CYBERTELL / CHECKLIST FOR GETTING STARTED WITH CYBERTELL

Checklist for getting started with CyberTell

What your company prepares before setup. With this information at hand, setup is done in a single session.

Step by step · 8 steps

01 Choose a contact person and the first admin

One person who manages CyberTell for the company: first name, last name and a personal business email address. Sign-in uses an email link and a passkey; there are no passwords.

02 Set up a security@ mailbox

Create a mailbox or forward for **security@your-domain.com** that reliably receives email and is read regularly. CyberTell sends the confirmation for your domain there. The address also serves as the contact point for security incidents.

> ! Without a working security@ mailbox the domain cannot be confirmed.

03 Prepare the domain and DMARC

Decide on the company's main domain and make sure you have access to its DNS management. For DMARC reporting, add a TXT record on **_dmarc.your-domain.com** with CyberTell as the report recipient:

```
v=DMARC1; p=none; rua=mailto:dmarc@cybertell.io
```

04 Mail sending for phishing simulations

Simulated phishing emails are sent through your own mail server. Have ready: SMTP host, port (usually 587), user, password, sender address and sender name. SPF and DMARC must be set for the sender domain; DKIM is recommended.

05 Allow simulations in the mail filter

So that test emails arrive, allow your own SMTP server and the sender domain in the mail filter: in Microsoft 365 via "Advanced delivery" (phishing simulation), in Google Workspace via an allowlist. Optionally use your own tracking domain: TXT record **_cybertell-verify.your-domain.com** plus a CNAME to the target shown in the portal. Allow this domain as well.

06 Employee list as CSV

All employees with first name, last name and business email address, optionally language (de, en, fr, it). Format: semicolon-separated, UTF-8, max. 2 MB. Every email address must be unique.

```
firstname;lastname;email;language
Max;Muster;max.muster@example.ch;de
```

07 Company profile and IT environment

Logo, website and a short description of the company. For the initial risk assessment, note: systems in use (Windows, Active Directory, Microsoft 365, macOS, Linux), firewall and endpoint protection, key suppliers and where personal data is processed.

08 Optional: integrations

For the SOC connection: firewall credentials (Sophos, Firewalla, pfSense) or an app registration in Microsoft Entra ID for Defender. Plus a Slack webhook for alerts and a plan for rolling out the CyberTell app to employee devices.

Ready to start when …

- [ ] the first admin is set and their email address works
- [ ] security@your-domain.com receives email
- [ ] access to DNS management is sorted
- [ ] the SMTP credentials for simulations are at hand
- [ ] the employee list is ready as CSV