

# Testen Sie Ihre E-Mail Security

## 13. & 22. Mai 2025



xorlab

### E-Mail-Sicherheit im Zeitalter von KI

Erkenntnisse aus über 20 realitätsnahen Angriffssimulationen

Webinar / 13.5.2025 / [adrian.kyburz@xorlab.com](mailto:adrian.kyburz@xorlab.com)



Mentimeter

### Webinar Live Polling

Join at [Menti.com](https://menti.com) | use code 8450 2453  
Or use QR Code ->

2 xorlab | Secure email your way

13 May 2025

# Testen Sie Ihre E-Mail Security

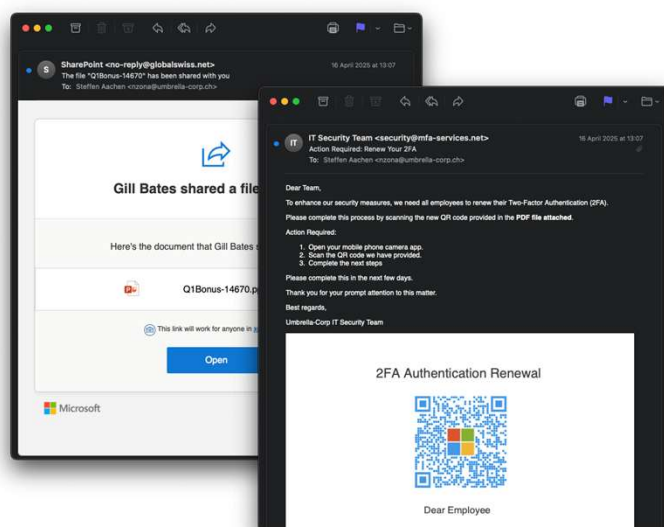
## 13. & 22. Mai 2025

### Menti-Umfrage

- Wie viele gefährliche E-Mails landen trotz Schutzmassnahmen in den Posteingängen eurer Mitarbeiter?
- Welche Branche, welche Grösse?



### Jeder zweite Angriff landet im Posteingang



#### Angriffstypen und -techniken

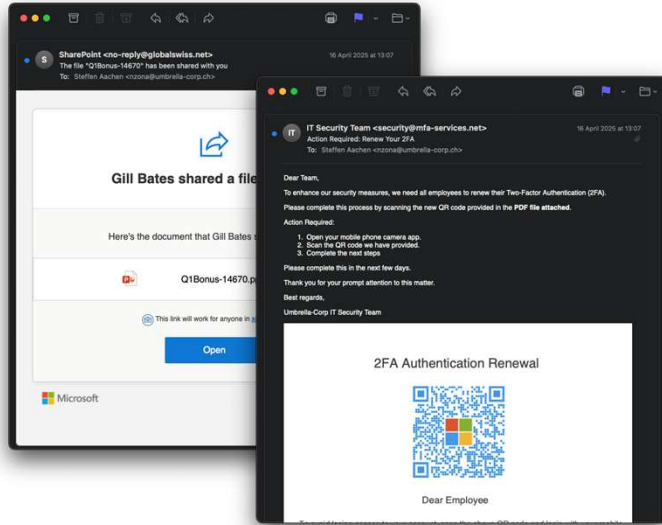
- Phishing
  - Mit Link
  - Via Service
- Business Email Compromise
  - Mit Anhang
  - QR-Rechnung
  - Email Thread Hijacking
  - Etc.
- Malware
  - Mit Anhang, archiviert, verschlüsselt
- Krypto-Erpressung



# Testen Sie Ihre E-Mail Security

## 13. & 22. Mai 2025

### Jeder zweite Angriff landet im Posteingang



#### Getestete Angriffstypen

Phishing

BEC: Business Email Compromise

Malware/Ransomware

Krypto-Erpressung

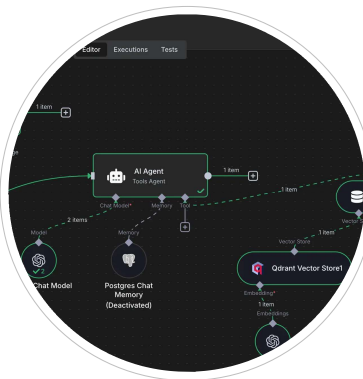


### KI, Automatisierung und Cybercrime-as-a-Service verändern die Spielregeln

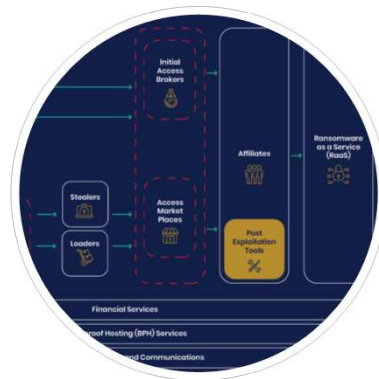
#### Generative AI



#### Automation



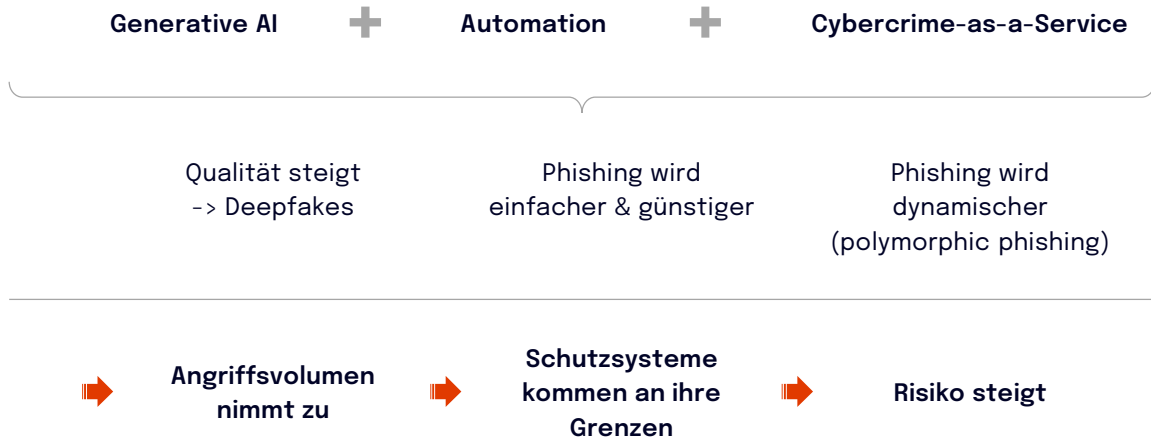
#### Cybercrime-as-a-Service



# Testen Sie Ihre E-Mail Security

## 13. & 22. Mai 2025

### KI, Automatisierung und Cybercrime-as-a-Service verändern die Spielregeln

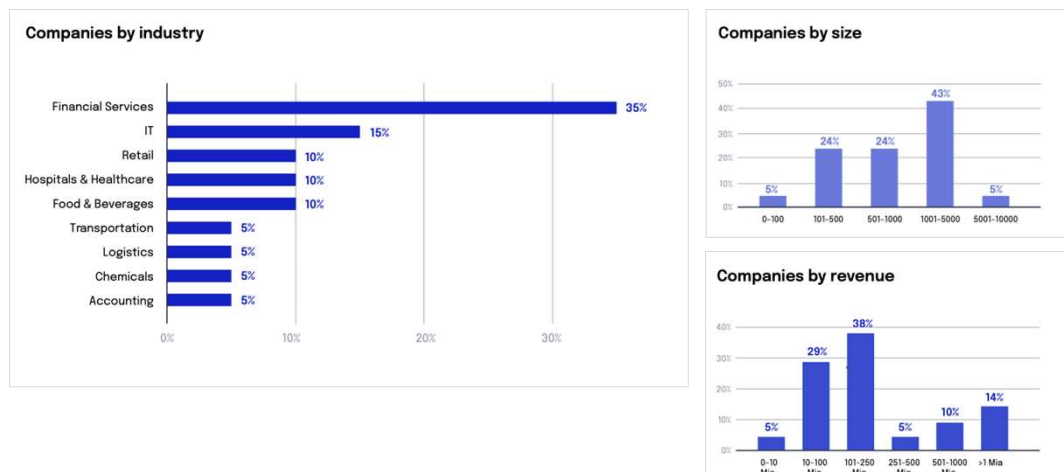


7 xorlab | Secure email your way

13 May 2025



### Wir haben die E-Mail-Security von 20 Firmen aus 9 Branchen getestet



8 xorlab | Secure email your way

13 May 2025



# Testen Sie Ihre E-Mail Security

## 13. & 22. Mai 2025

### Getestete E-Mail Security Systeme

|                                              | Verbreitung in % | Zugestellte Angriffe in % |
|----------------------------------------------|------------------|---------------------------|
| Secure E-Mail Gateway (SEG)                  | 29%              |                           |
| Cloud Email Provider Built-In Security (CEP) | 43%              |                           |
| CEP & Integrated Cloud Email Security        | 14%              |                           |
| SEG > CEP                                    | 14%              |                           |



### Webinar Live Polling

Join at Menti.com | use code 8450 2453

Or use QR Code ->



# Testen Sie Ihre E-Mail Security

## 13. & 22. Mai 2025

### Menti-Umfrage

- Welches Setup nutzt ihr? SEG, CEP, CEP + ICES, SEG + CEP (explain the terms, make explicit use Microsoft)
- Welches Setup bietet den höchsten Schutz – SEG, SEG + M365, MDO, MDO + ICES?



### Getestete E-Mail Security Systeme

|                                              | Verbreitung in % | Zugestellte Angriffe in % |
|----------------------------------------------|------------------|---------------------------|
| Secure E-Mail Gateway (SEG)                  | 29%              | 57%                       |
| Cloud Email Provider Built-In Security (CEP) | 43%              | 47%                       |
| CEP & Integrated Cloud Email Security        | 14%              | 41%                       |
| SEG > CEP                                    | 14%              | 76%                       |



# Testen Sie Ihre E-Mail Security

## 13. & 22. Mai 2025

Wenn 53% der Angriffe  
in der Inbox landen...

ETH zürich



32% der Teilnehmer haben  
mindestens einmal geklickt



25% der Teilnehmer haben mindestens  
eine gefährliche Aktion ausgeführt

13 xorlab | Context matters

Phishing in Organizations: Findings from a Large-Scale and Long-Term Study | ETH Zürich | Dec. 2021

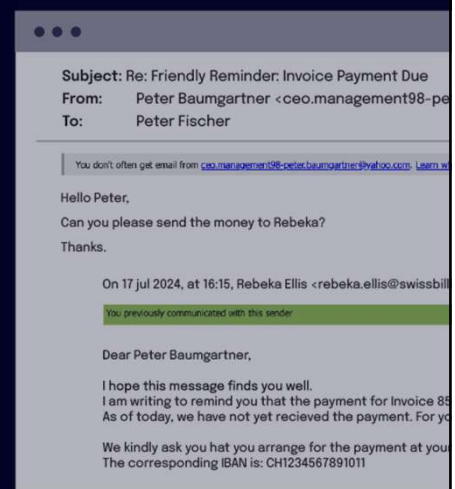
6/27/24



## Welche Angriffstypen funktionieren besonders gut?

Angriffe in der Inbox

|                           |     |
|---------------------------|-----|
| Business Email Compromise | 68% |
| Malware/Ransomware        | 53% |
| Phishing                  | 52% |
| Krypto-Erpressung         | 37% |



14 xorlab | Secure email your way

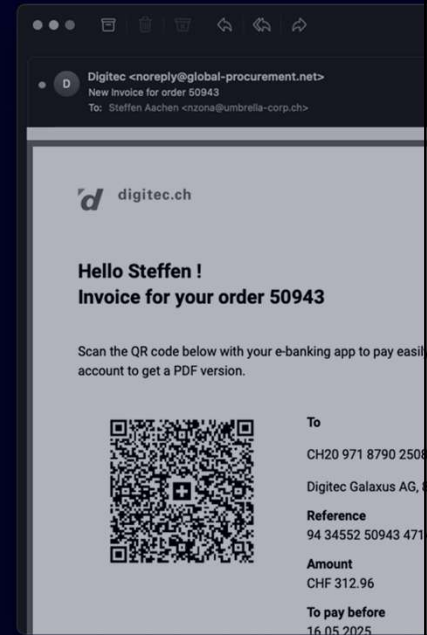
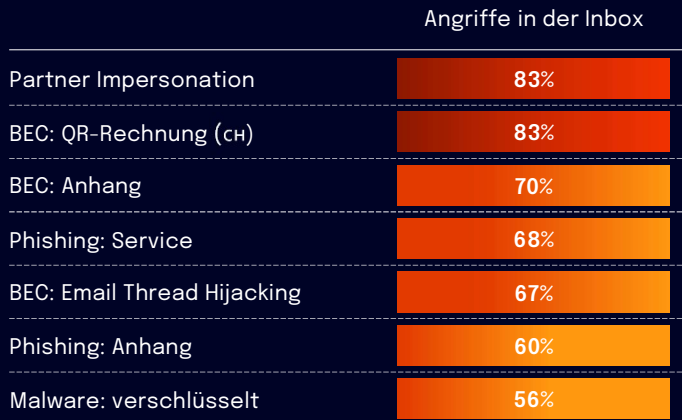
13 May 2025



# Testen Sie Ihre E-Mail Security

## 13. & 22. Mai 2025

### Welche Angriffstechniken funktionieren besonders gut?



### 60+ Getestete Angriffstypen und -techniken

|         |                |                  |               |              |
|---------|----------------|------------------|---------------|--------------|
| Typ     | Phishing       | BEC              | Malware       | Krypto-Erpr. |
| Subtyp  | Cred. Phishing | VIP Fraud        | Ransomware    | Sextortion   |
|         |                | Invoice Fraud    |               |              |
|         |                | Payroll Fraud    |               |              |
| Technik | Link           | Text             | Anhang        |              |
|         | HTML/SVG       | Rechnung         | Archiv        |              |
|         | Anhang         | Thread Hijacking | Verschlüsselt |              |
|         | Via Service    |                  |               |              |



# Testen Sie Ihre E-Mail Security

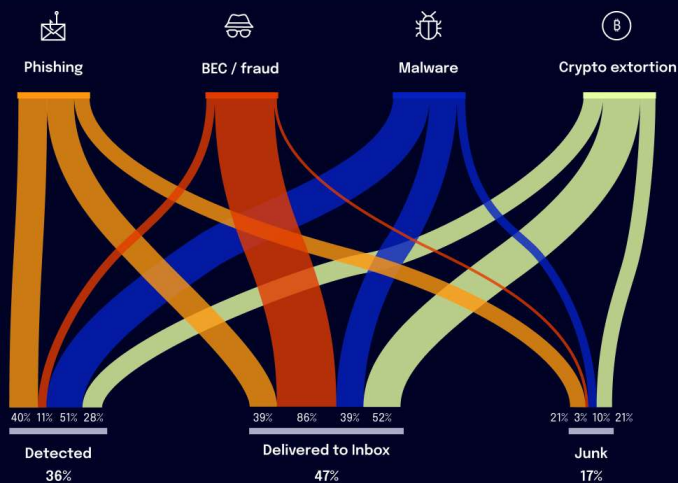
## 13. & 22. Mai 2025

### Zentrale Ergebnisse

- 1 53% der Angriffe landen in der Inbox.
- 2 Problemfall Business Email Compromise: 68 % der BEC-Angriffe werden nicht erkannt.
- 3 Zusammen mit einem Cloud Email Provider, z.B. Microsoft 365, können Secure Email Gateways (SEG) mehr schaden als nützen.
- 4 Aber auch der integrierte Security Filter von Microsoft weist Lücken auf.



### Wie gut schützt Microsoft 365?



4 von 10 getesteten Firmen setzen nur auf Defender for O365 und/oder EOP.

Mit Defender for O365 landen immer noch 47% der Angriffe in der Inbox.

Von allen Angriffstypen war BEC der effektivste. 86% der Angriffe kamen durch.



# Testen Sie Ihre E-Mail Security

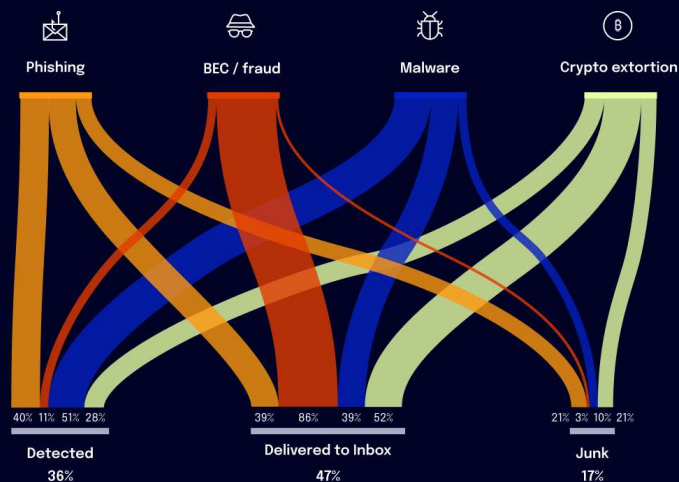
## 13. & 22. Mai 2025

### Wie gut schützt Microsoft 365?

4 von 10 getesteten Firmen setzen nur auf Defender for O365 und/oder EOP.

Mit Defender for O365 landen immer noch 47% der Angriffe in der Inbox.

Von allen Angriffstypen war BEC der effektivste. 86% der Angriffe kamen durch.



### Warum scheitern klassische Schutzsysteme?



Viele Hersteller haben sich darauf spezialisiert, Signaturen, IOA/IOCs etc. zu erkennen.



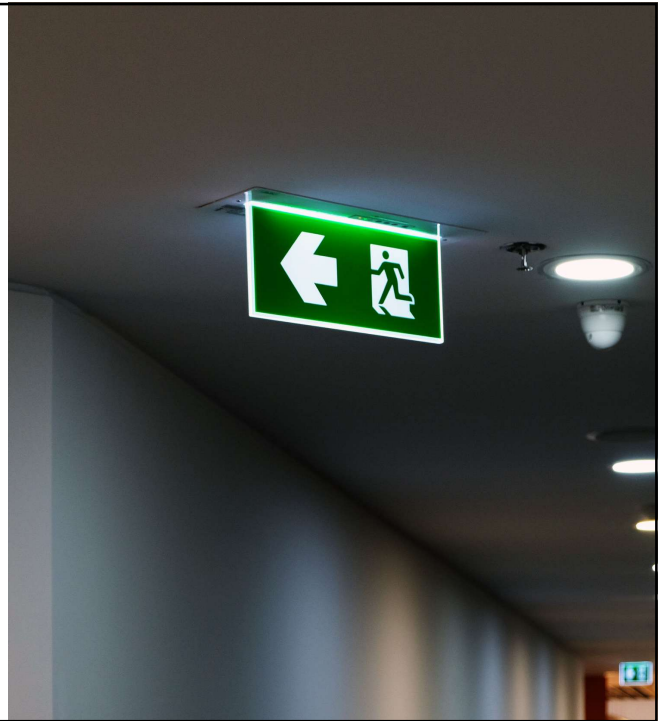
# Testen Sie Ihre E-Mail Security

## 13. & 22. Mai 2025

### Handlungs- empfehlungen

1. Regelmässige Angriffssimulationen
2. BEC-Drills
3. Ergebnisse für Policy-Updates nutzen
4. Microsoft 365 zusätzlich absichern
5. SEG-Konfigurationsaudit

21 xorlab | Secure email your way



 Mentimeter

### Webinar Live Polling

Join at Menti.com | use code 8450 2453

Or use QR Code ->



22 xorlab | Secure email your way

13 May 2025



# Testen Sie Ihre E-Mail Security

## 13. & 22. Mai 2025

### Menti-Umfrage

- Plant Ihr Unternehmen, in den nächsten 6 Monaten in die Email Security zu investieren?



### Fazit und Ausblick

- 1 Klassische E-Mail-Sicherheitslösungen sind überfordert.
- 2 Eine realistisch geführte «Attack Simulation» bringt Klarheit.
- 3 Jetzt ist ein guter Zeitpunkt, um auf proaktive E-Mail-Sicherheit umzustellen.

#### Attack Simulation anfordern



<https://www.avantec.ch/webcast-testen-sie-ihre-e-mail-security/#simulation>

#### Analysebericht lesen



<https://www.xorlab.com/de/email-attack-simulation-insights>



# Testen Sie Ihre E-Mail Security

## 13. & 22. Mai 2025

### About xorlab

xorlab is an email security platform for security analysts and detection engineers. It simplifies building and managing detection rules so you can respond to new threats faster.

|                                                                                   |                                                                                   |                                                                                   |                                                                                                           |                                                                                                                |                                                                                               |
|-----------------------------------------------------------------------------------|-----------------------------------------------------------------------------------|-----------------------------------------------------------------------------------|-----------------------------------------------------------------------------------------------------------|----------------------------------------------------------------------------------------------------------------|-----------------------------------------------------------------------------------------------|
|  |  | Julius Bär                                                                        |  swisscom                |  Implenia                   | Hoval                                                                                         |
| Vontobel                                                                          | HAUFE Group                                                                       |  |  solothurner spitäler ag |                             |  Netcetera |
|  |  |  |                          |  Universitäts Spital Zürich |            |

25 xorlab | Secure email your way 13 May 2025

### Warum scheitern klassische Schutzsysteme?

Cyber Security Pyramid of Pain

|                        |             |
|------------------------|-------------|
| TTPs                   | Thought!    |
| Tools                  | Challenging |
| Network/host artefacts | Annoying    |
| Domain names           | Simple      |
| IP addresses           | Easy        |
| Hash values            | Trivial     |

Viele Hersteller haben sich darauf spezialisiert, Signaturen, IOA/IOCs etc. zu erkennen.

26 xorlab | Secure email your way 13 May 2025

## Slide 25

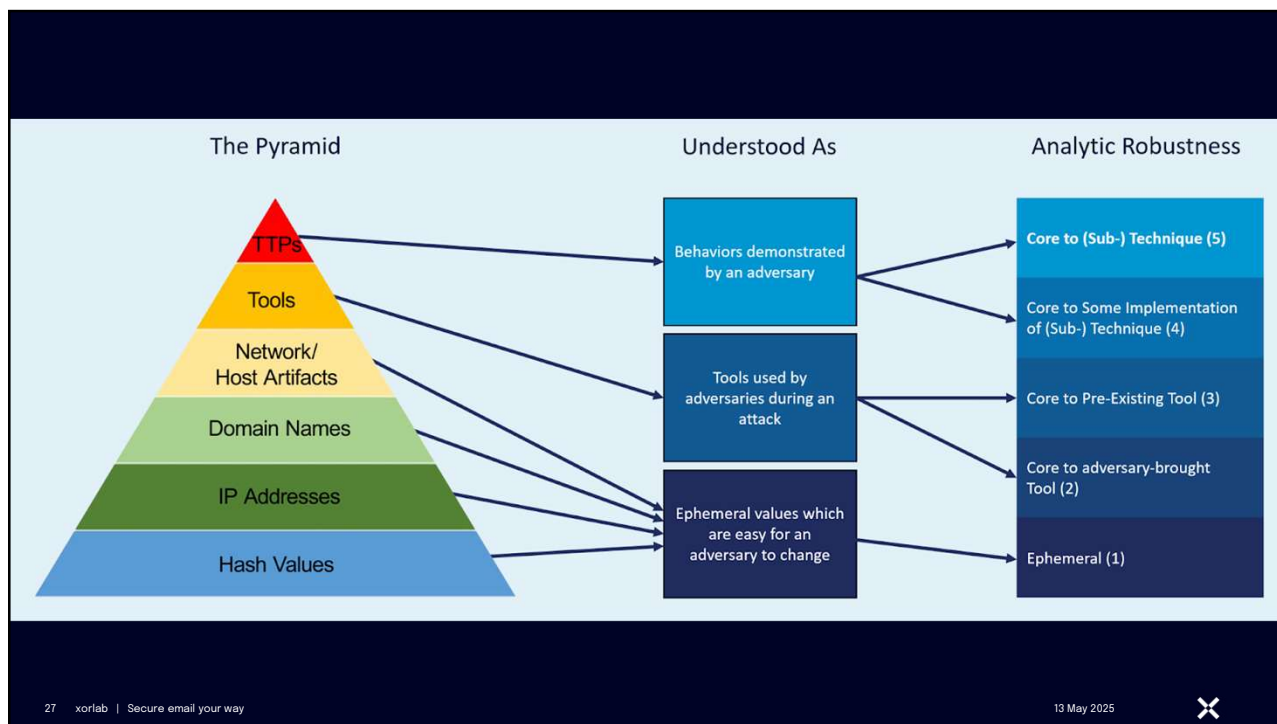
---

- 0 This one first two rows match the website logo block, last row I left 3 that was additionally there we didn't pick for the website ( Sturm gruppe, Leonteq)

Nikolett Grozdics; 2025-05-12T09:14:58.155

# Testen Sie Ihre E-Mail Security

## 13. & 22. Mai 2025



# Testen Sie Ihre E-Mail Security

## 13. & 22. Mai 2025

**About xorlab**

xorlab is an email security platform for security analysts and detection engineers. It simplifies building and managing detection rules so you can respond to new threats faster.

|                                                                                           |                                                                                   |                                                                                              |                                                                                                                              |                                                                                                                                   |                                                                                     |
|-------------------------------------------------------------------------------------------|-----------------------------------------------------------------------------------|----------------------------------------------------------------------------------------------|------------------------------------------------------------------------------------------------------------------------------|-----------------------------------------------------------------------------------------------------------------------------------|-------------------------------------------------------------------------------------|
|          |  | Julius Bär                                                                                   |  swisscom                                   |  Implenia                                      |  |
| Vontobel                                                                                  | HAUFE Group                                                                       |             |  <small>solothurner<br/>spitäler ag</small> |                                                |  |
|  finnova | ALTOO                                                                             |  climeworks |                                             |  <small>Universitäts<br/>Spital Zürich</small> |  |

29 xorlab | Secure email your way

13 May 2025

- 0 This one matches the website logo block  
Nikolett Grozdics; 2025-05-12T09:13:27.298