Your friendly Hackers


RED TEAM TAGEBUCH
KAPITEL 1
KAPITEL 2

CANCOM

Philipp Allmer

Philipp Reiter

Agenda

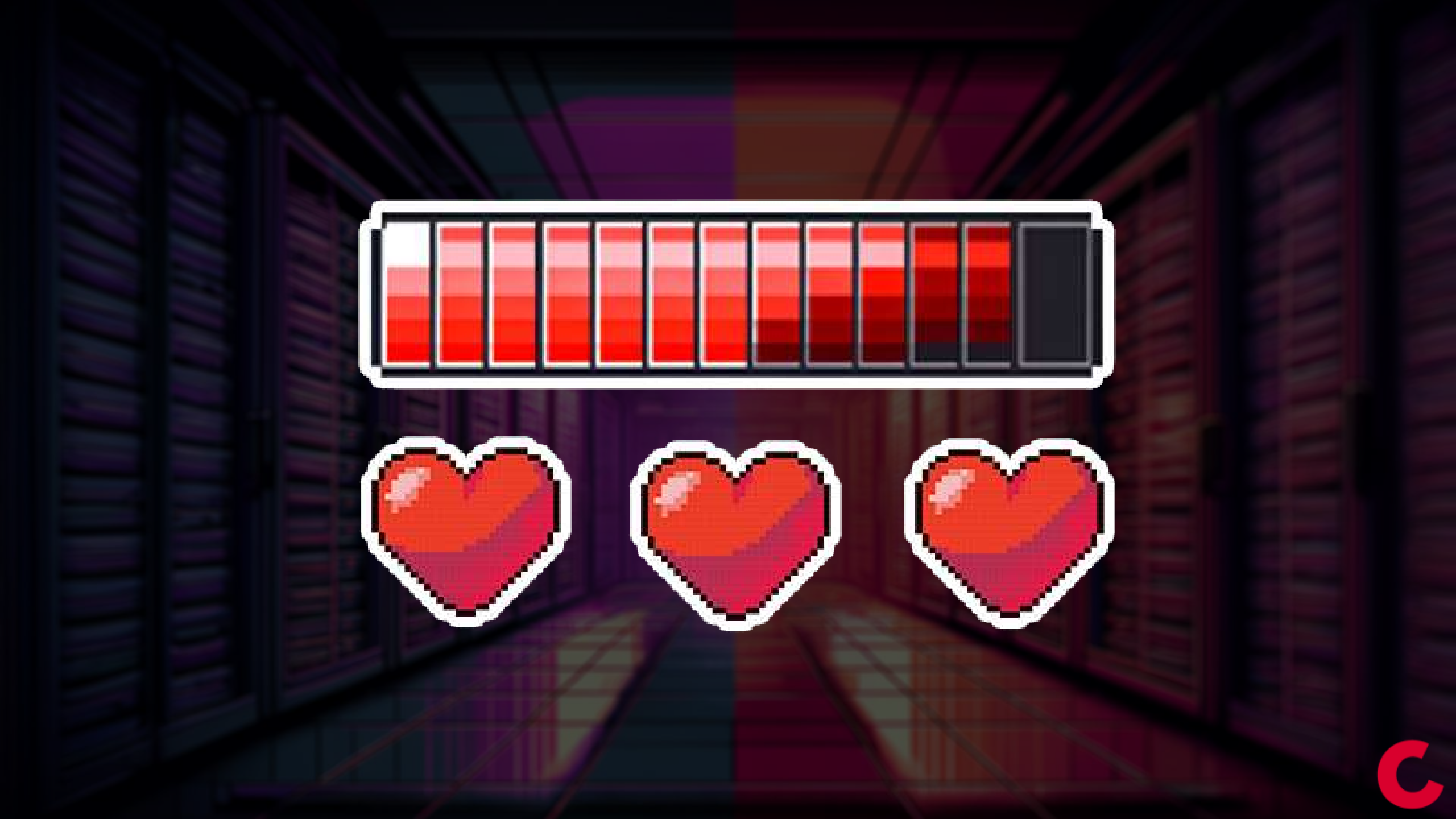
Catch Up
Auditor Life
Company Struggle
Nicht berühren
Learnings

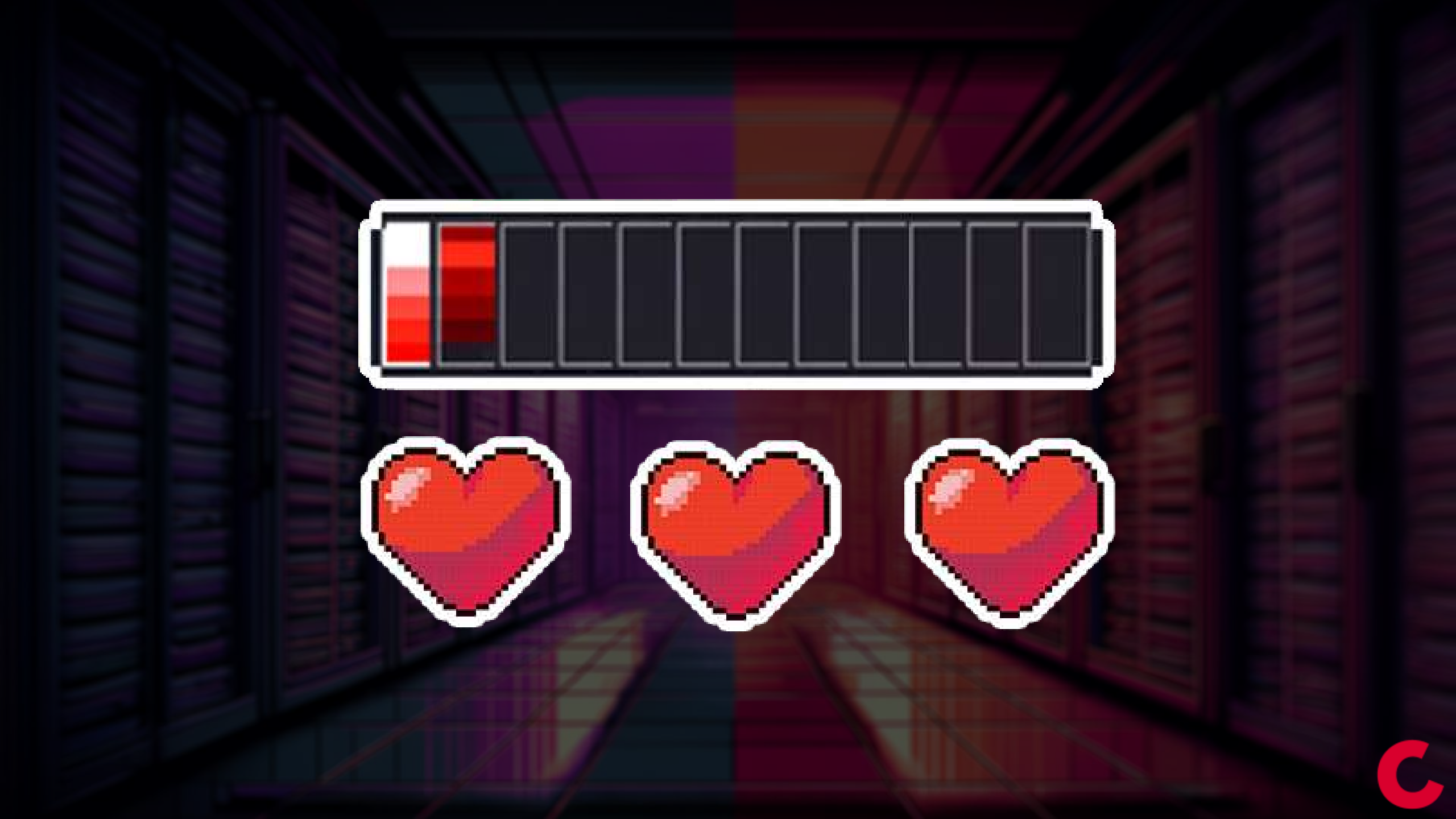

Catch Up

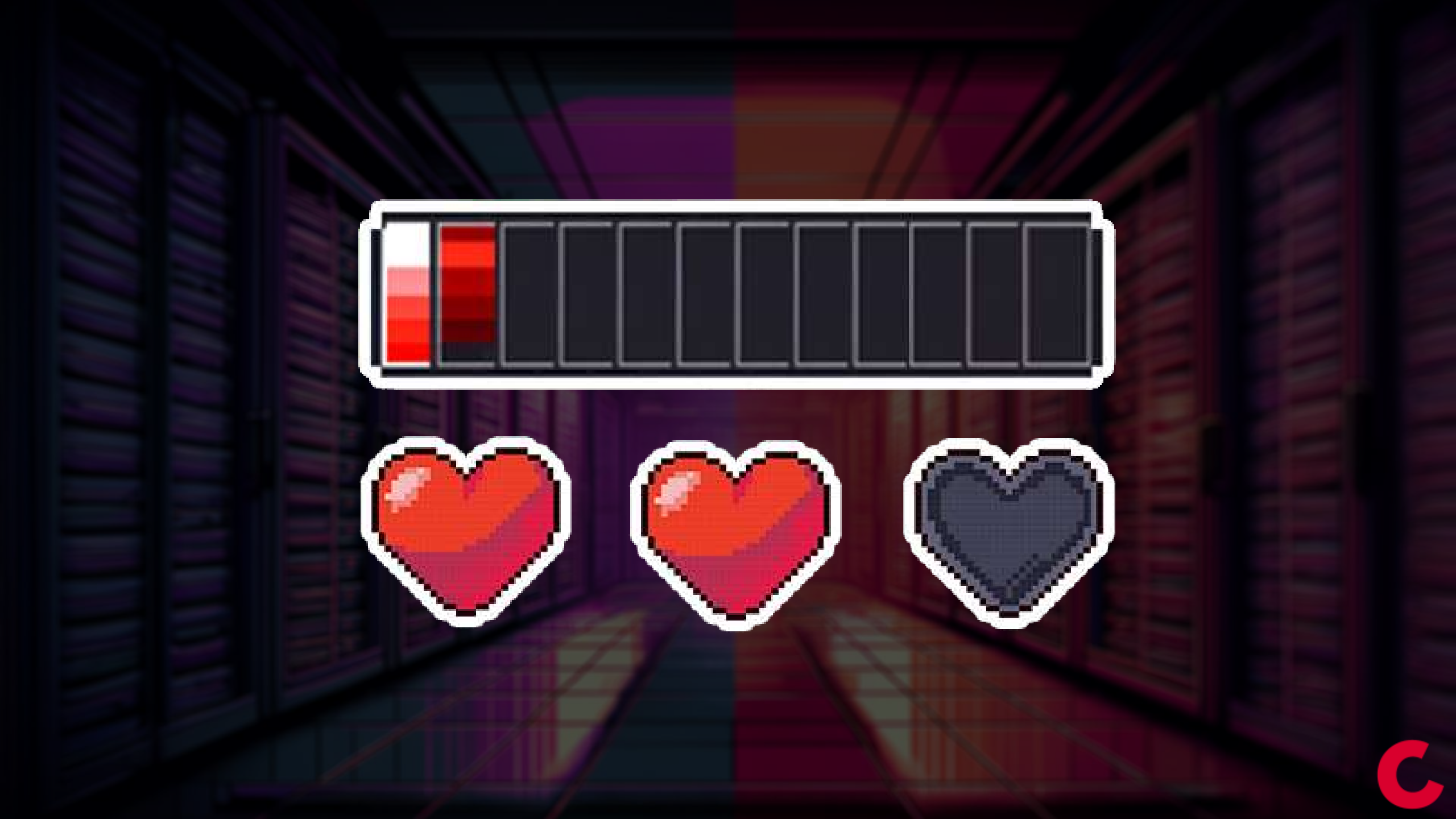

Hannes Trunde
K-Businesscom AG
fh
st.pölten
Hannes Trunde

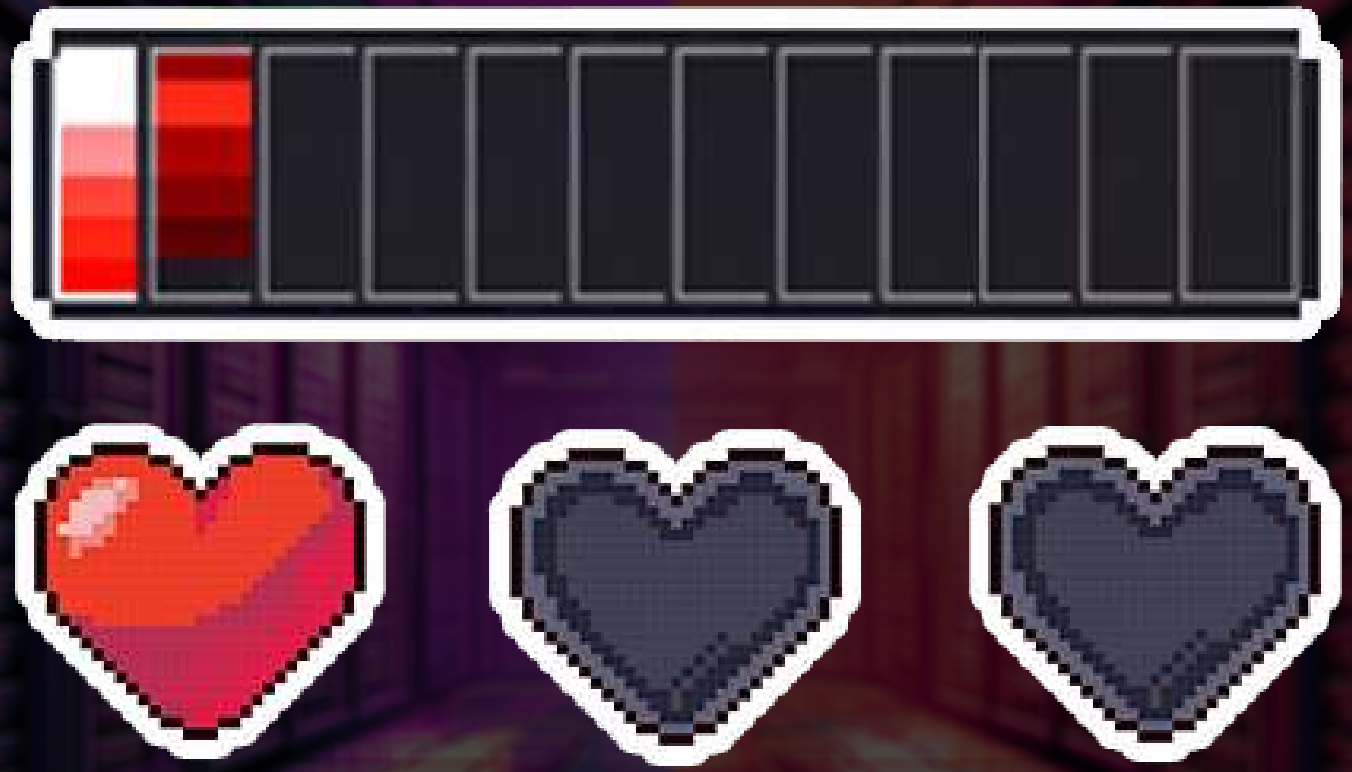
≠

≠










Auditor Life

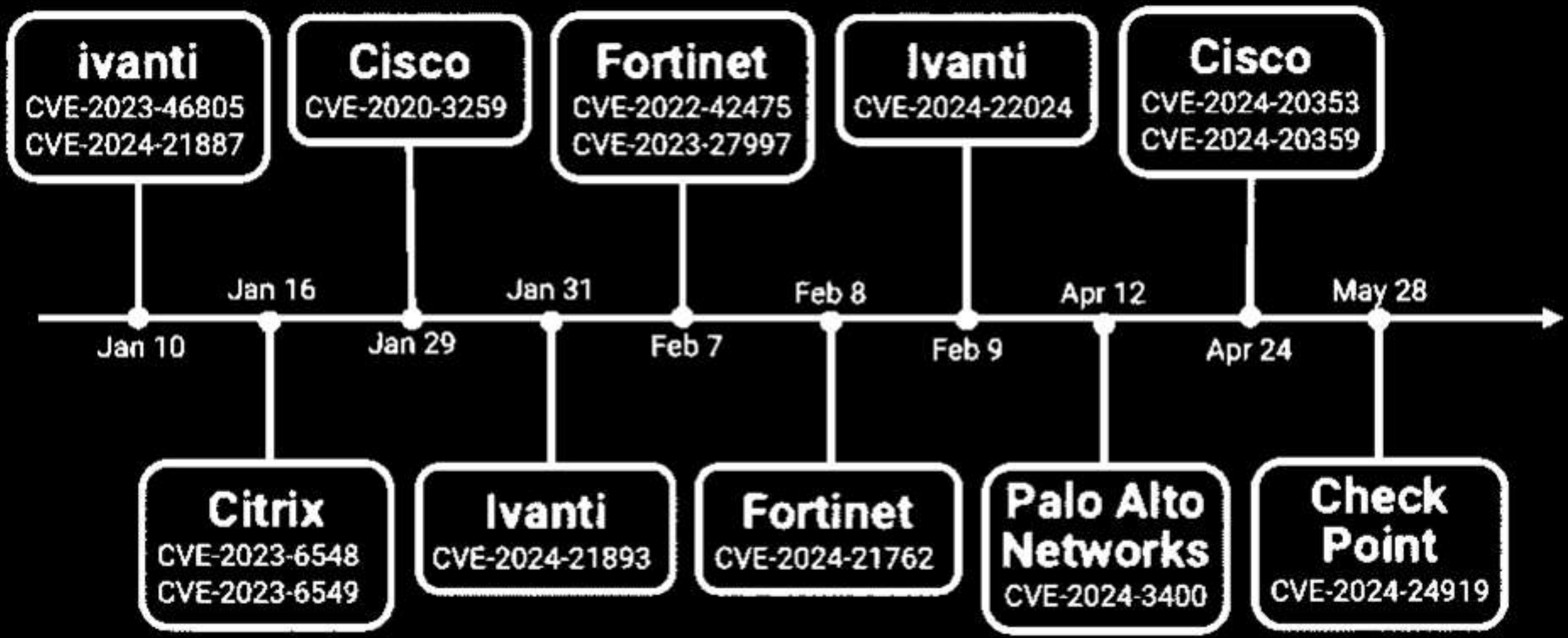
Stromkabel vergessen

well, that's bad for hannes. maybe playing around and replacing or changing the ssh keys was a bad idea. We will look, but whatever happened, it was fun. not.

Erwischt werden

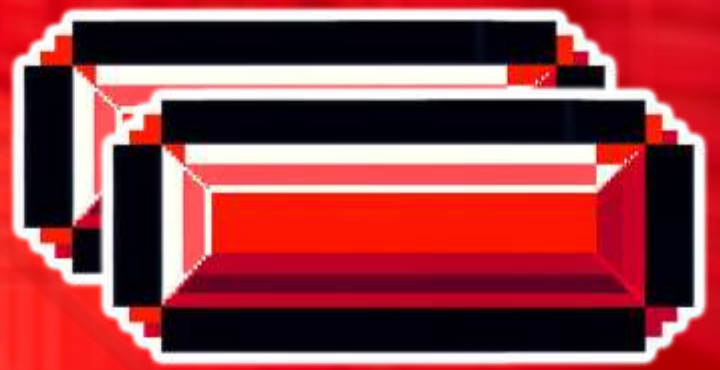

Company Struggle

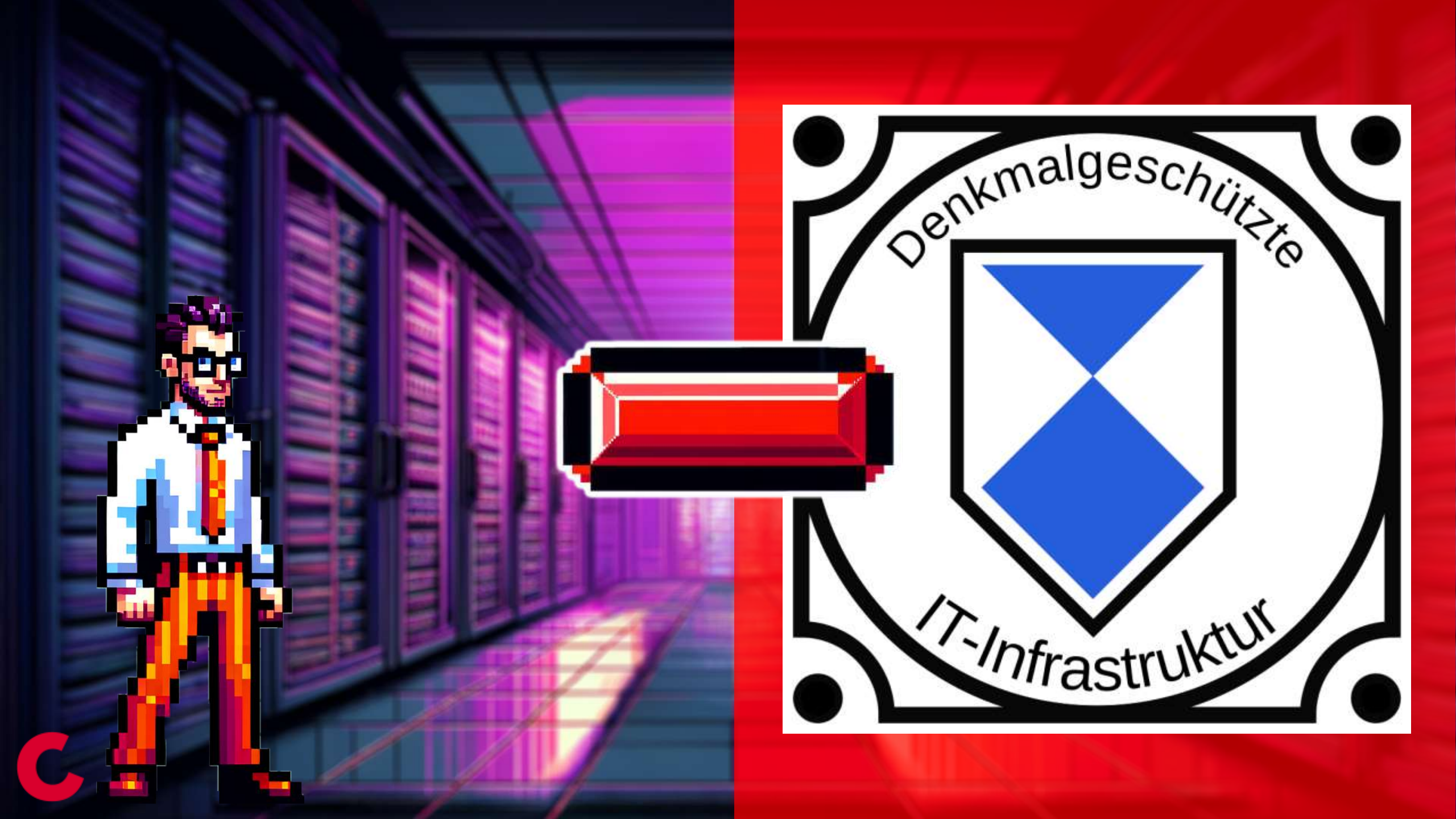
Bluescreen Update



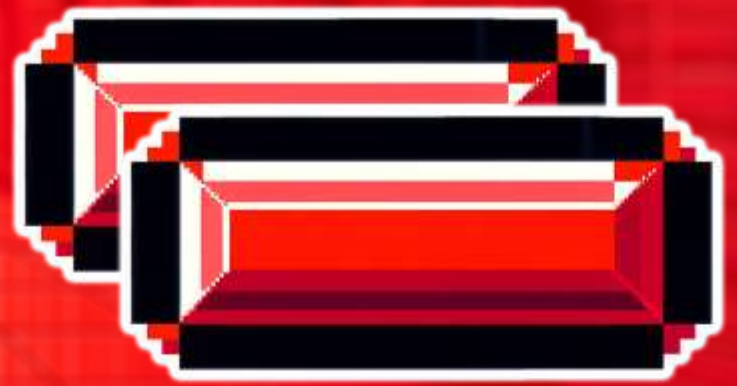
https://www.hackmageddon.com/2024/04/22/cves-targeting-remote-access-technologies/

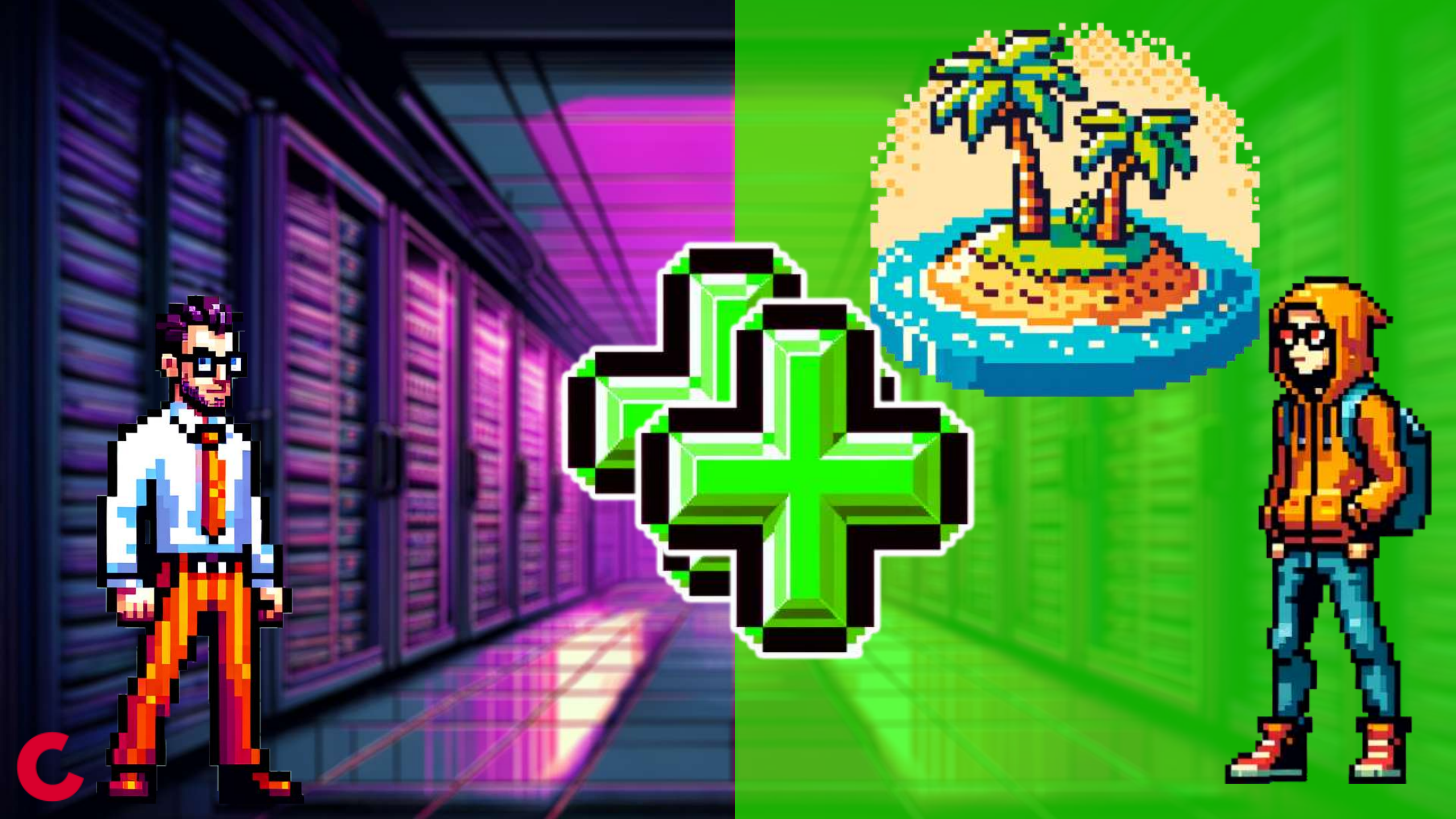
Surprise Hotfix Einsatz

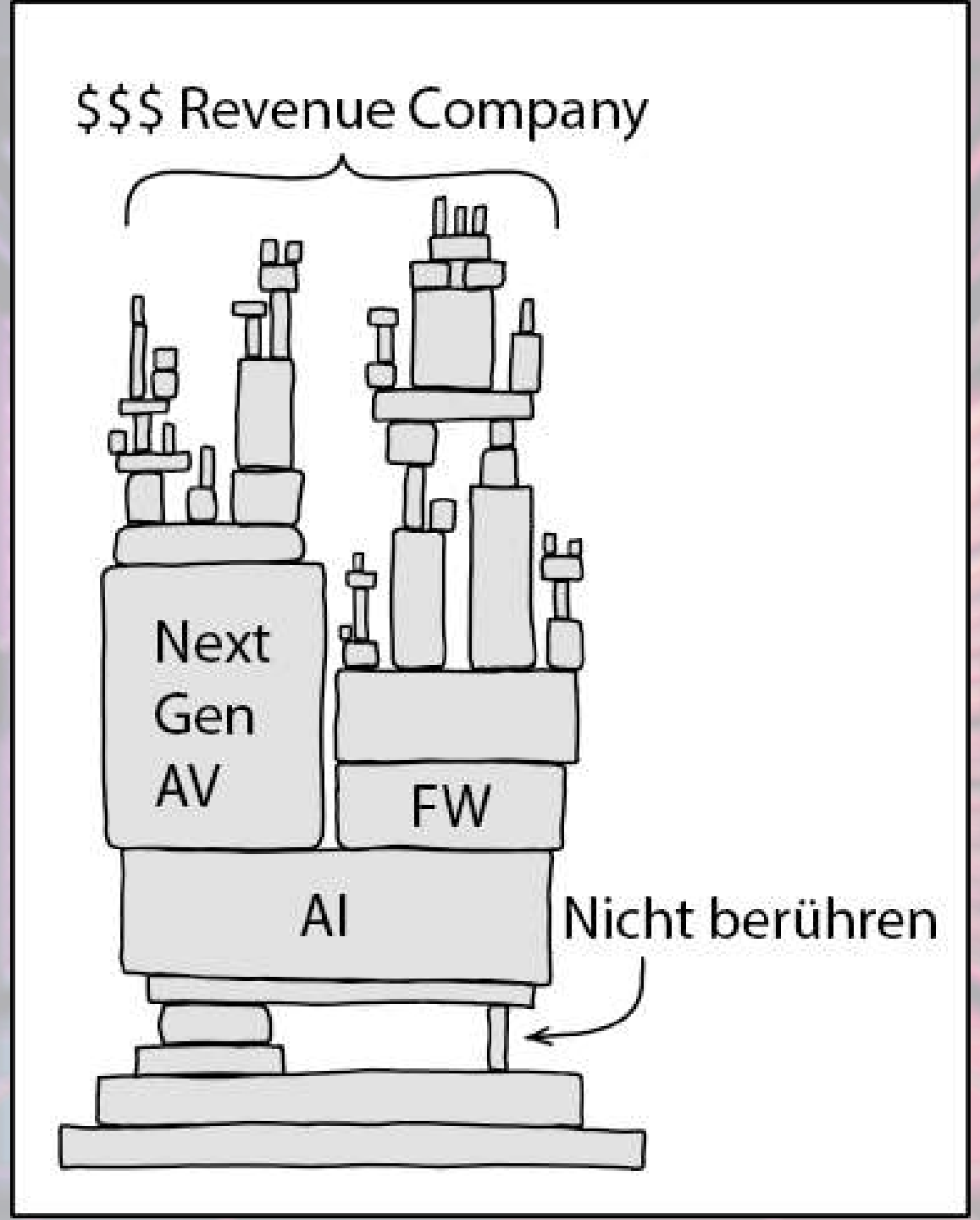



Denkmalgeschützte
IT-Infrastruktur

Surprise Backup





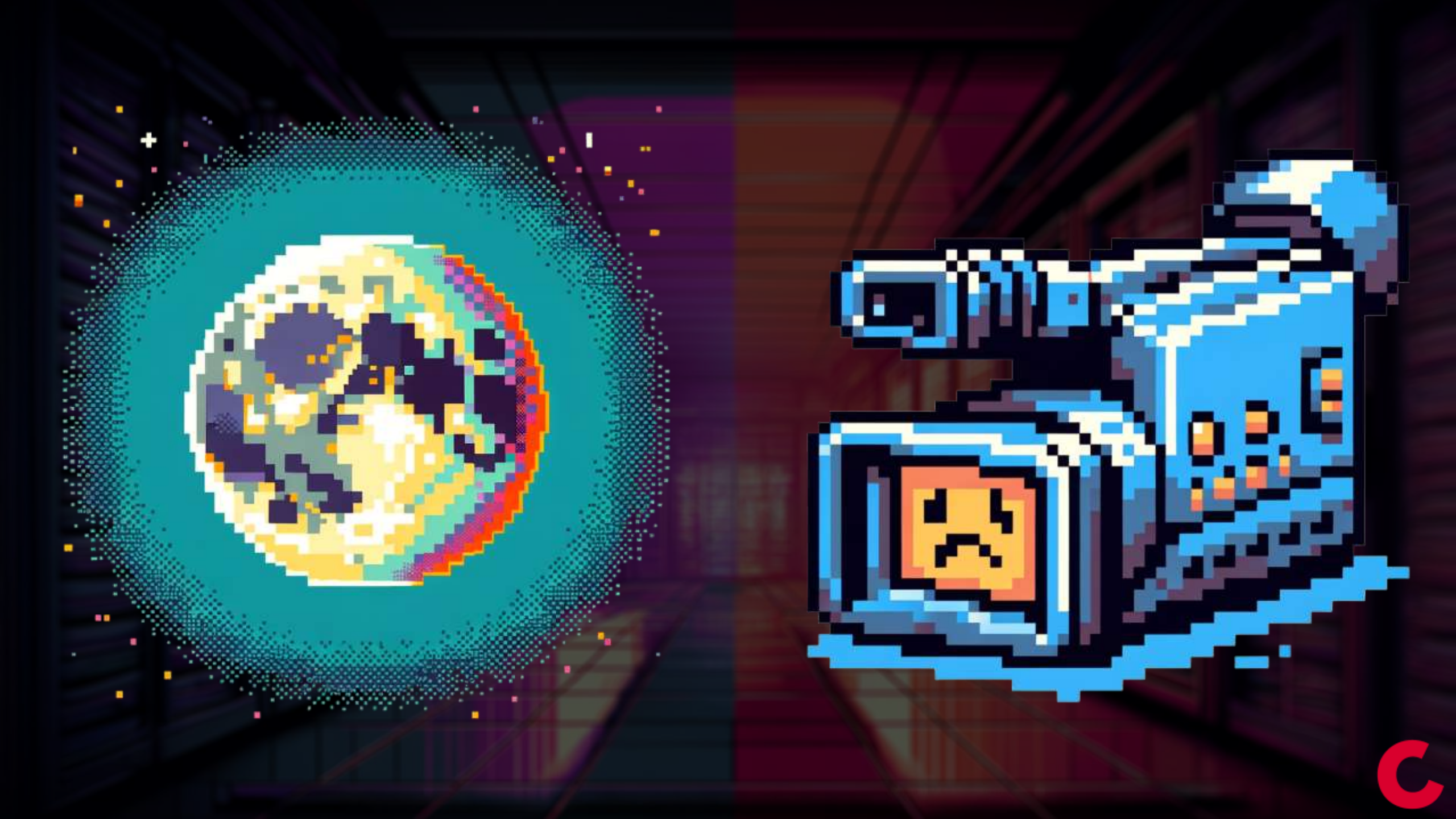


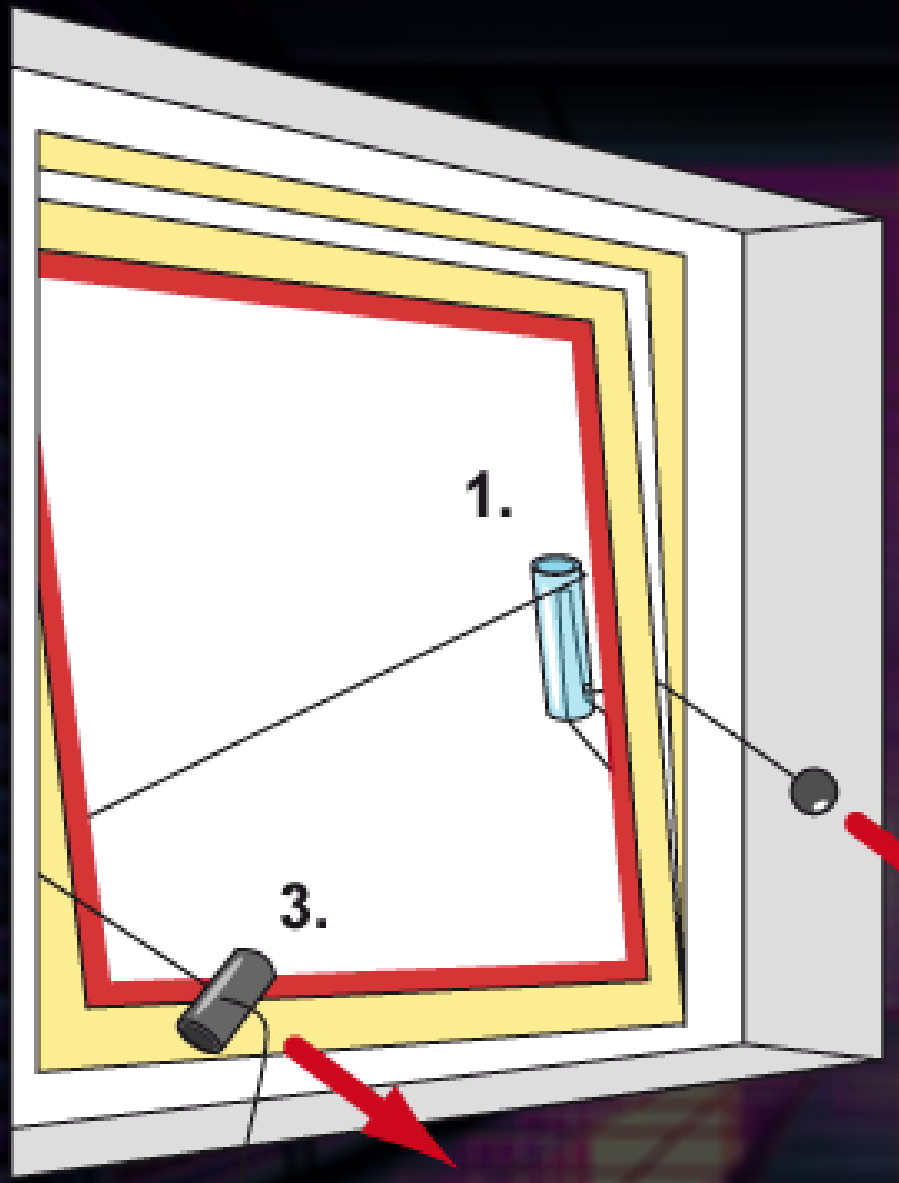
Basis Bild: https://xkcd.com/2347/

Basis Bild: https://xkcd.com/2347/


Nicht berühren

Physical Presence: Night

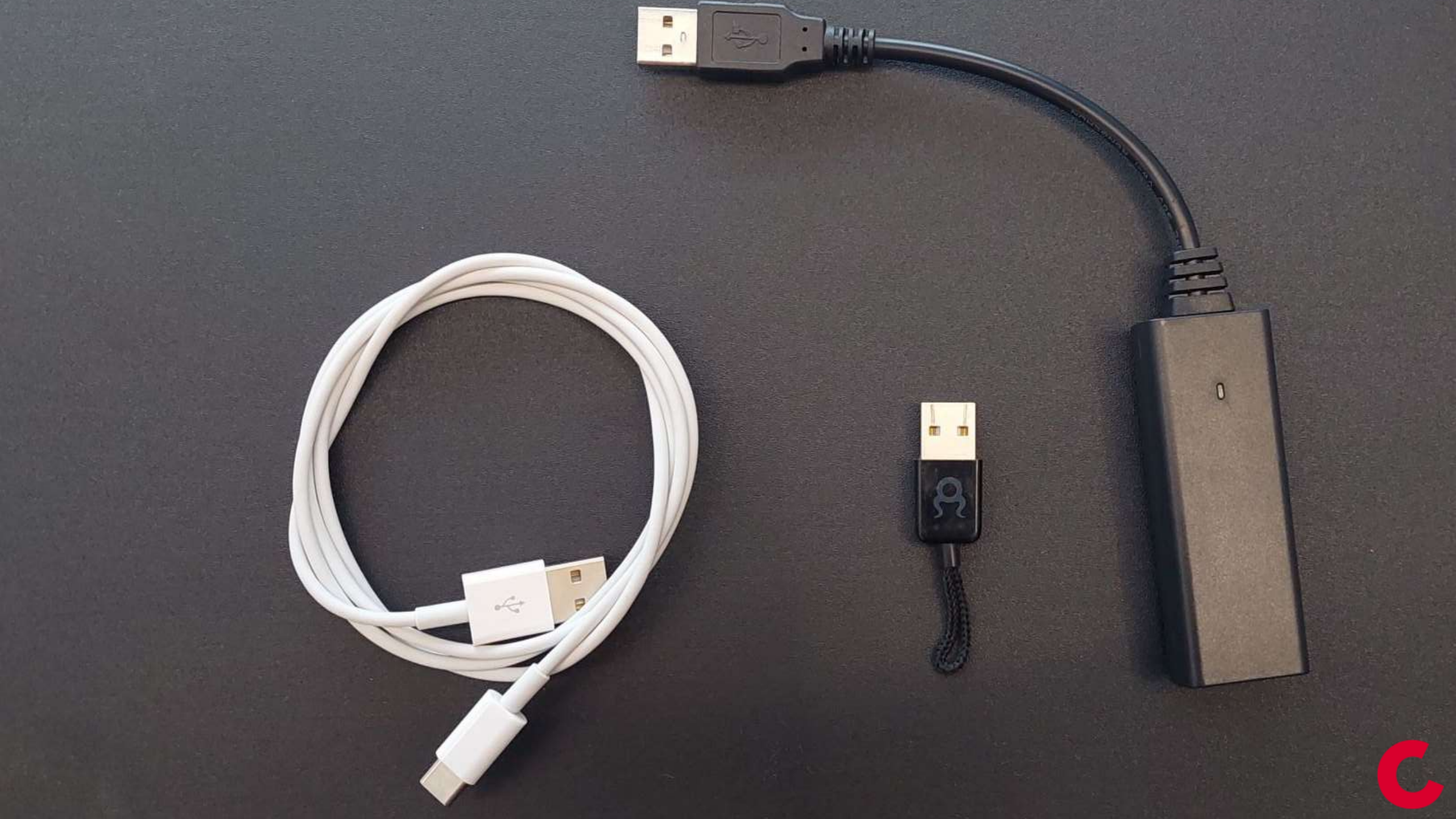




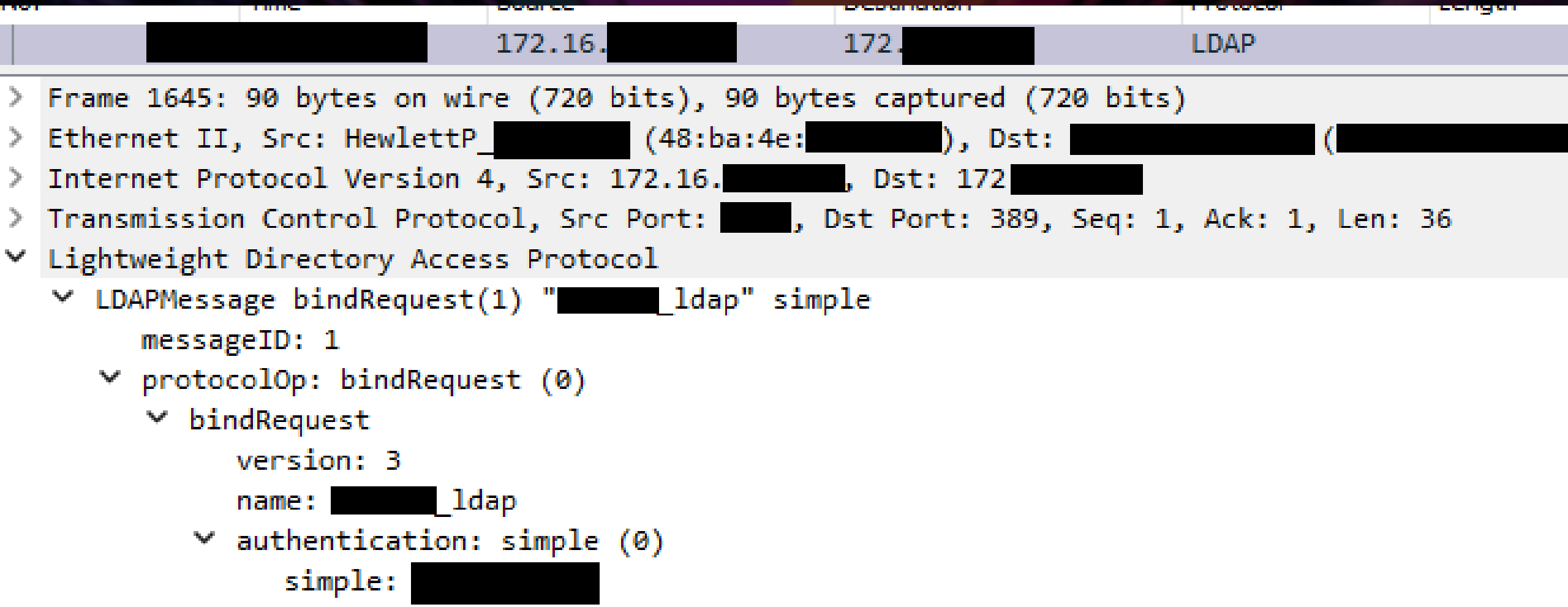
https://shop.multipick.com/media/images/popup/image_33967_5.png

Fix?

Bild: https://www.fenster-sofort.at

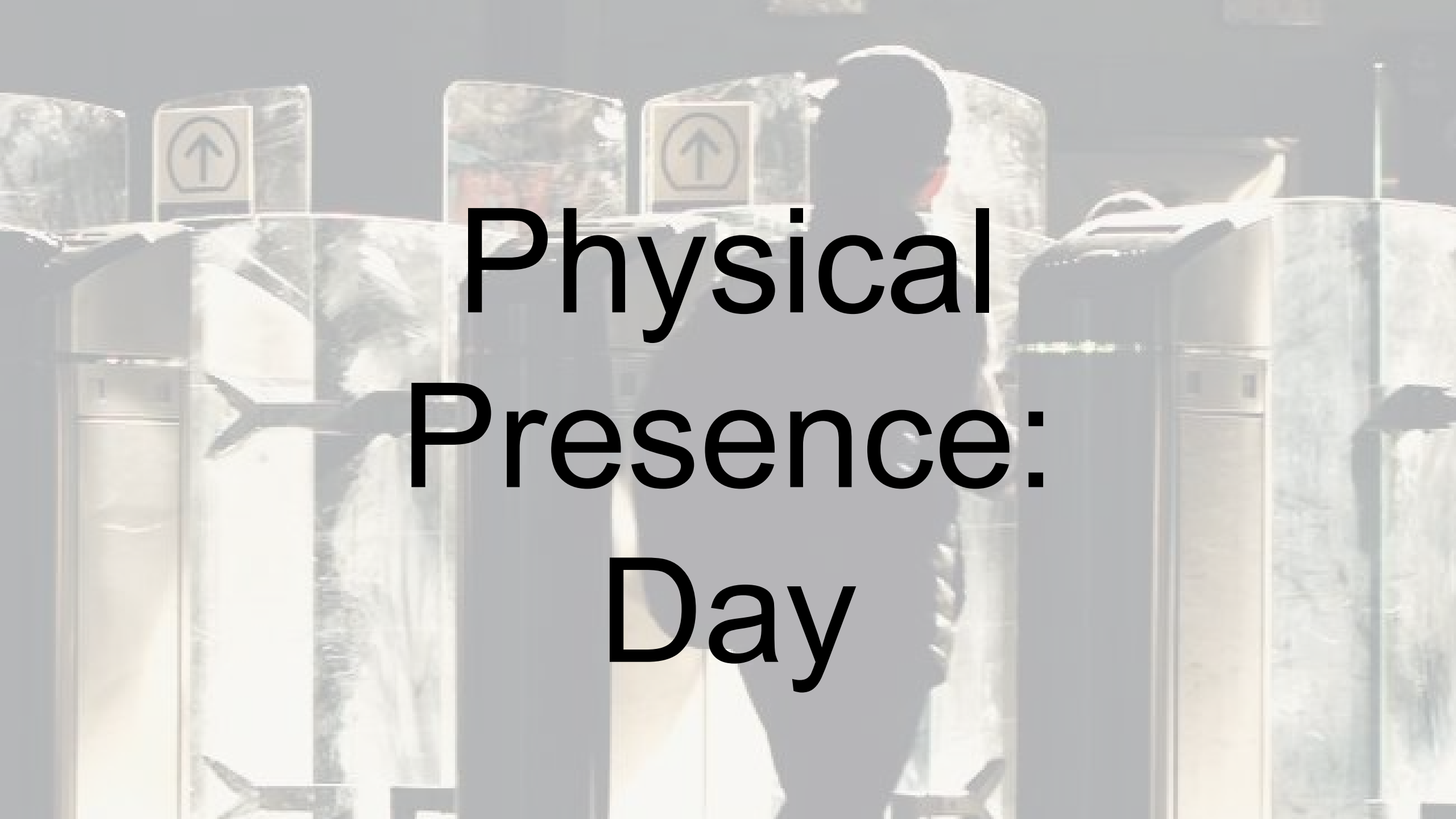


Drucker & LDAPS

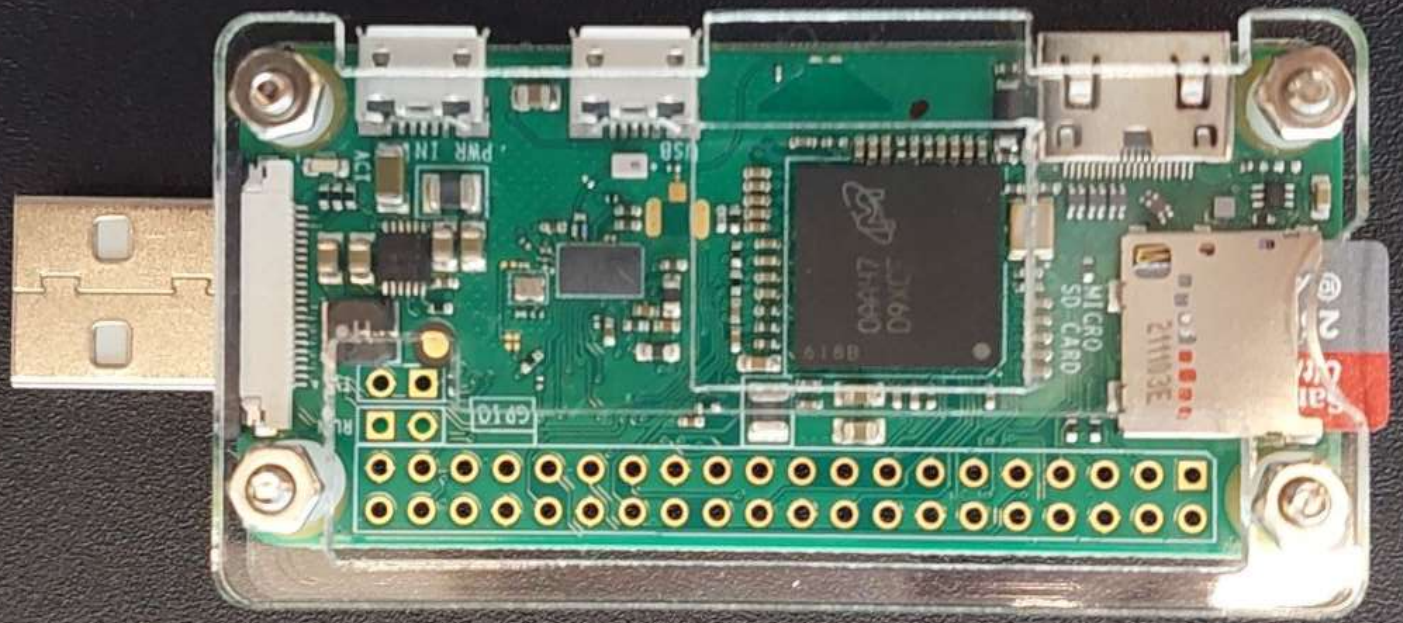


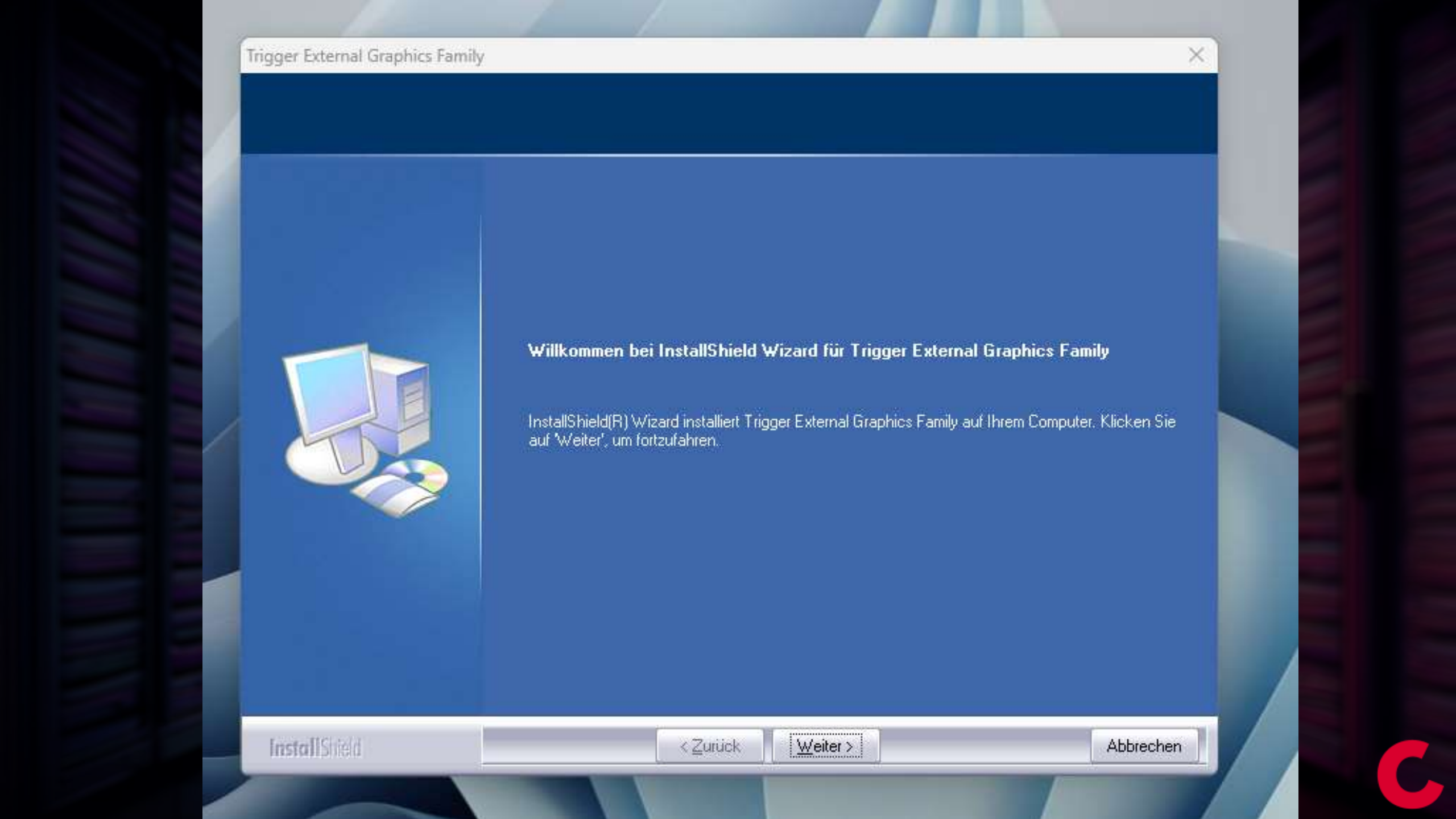
Integrators (krit.)
&
Standardpasswörter

```
name: [redacted]_ldap
authentication: simple (0)
    simple: [redacted]
```



Physical Presence: Day


PWR IN
ACT
USB
GP10
MICRO
SD CARD


Trigger External Graphics Family
Willkommen bei InstallShield Wizard für Trigger External Graphics Family
InstallShield(R) Wizard installiert Trigger External Graphics Family auf Ihrem Computer. Klicken Sie auf 'Weiter', um fortzufahren.
InstallShield
< Zurück
Weiter >
Abbrechen

Fixes?

- Physical Security?
- Üben, üben, üben!11!
- Greifbare Notfallinfos!
- Integrators: Pwds Reuse!
- CoInstaller deaktivieren

SCCM Site System Takeover

System Center Configuration Manager

Server

System Center Configuration Manager

Server

Client

System Center Configuration Manager

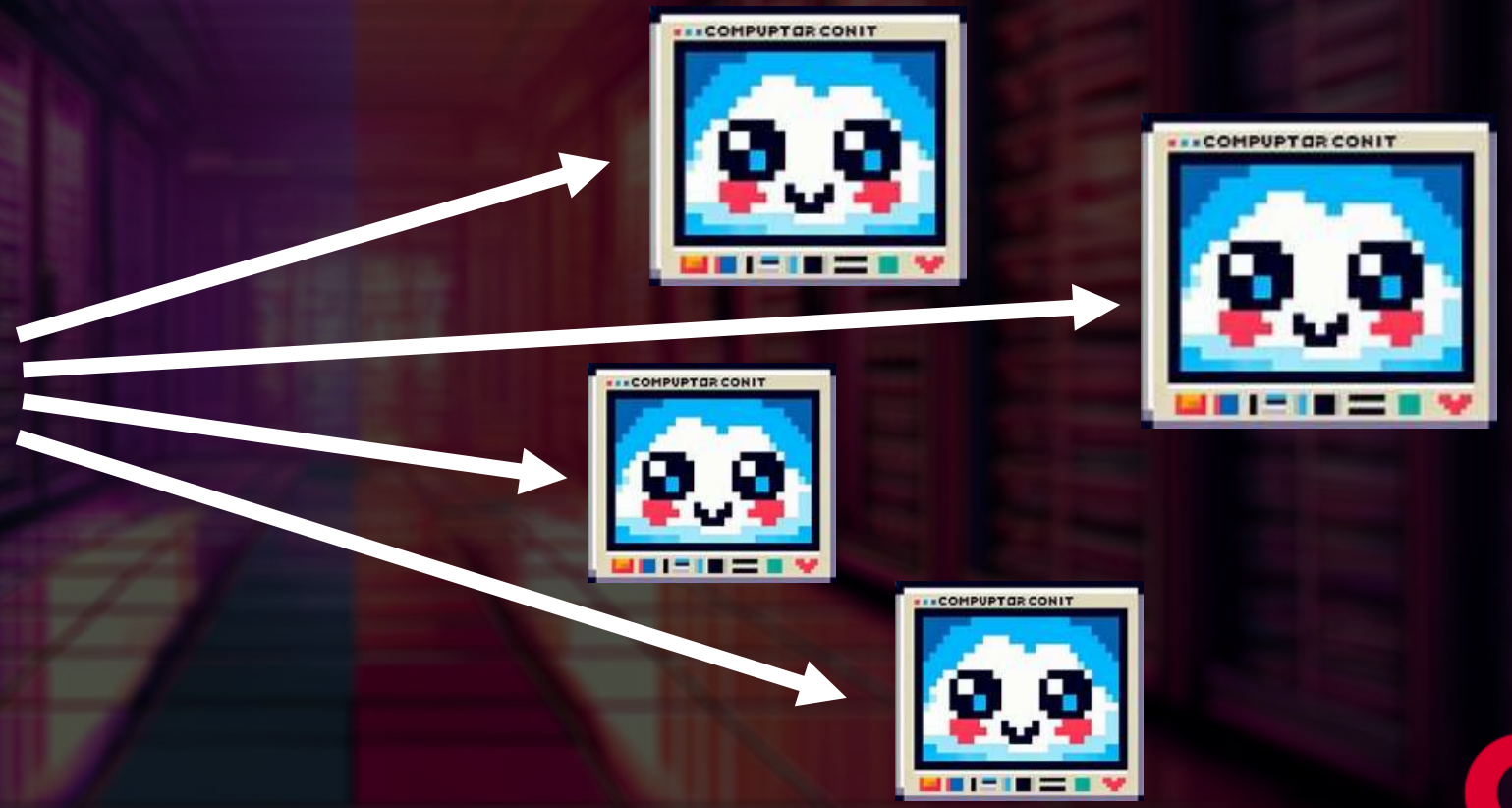
Server

Client

System C2 Manager

Server

Client



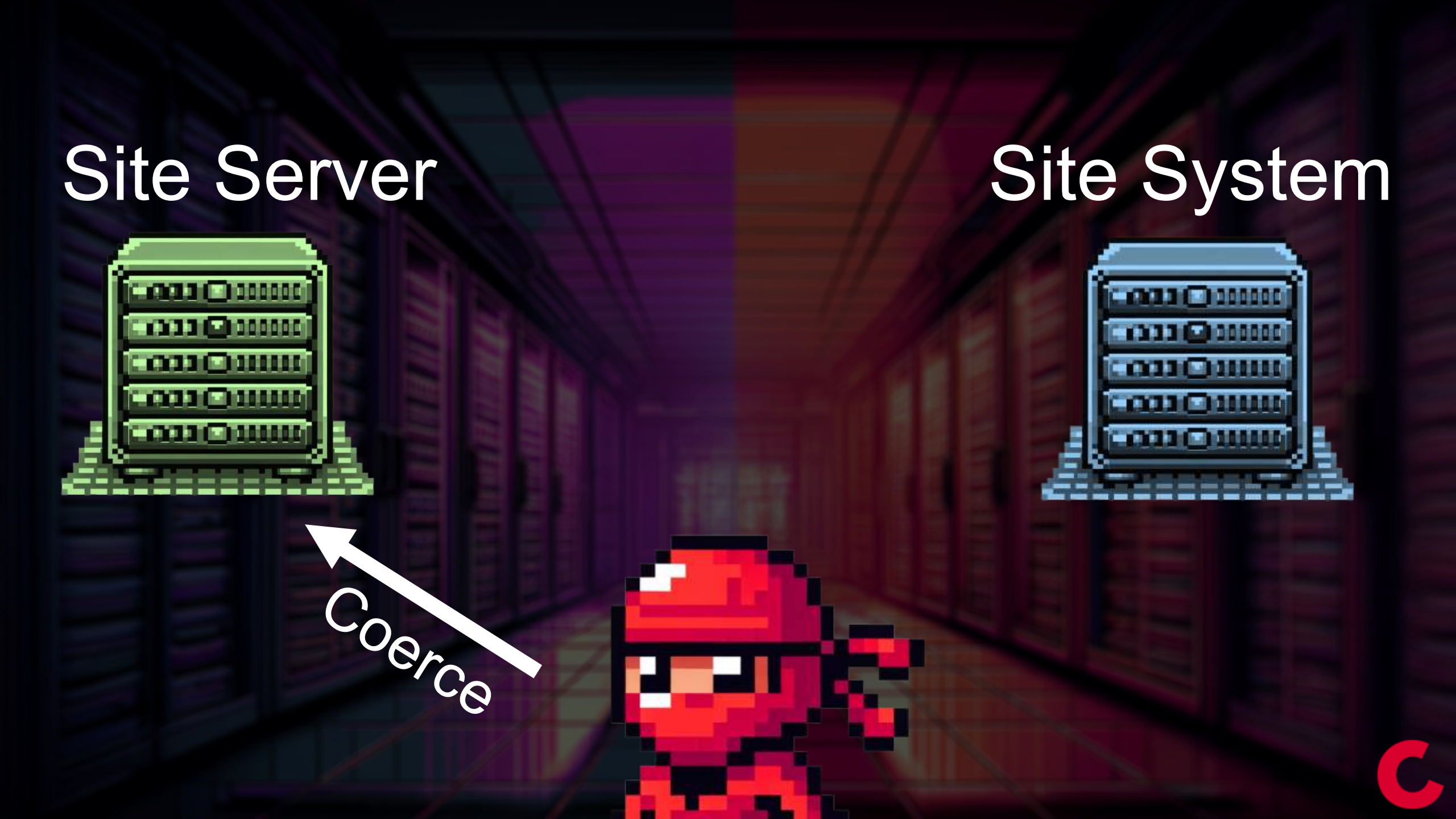
Site Server

Site System

Site Server

Admin

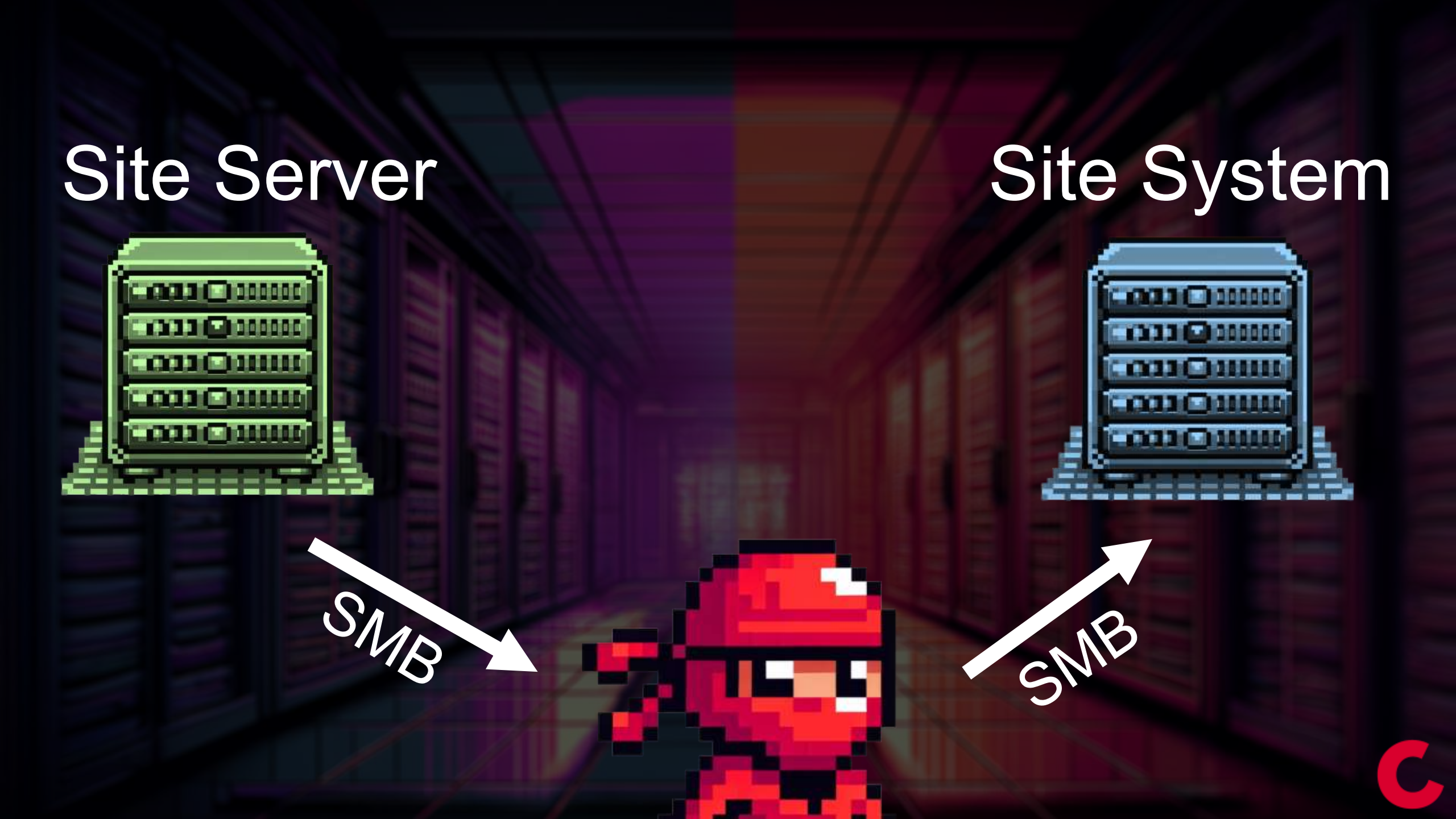
Site System


Site Server
Site System
Coerce

Site Server

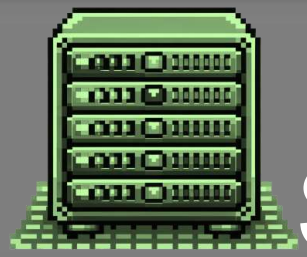
Site System

SMB


Site Server
Site System
SMB
SMB

```
ntlmrelayx> socks
Protocol  Target                                  Username                                AdminStatus
--------  ------------------------------------  --------------------------------------  -----------
SMB                                                                                     TRUE
SMB                                                                                     TRUE
SMB                                                                                     TRUE
SMB                                                                                     TRUE
```

Site System



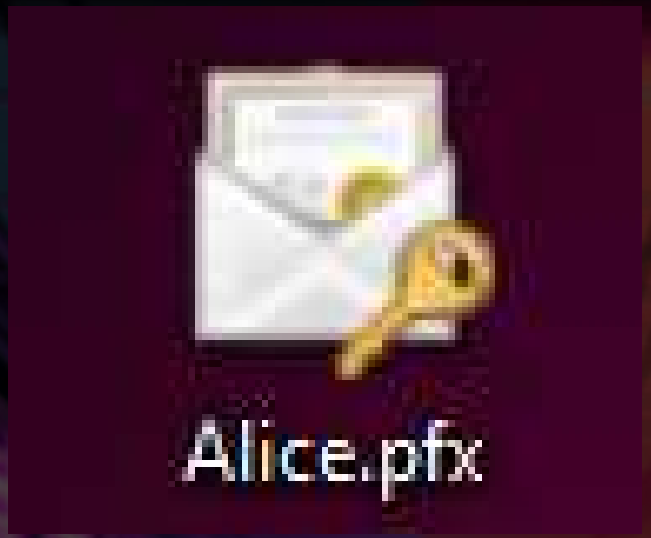
Site Server

Fixes?

- Netzwerk Segmentierung
- SMB Signing
- Monitoring

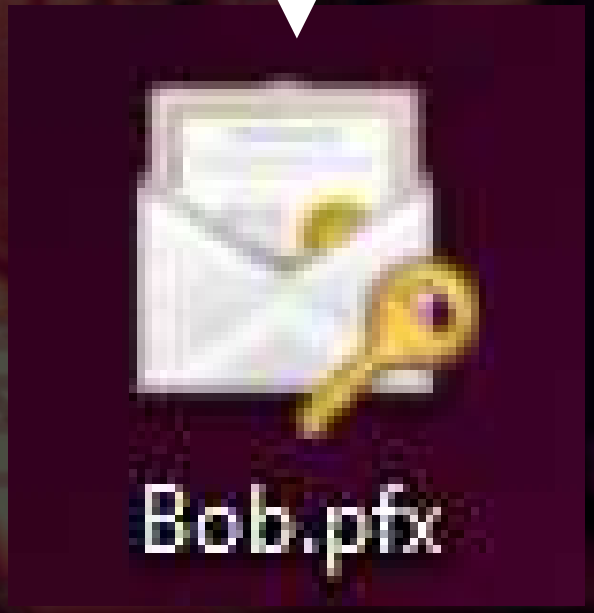
Zertifikatsstellen: ESC 1

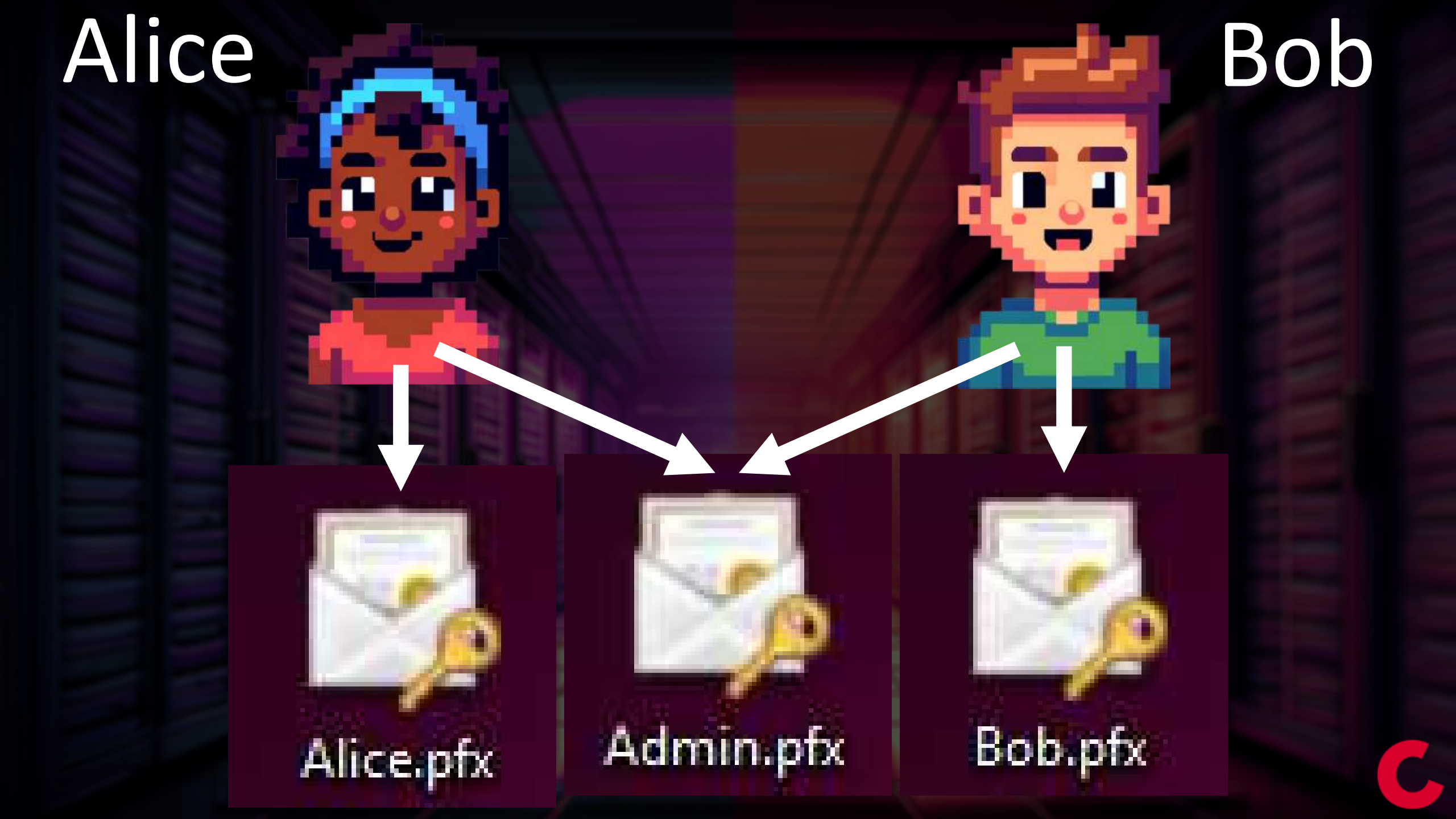
Alice



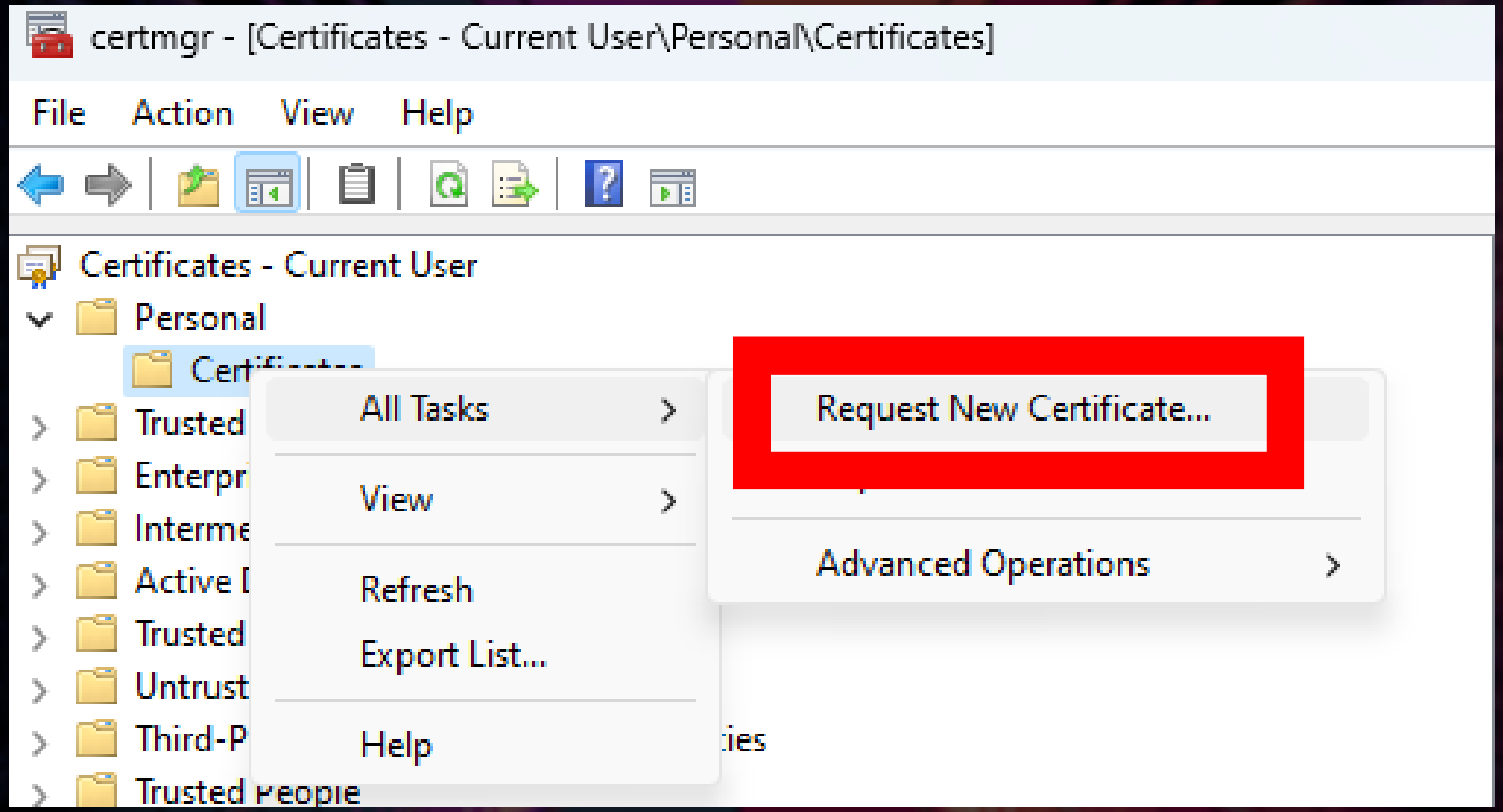
Alice

Bob




Alice
Bob
Alice.pfx
Admin.pfx
Bob.pfx

Als Alice:


certmgr - [Certificates - Current User\Personal\Certificates]
File
Action
View
Help
Certificates - Current User
Personal
Trusted
Enterpr
Interme
Active
Trusted
Untrust
Third-P
Trusted People
All Tasks
View
Refresh
Export List...
Help
Request New Certificate...
Advanced Operations

Als Alice:


Antragstellername:
Typ:
Allgemeiner Name
Wert:
Hinzufügen >
< Entfernen
CN=Administrator
Alternativer Name:
Typ:
Benutzerprinzipalname
Wert:
Hinzufügen >
Benutzerprinzipalname
administrator@

Als Alice:

```
[*] Using principal: administrator@
[*] Trying to get TGT ...
[*] Got TGT
[*] Saved credential cache to 'administrator.ccache'
[*] Trying to retrieve NT hash for 'administrator'
[*] Got NT hash for 'administrator@                '
```

Fixes?

- Konfiguration anpassen
- Client Authentication
- Enroll Rechte einschränken

- ESC n

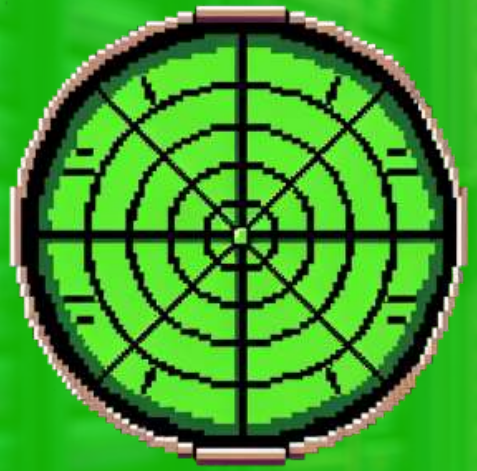
Basis Bild: https://xkcd.com/2347/


Learnings

AKTUELL?

Ziel

Periodische Tätigkeiten



Your friendly Hackers