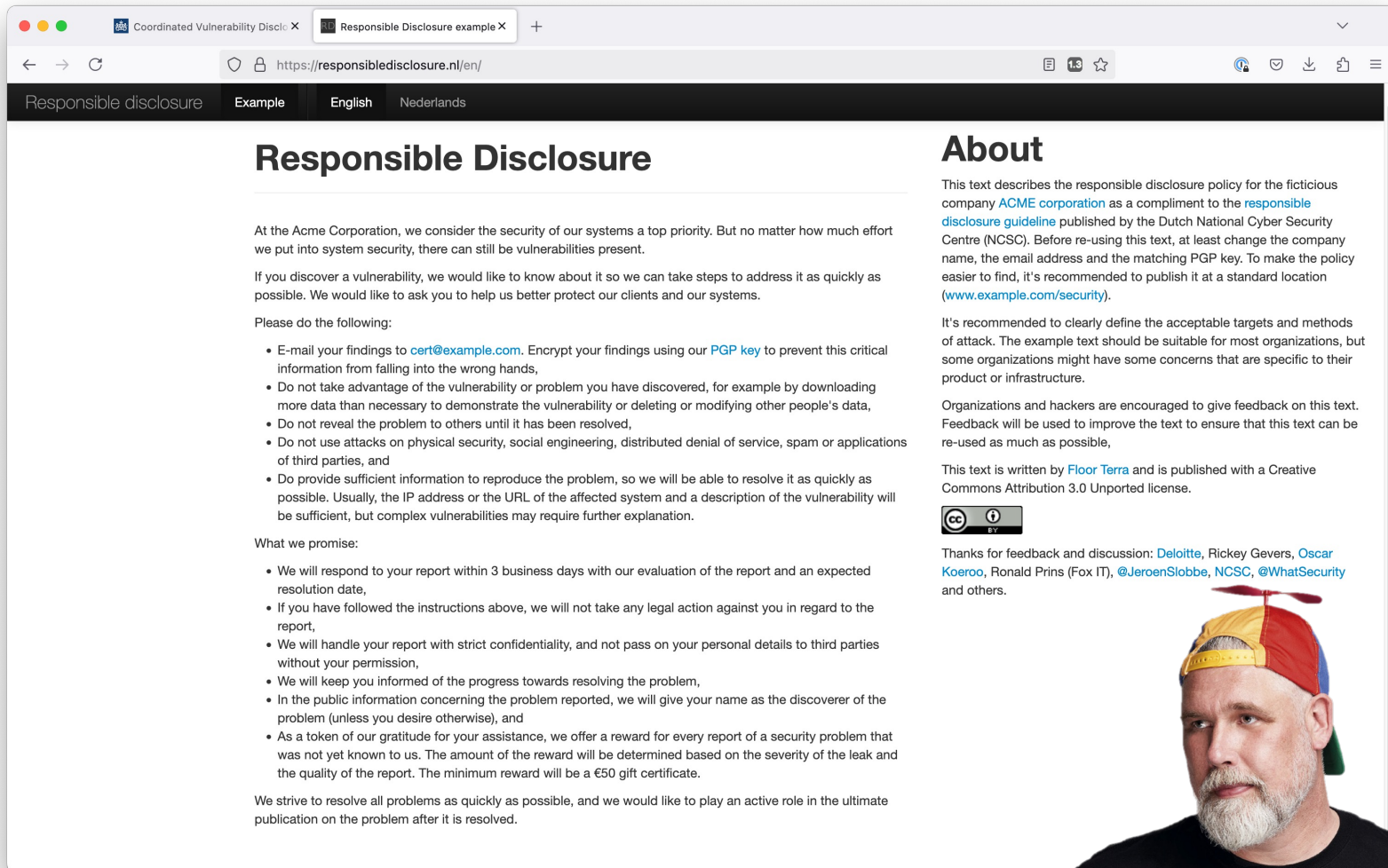
- Put them in a room with a network, food and Club-Mate
- **Find vulnerabilities**



Venn diagram



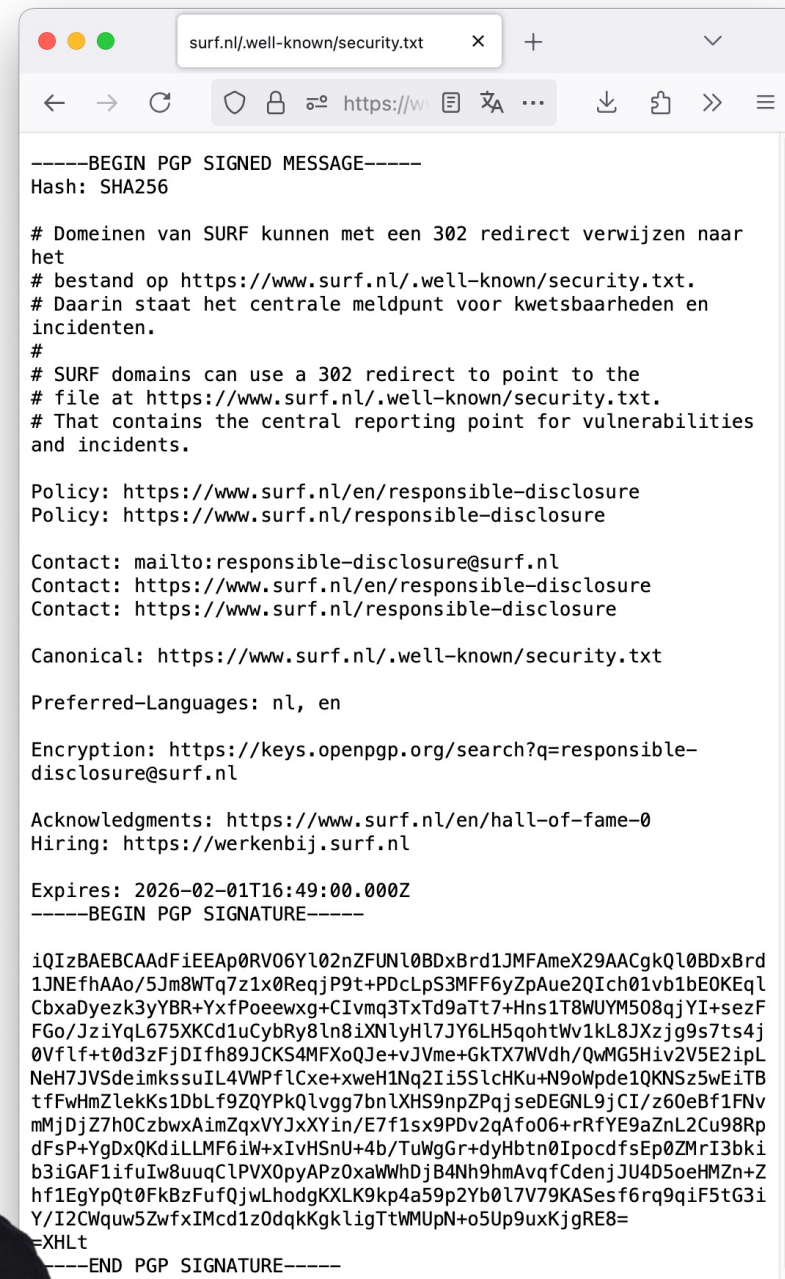
Responsible Disclosure



The screenshot shows a web browser displaying the 'Responsible Disclosure' page. The page has a dark header with navigation links: 'Responsible disclosure', 'Example', 'English', and 'Nederlands'. The main content area is titled 'Responsible Disclosure' and contains the following sections:

- About:** A paragraph explaining the policy for the fictitious company ACME corporation, mentioning the Dutch National Cyber Security Centre (NCSC) and a PGP key for secure communication.
- What we promise:** A list of five promises, including responding within 3 business days, confidentiality, and a reward for security problems.
- What we expect:** A list of five expectations, including providing sufficient information, not using attacks, and not revealing the problem to others.

At the bottom of the page, there is a photo of a man with a beard and a red and yellow cap, wearing a black t-shirt.



The screenshot shows a web browser displaying a PGP signed message. The message is titled '-----BEGIN PGP SIGNED MESSAGE-----' and contains the following text:

```
Hash: SHA256

# Domeinen van SURF kunnen met een 302 redirect verwijzen naar
# het
# bestand op https://www.surf.nl/.well-known/security.txt.
# Daarin staat het centrale meldpunt voor kwetsbaarheden en
# incidenten.
#
# SURF domains can use a 302 redirect to point to the
# file at https://www.surf.nl/.well-known/security.txt.
# That contains the central reporting point for vulnerabilities
# and incidents.

Policy: https://www.surf.nl/en/responsible-disclosure
Policy: https://www.surf.nl/responsible-disclosure

Contact: mailto:responsible-disclosure@surf.nl
Contact: https://www.surf.nl/en/responsible-disclosure
Contact: https://www.surf.nl/responsible-disclosure

Canonical: https://www.surf.nl/.well-known/security.txt

Preferred-Languages: nl, en

Encryption: https://keys.openpgp.org/search?q=responsible-
disclosure@surf.nl

Acknowledgments: https://www.surf.nl/en/hall-of-fame-0
Hiring: https://werkenbij.surf.nl

Expires: 2026-02-01T16:49:00.000Z
-----BEGIN PGP SIGNATURE-----

iQIzBAECAAdFiEEAp0RV06Yl02nZFUNl0BDxBrd1JMFameX29AACgkQl0BDxBrd
1JNEfhAAo/5Jm8WTq7z1x0ReqjP9t+PdCLpS3MFF6yZpAue2QIch01vb1bE0KEqL
CbxADyezK3yYBfPoeewxg+CIvmq3TxTd9aTt7+Hns1T8WUYM508qjYI+sezF
FGo/JziYqL675XKCd1uCybRy8ln8iXNlyHl7JY6LH5qohtWv1kL8JXzjg9s7ts4j
0VfLf+t0d3zFjDIfh89JCKS4MFxQ0Je+vJVme+GkTX7WVdh/QwMG5Hiv2V5E2ipL
NeH7JVSdeimkssuIL4VWPfLcxe+xweH1Nq2Ii5S1cHKu+N9oWpde1QKNSz5wEiTB
tffWmZlekKs1DbLf9ZQYPkQlvvg7bnlXHS9npZPqjseDEGNL9jCI/z60eBf1FNv
mMjDjZ7h0CzbxwAimZqxVYjXxYin/E7f1sx9PDv2qAfo06+rRfYE9aZnL2Cu98Rp
dFsP+YgDxQKdiLLMF6iW+xIvHSnU+4b/TuWgGr+dyHbnt0IpocdfsEp0ZMrI3bki
b3iGAF1ifuIw8uuqCLPVX0pyAPz0xaWWhdjb4N9hmAvqfCdenjJU4D5oeHMZn+Z
hf1EgYpQt0FkBzFufqjwLhdgKXLK9kp4a59p2Yb0l7V79KASes6f9q9qif5tG3i
Y/I2Cwquw5ZwfxIMcd1z0dqkGgkligTtWMUpN+o5Up9uxKjgRE8=
=XHLt
-----END PGP SIGNATURE-----
```

| Impressions



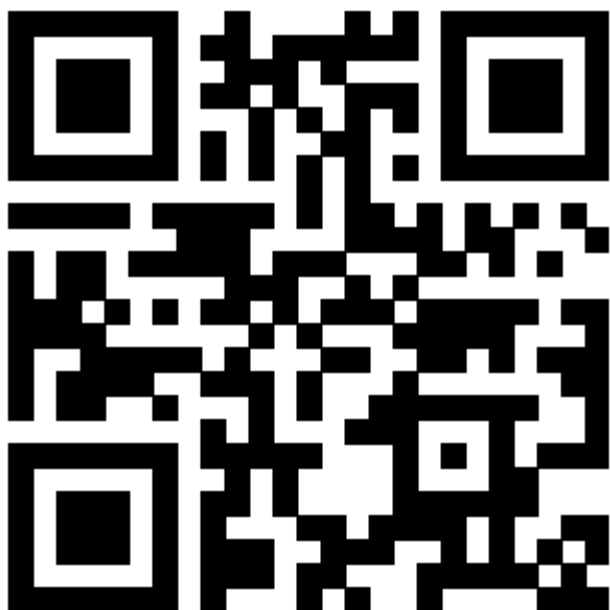
| Impressions



Switch



| DIY



edu.nl/7mu6a

joost.gadellaa@surf.nl

