

Security beginnt in der Ausbildung

Impulsvortrag für ICT-BerufsbildnerInnen

10. FEBRUAR 2026



Frontify



**ICT Berufsbildung
Ostschweiz**

Vanessa Sutter

- Product Security Lead bei Frontify
- Mitglied Vorstand ICT Berufsbildung Ostschweiz
- Prüfungsexpertin InformatikerInnen EFZ

#Informatikerin Applikationsentwicklung EFZ

#Wirtschaftsinformatik Bsc

Ich weiss, wie Lernende denken, ich war selbst dort.



Montagmorgen,
09:00 Uhr

Ein Lernender führt `npm install` aus. Alles funktioniert. Tests sind grün.



Warum ist Security JETZT so wichtig?

36%

aller Cyberangriffe starten
mit Social Engineering

Supply Chain Angriffe verdoppelt (30% aller Breaches)

AI macht Phishing täuschend echt

Verlagerung in Cloud und Build-Pipelines

Die Top 4 Bedrohungen

Supply Chain Abuse

npm, IDE-Plugins

AI-Phishing

Deepfakes, Voice Cloning

Cloud & CI/CD Exploitation

Pipelines, GitHub Actions

Credential Theft

Tokens, Keys, Cookies

<https://services.google.com/fh/files/misc/cybersecurity-forecast-2026-en.pdf>



Fall 1: Shai-Hulud – Der npm Wurm

September 2025: `rxnt-authentication` installiert

Selbstreplizierender Wurm

- 180+ Pakete infiziert
- AWS-Keys & GitHub-Tokens gestohlen

Fall 2: Wenn Vertrauen zur Waffe wird

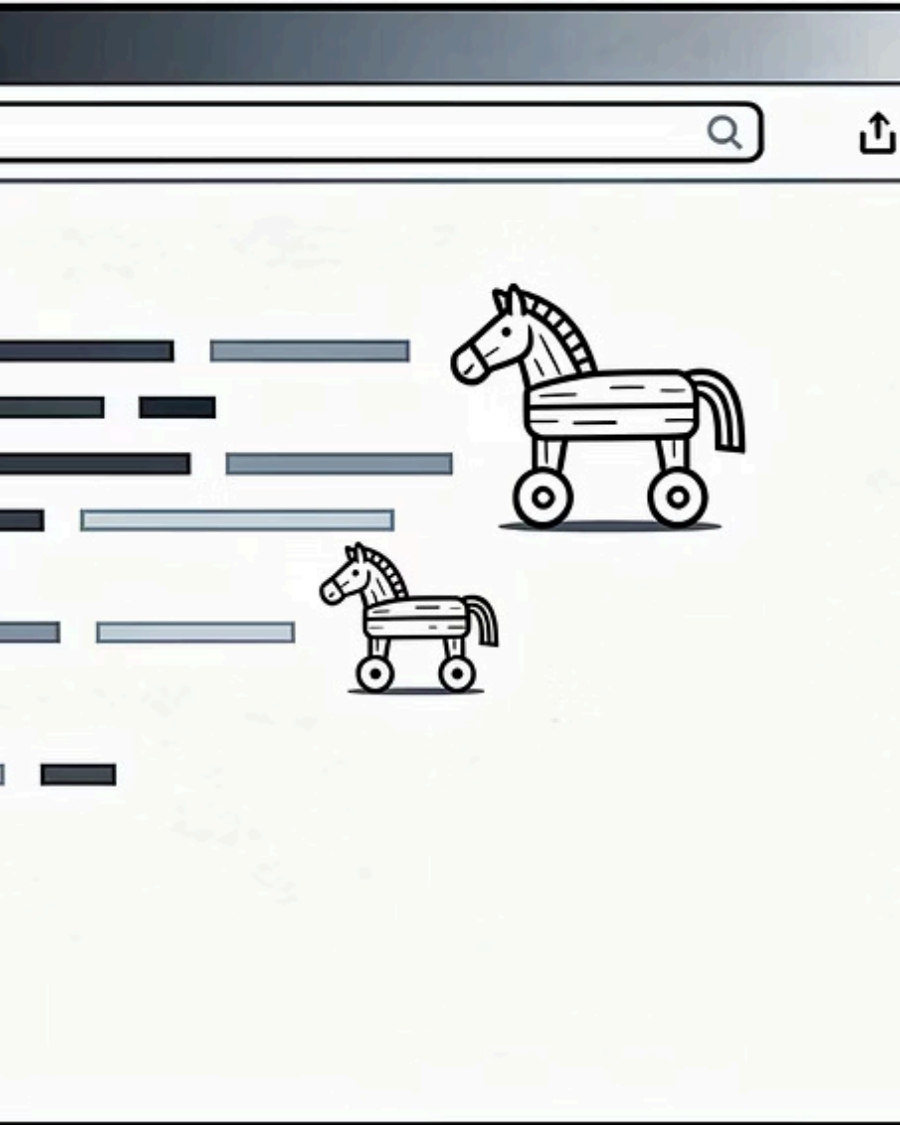
Maintainer von chalk (300M Downloads/Woche) erhält E-Mail

"Aktualisiere 2FA in 48h"

Absender: npmjs.help → Er klickt. Angreifer übernehmen Pakete.

Social Engineering = Zeitdruck + Vertrauen





Fall 3: Glassworm – Trojaner im Editor

Dezember 2025: 24 VSCode Extensions

Versprechen

"AI Code Completion"

Realität

Stiehlt .env Files, Git
Credentials, sendet
Code

Fall 4: AI-Deepfake

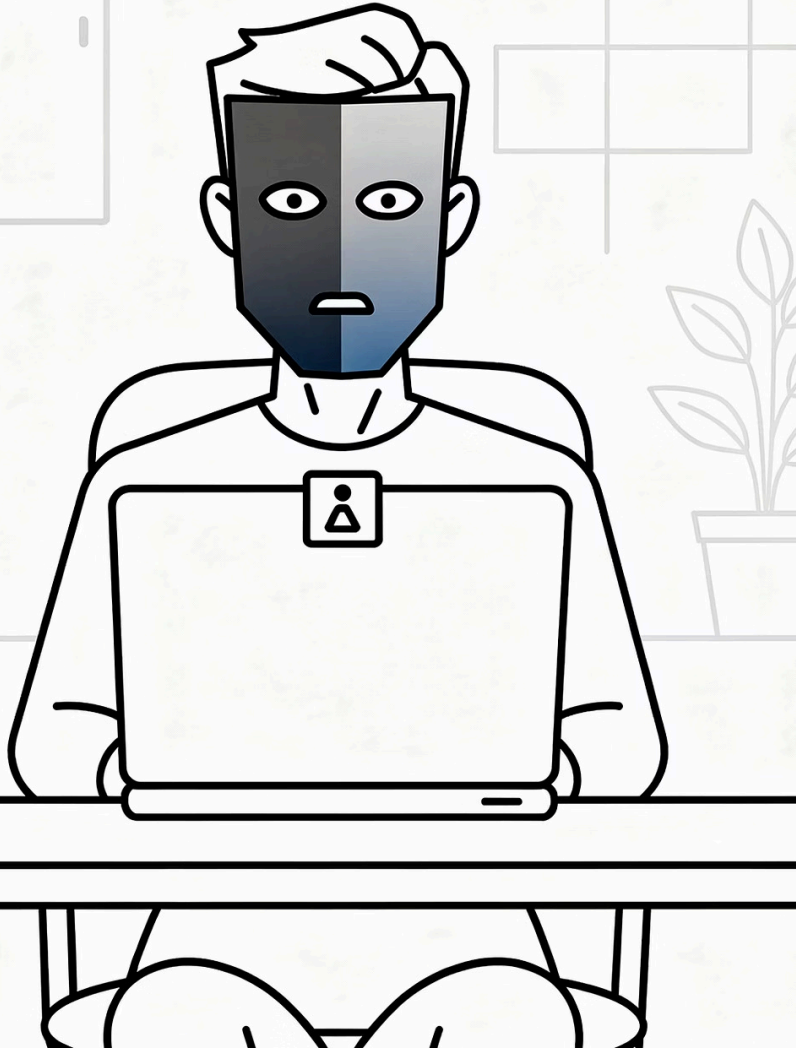
Lernender erhält Teams-Call vom "CTO"

Voice Cloning → identische Stimme

"Ich brauche DRINGEND Prod-Server Zugang"

→ 65% nutzen heute Impersonation

AI macht Social Engineering skalierbar



Fall 5: DataByCloud – Der Browser-Spion

Januar 2026: "Data Access Tool" im Chrome Store. 251 Downloads.

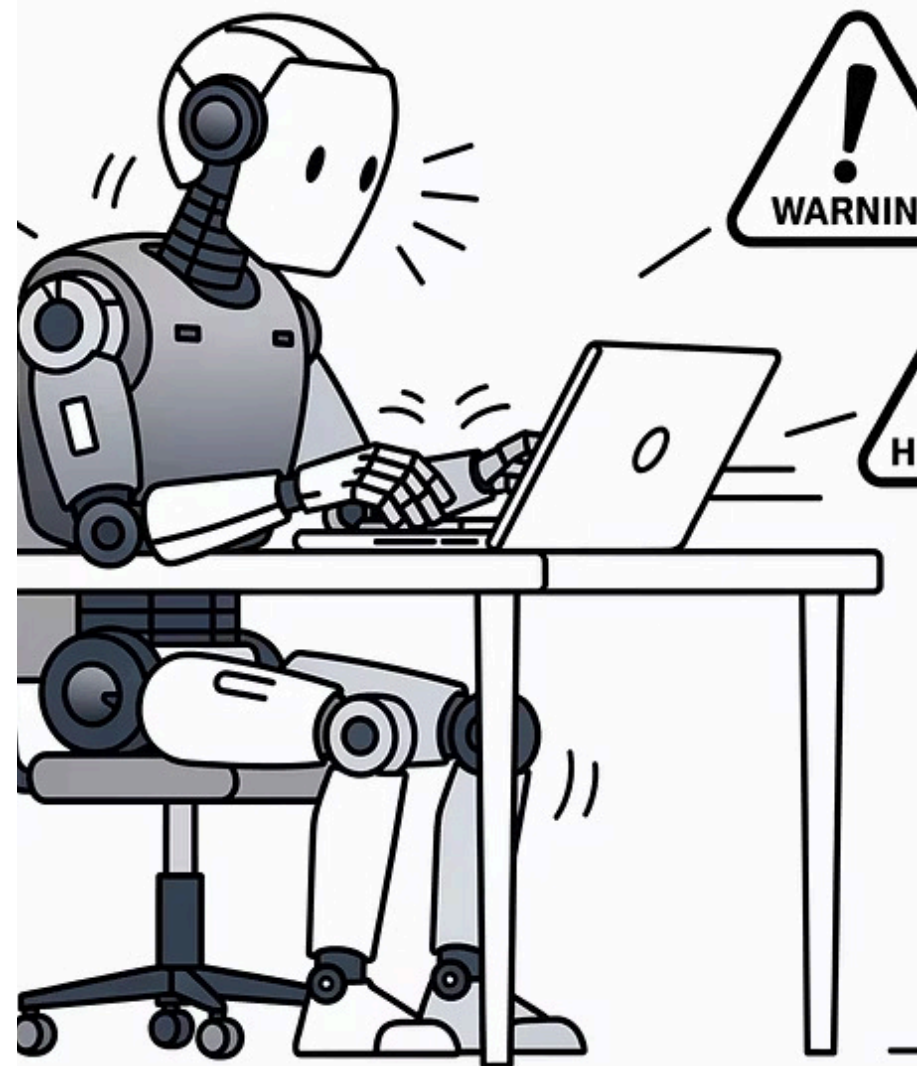
5 koordinierte Extensions

Stehlen Enterprise Logins, Cookies, History



Fall 6: Vibe Coding – Schnell aber gefährlich

AI erstellt Todo-App in 5 Minuten



Warum ALLE betroffen sind

Applikationsentwickler

npm, Vibe Coding, GitHub OAuth

Plattformentwickler

Cloud-Tools, Automation

Mediamatiker

Browser Extensions, CMS-Plugins

ICT-Fachleute

Admin-Tools, System-Plugins

Was können wir tun?

Praktische Tipps für die Ausbildung



1. Security Mindset entwickeln



Kritisches Denken fördern:

- "Was könnte schiefgehen?"
- "Wer hat Zugriff?"
- "Warum so viele Berechtigungen?"

2. Hands-on statt Theorie



Fälle analysieren

Gemeinsam echte Incidents durchgehen



Code Reviews

"Ist das sicher?" als Standard-Frage



CTF Challenges

TryHackMe, HackTheBox



Phishing-Simulationen

Praktische Übungen im Team



Security lernt man durch Tun

3. Sichere Dependency-Praktiken



- `npm audit` regelmässig nutzen
- Maintainer überprüfen
- Lock-Files verwenden
- Dependencies minimal halten

4. IDE und Tool-Hygiene

01

Nur verifizierte Quellen

Extensions aus offiziellen Stores

03

Updates kontrollieren

Changelog lesen vor Update

02

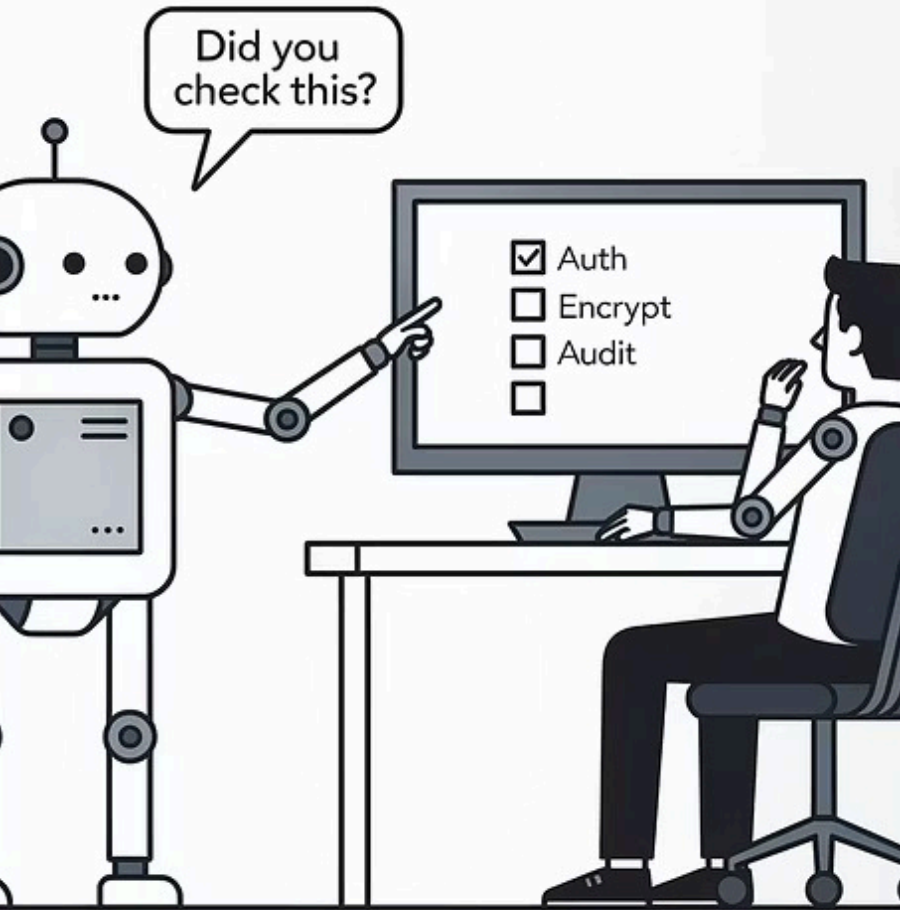
Berechtigungen prüfen

Browser + IDE Permissions checken

04

Aufräumen

Ungenutzte Plugins entfernen



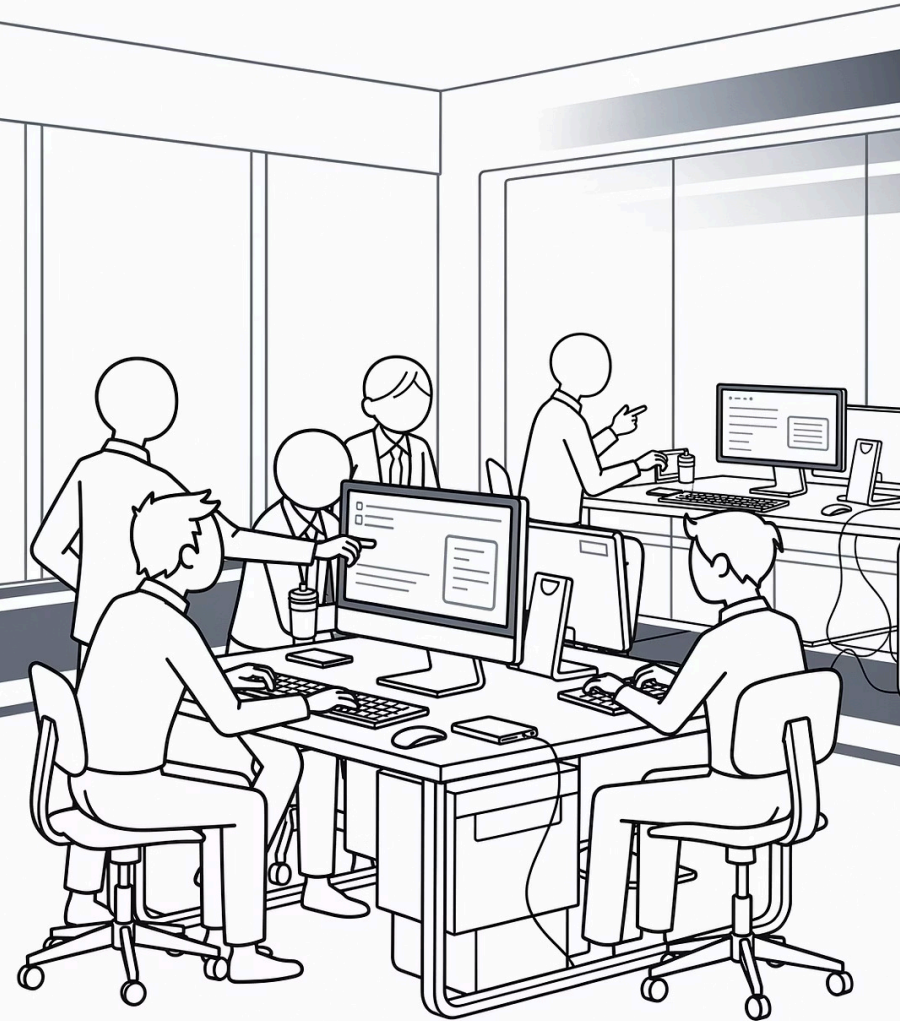
5. Vibe Coding sicher gestalten

AI-Code ist nur Entwurf
Nie blind übernehmen

Security Review
Keys, Auth, Validation
prüfen

GitHub OAuth Scopes
Minimal nötige Rechte

Nie Secrets in Public
Repos
Environment Variables
nutzen



6. Kostenlose Lernressourcen

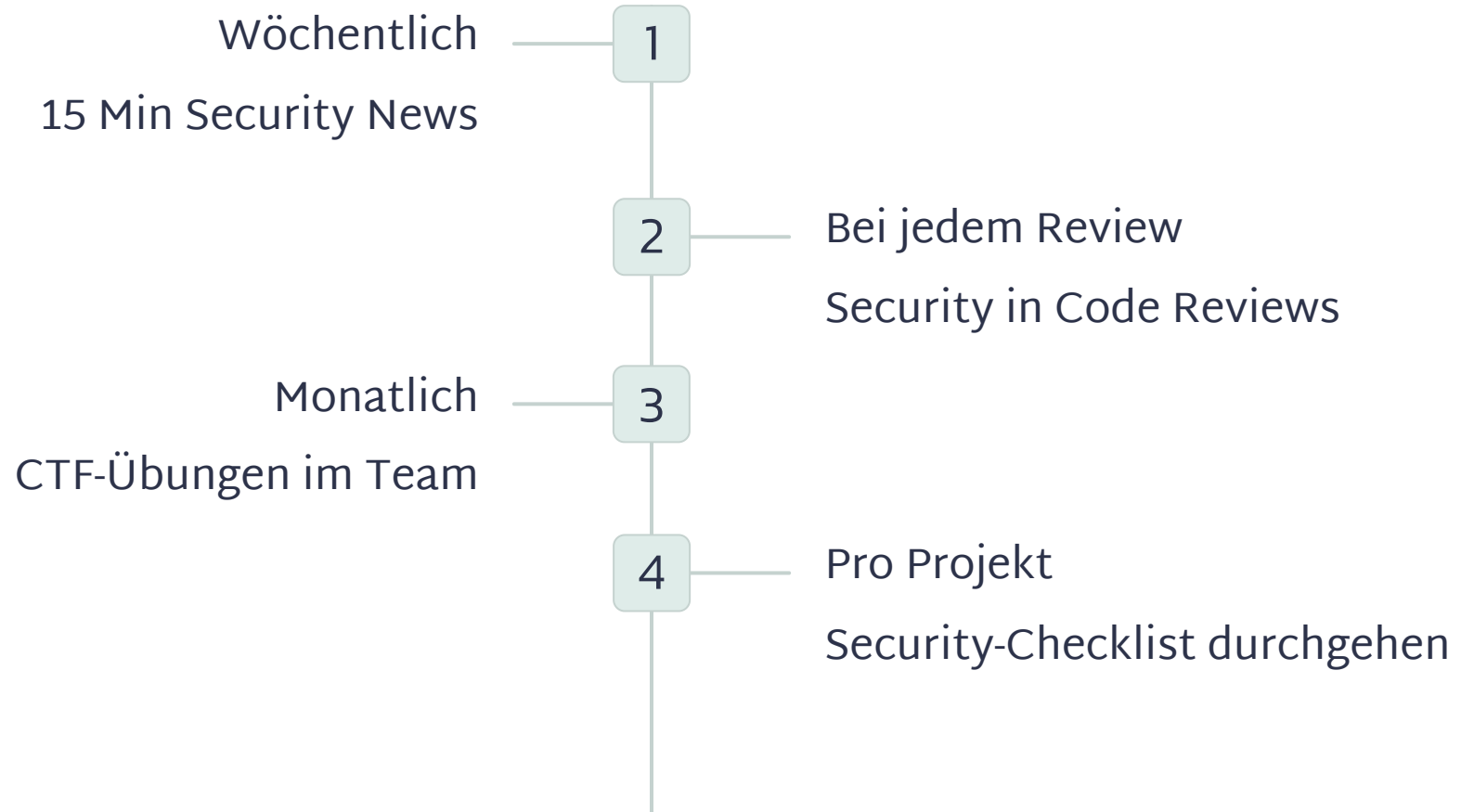
Plattformen

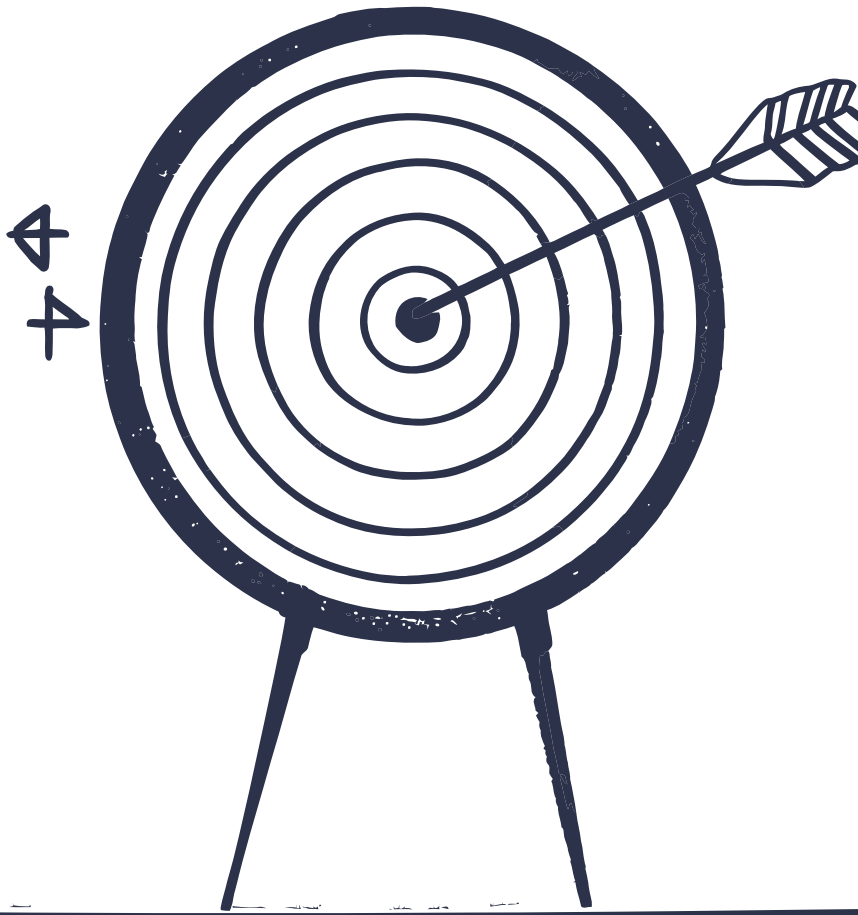
- TryHackMe
- HackTheBox
- OWASP

Community

- OWASP Schweiz
- Local Meetups

Integration in den Ausbildungsalltag





Kleine Schritte, grosse Wirkung

Ihr müsst nicht alles auf einmal umsetzen

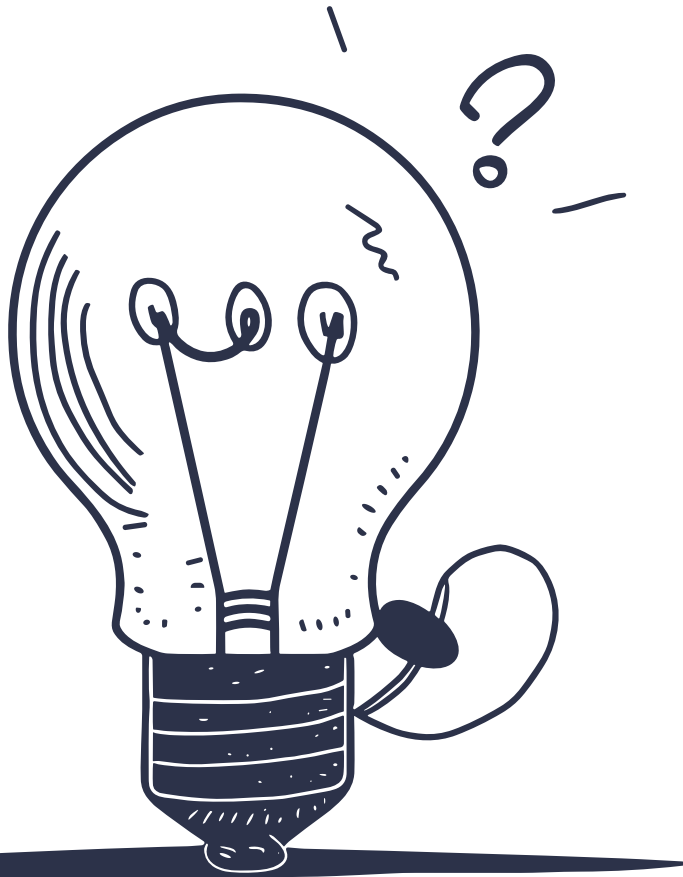
- Startet mit 1 Thema/Monat
- Schrittweise integrieren
- Gemeinsam lernen

Security ist eine Reise

Jeder Schritt zählt.

Eure Lernenden sind die nächste Generation von Security-bewussten Fachkräften.





Vielen Dank!

Fragen?

Gerne stehe ich für Austausch zur Verfügung

vanessa.sutter@frontify.com

<https://www.linkedin.com/in/vanessa-sutter/>