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

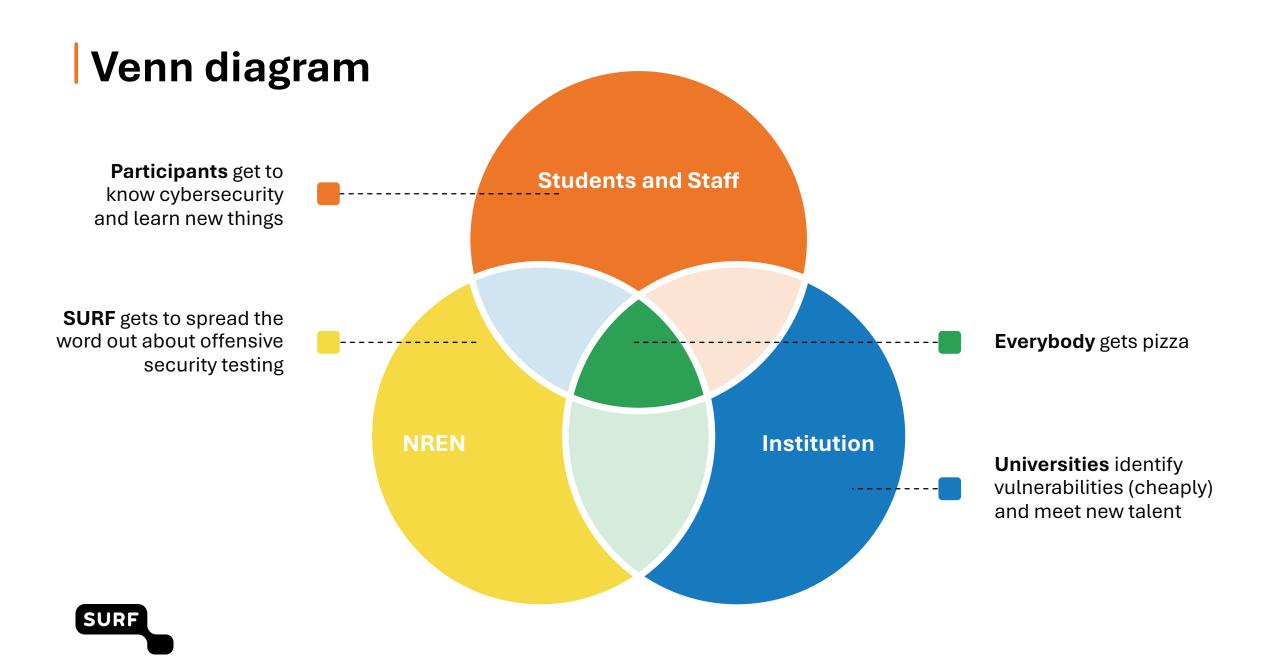
 Invite your favourite troublemakers:

Students and IT staff!

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







Responsible Disclosure

e e e 📓 Coordinated Vuln	erability Disclo X	RD Responsible Disclo	osure example $ imes$	+			~	/
$\leftarrow \rightarrow C$	ightarrow C $ ightarrow$ https://responsibledisclosure.nl/en/		ure.nl/en/	目 🗈 公	0	V 1	<u>ک</u> ک	≏ =
Responsible disclosure	Example	English Nede	erlands					

Responsible Disclosure

At the Acme Corporation, we consider the security of our systems a top priority. But no matter how much effort we put into system security, there can still be vulnerabilities present.

If you discover a vulnerability, we would like to know about it so we can take steps to address it as quickly as possible. We would like to ask you to help us better protect our clients and our systems.

Please do the following:

- E-mail your findings to cert@example.com. Encrypt your findings using our PGP key to prevent this critical information from falling into the wrong hands,
- Do not take advantage of the vulnerability or problem you have discovered, for example by downloading
 more data than necessary to demonstrate the vulnerability or deleting or modifying other people's data,
- Do not reveal the problem to others until it has been resolved,
 Do not use attacks on physical security, social engineering, distributed denial of service, spam or applications
- bo not use attacks on physical security, social engineering, distributed denial of service, sparn or applications of third parties, and
- Do provide sufficient information to reproduce the problem, so we will be able to resolve it as quickly as
 possible. Usually, the IP address or the URL of the affected system and a description of the vulnerability will
 be sufficient, but complex vulnerabilities may require further explanation.

What we promise:

- We will respond to your report within 3 business days with our evaluation of the report and an expected
 resolution date,
- If you have followed the instructions above, we will not take any legal action against you in regard to the report,
- We will handle your report with strict confidentiality, and not pass on your personal details to third parties without your permission,
- We will keep you informed of the progress towards resolving the problem,
- In the public information concerning the problem reported, we will give your name as the discoverer of the
 problem (unless you desire otherwise), and
- As a token of our gratitude for your assistance, we offer a reward for every report of a security problem that
 was not yet known to us. The amount of the reward will be determined based on the severity of the leak and
 the quality of the report. The minimum reward will be a €50 gift certificate.

We strive to resolve all problems as quickly as possible, and we would like to play an active role in the ultimate publication on the problem after it is resolved.

About

This text describes the responsible disclosure policy for the ficticious company ACME corporation as a compliment to the responsible disclosure guideline published by the Dutch National Cyber Security Centre (NCSC). Before re-using this text, at least change the company name, the email address and the matching PGP key. To make the policy easier to find, it's recommended to publish it at a standard location (www.example.com/security).

It's recommended to clearly define the acceptable targets and methods of attack. The example text should be suitable for most organizations, but some organizations might have some concerns that are specific to their product or infrastructure.

Organizations and hackers are encouraged to give feedback on this text. Feedback will be used to improve the text to ensure that this text can be re-used as much as possible,

This text is written by Floor Terra and is published with a Creative Commons Attribution 3.0 Unported license.



Thanks for feedback and discussion: Deloitte, Rickey Gevers, Oscar Koeroo, Ronald Prins (Fox IT), @JeroenSlobbe, NCSC, @WhatSecurity and others.



-----BEGIN PGP SIGNED MESSAGE-----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=responsibledisclosure@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-----

iQIzBAEBCAAdFiEEAp0RV06Yl02nZFUNl0BDxBrd1JMFAmeX29AACgkQl0BDxBrd 1JNEfhAAo/5Jm8WTq7z1x0ReqjP9t+PDcLpS3MFF6yZpAue2QIch01vb1bE0KEql CbxaDyezk3yYBR+YxfPoeewxg+CIvmq3TxTd9aTt7+Hns1T8WUYM508qjYI+sezF FGo/JziYqL675XKCd1uCybRy8ln8iXNlyHl7JY6LH5qohtWv1kL8JXzjg9s7ts4j 0Vflf+t0d3zFjDIfh89JCK54MFXoQJe+vJVme+GkTX7WVdh/QwMG5Hiv2V5E2ipL NeH7JVSdeimkssuIL4VWPf1Cxe+xweH1Nq2Ii5S1cHKu+N90Wpde1QKNSz5wEiTB tfFwHmZlekKs1DbLf9ZQYPkQlvgg7bn1XH59npZPqjseDEGNL9jCI/z60eBf1FNv mMjDjZ7h0CzbwxAimZqxVYJxXYin/E7f1sx9PDv2qAfo06+rRfYE9aZnL2Cu98Rp dFsP+YgDxQKdiLLMF6iW+xIvHSnU+4b/TuWgGr+dyHbtn0IpocdfsEp0ZMrI3bki b3iGAF1ifuI%8uuqClPVX0pyAP20xaWWhDjB4Nh9hmAvqfCdenjJU4D5oeHMZn+Z hf1EgYpQt0FkBzFufQjwLhodgKXLK9kp4a59p2Yb017V79KASesf6rq9qiF5tG3i ¥/I2CWquw5ZwfxIMcd1z0dqkKgkligTtWMUpN+o5Up9uxKjgRE8= EXHLt

--END PGP SIGNATURE-----



Impressions









Impressions









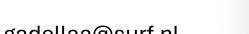
edu.nl/7mu6a

DIY

Q **Event kit** $\equiv \hat{}$ \gg < \rightarrow Event kit +Kind Name ✓ Size > D Promotion & Marketing material -- Folder Handouts -- Folder > Guides & Additional -- Folder > README.odt 47 KB **OpenD...ent Text** Q&A Halon.odt 7 KB **OpenD...ent** Text Contracting a triage provider.odt 10 KB OpenD...ent Text Checklist before event.odt **OpenD...ent** Text 21 KB

SURF

joost.gadellaa@surf.nl



About scoping.odt

Û 📿

22 KB

OpenD...ent Text