xorlab

AVANITEC
Competence. Security. Trust.

E-Mail Security neu gedacht

CISO Roundtable | 29. Februar 2024

Adrian Kyburz, adrian.kyburz@xorlab.com

Agenda

#	Inhalt	Speaker	Dauer
1	Begrüssung und Einleitung	Mark Stäheli, AVANTEC	15 Min.
2	Aktuelle Bedrohungslage in der E-Mail Security	Adrian Kyburz, xorlab	15 Min.
3	Context matters: der Ansatz von xorlab	Antonio Barresi, xorlab	20 Min.
4	Mehr Kontrolle in der E-Mail Security – Erfahrungen nach 3 Jahren mit xorlab	Lukas Kellenberger, Bank Vontobel	15 Min.
5	Q&A und offene Diskussion, anschl. 20 Min. Pause		40 Min.
7	Third-Party Risk Management	Antonio Barresi, xorlab	15 Min.
8	Input: Threat Intelligence	Christian Grob, AVANTEC	15 Min.
9	Trends & Ausblick	Christine Hakenjos, xorlab	15 Min.
10	Weiterführender Austausch beim Stehlunch		Offen

xorlab

AVANITEC
Competence. Security. Trust.

1. Aktuelle Bedrohungslage in der E-Mail Security

E-Mail Security neu gedacht | CISO Roundtable

Adrian Kyburz, adrian.kyburz@xorlab.com

Who am I

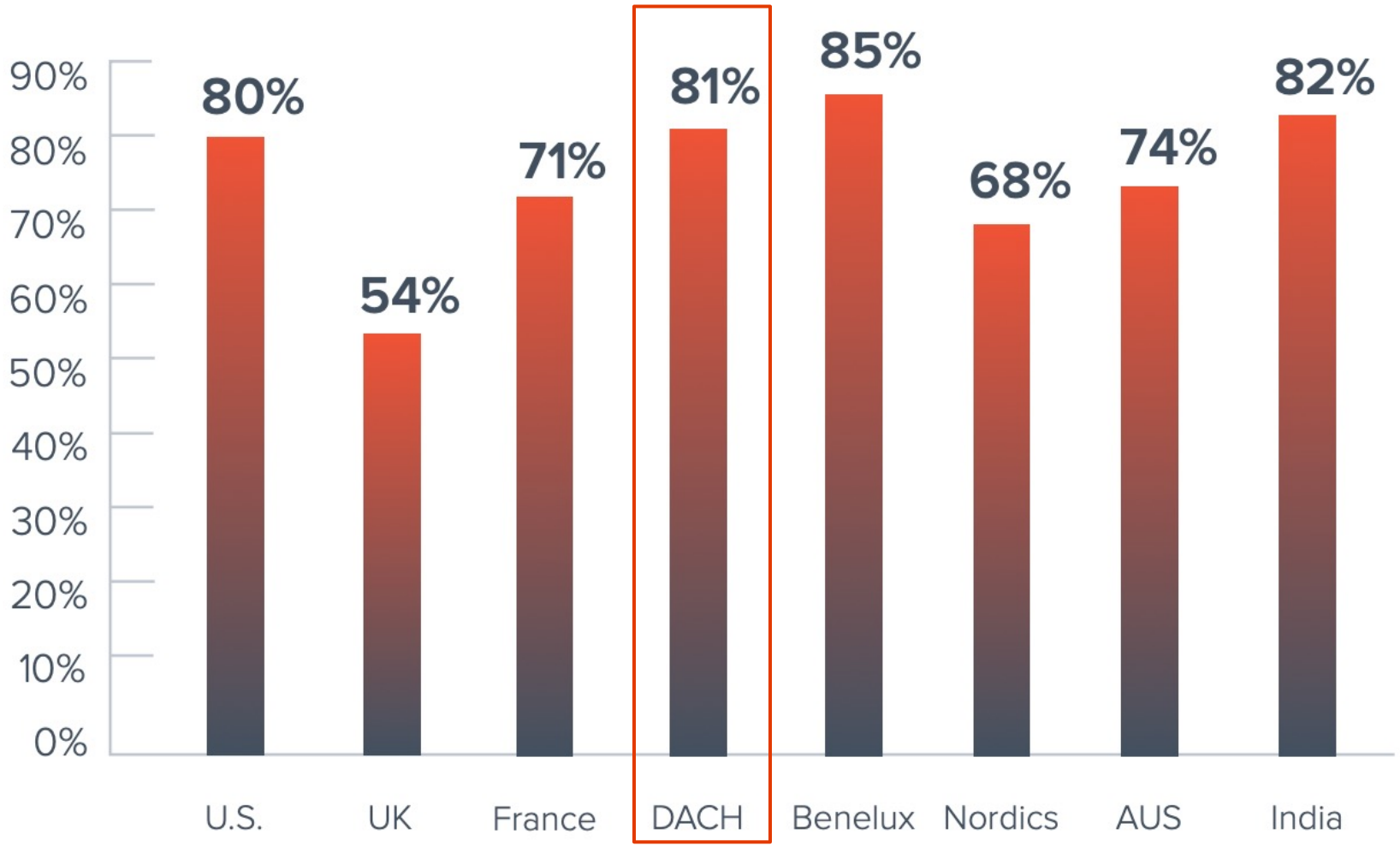
Adrian Kyburz

Head of Marketing

- Seit 6+ Jahren mit xorlab auf der Suche nach der bestmöglichen E-Mail Security für unsere Kunden
- Abgeschlossenes ETH-Informatikstudium mit Schwerpunkt Informationssicherheit
- Begeisterter Gleitschirmpilot

Has your organization faced any successful email-based security attacks in the past year?

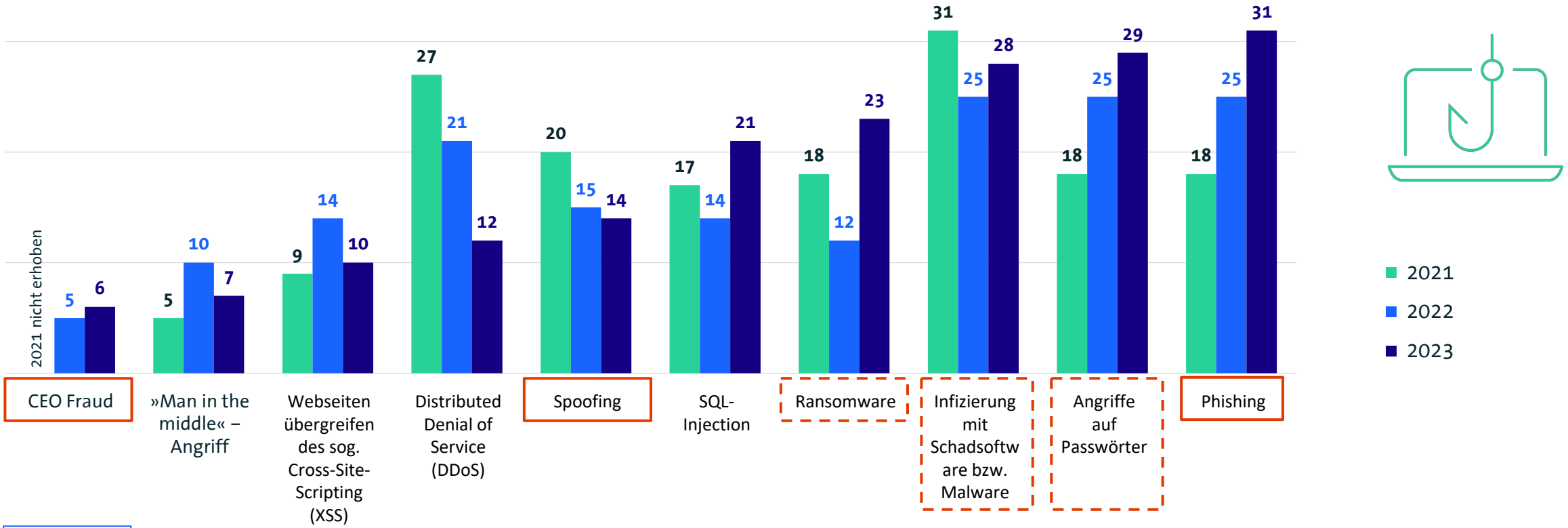
(n=1,350)



81% der befragten Unternehmen im deutschsprachigen Raum hatten 2022 einen Schaden, der auf einen E-Mail-Angriff zurückgeführt werden konnte.

Häufige Schäden durch Phishing, Passwortklau & Malware

Welche der folgenden Arten von Cyberangriffen haben innerhalb der letzten 12 Monaten in Ihrem Unternehmen einen Schaden verursacht?



in Prozent

Basis: Alle Unternehmen (n=1.002) | Mehrfachnennungen möglich | Quelle: Bitkom Research 2023

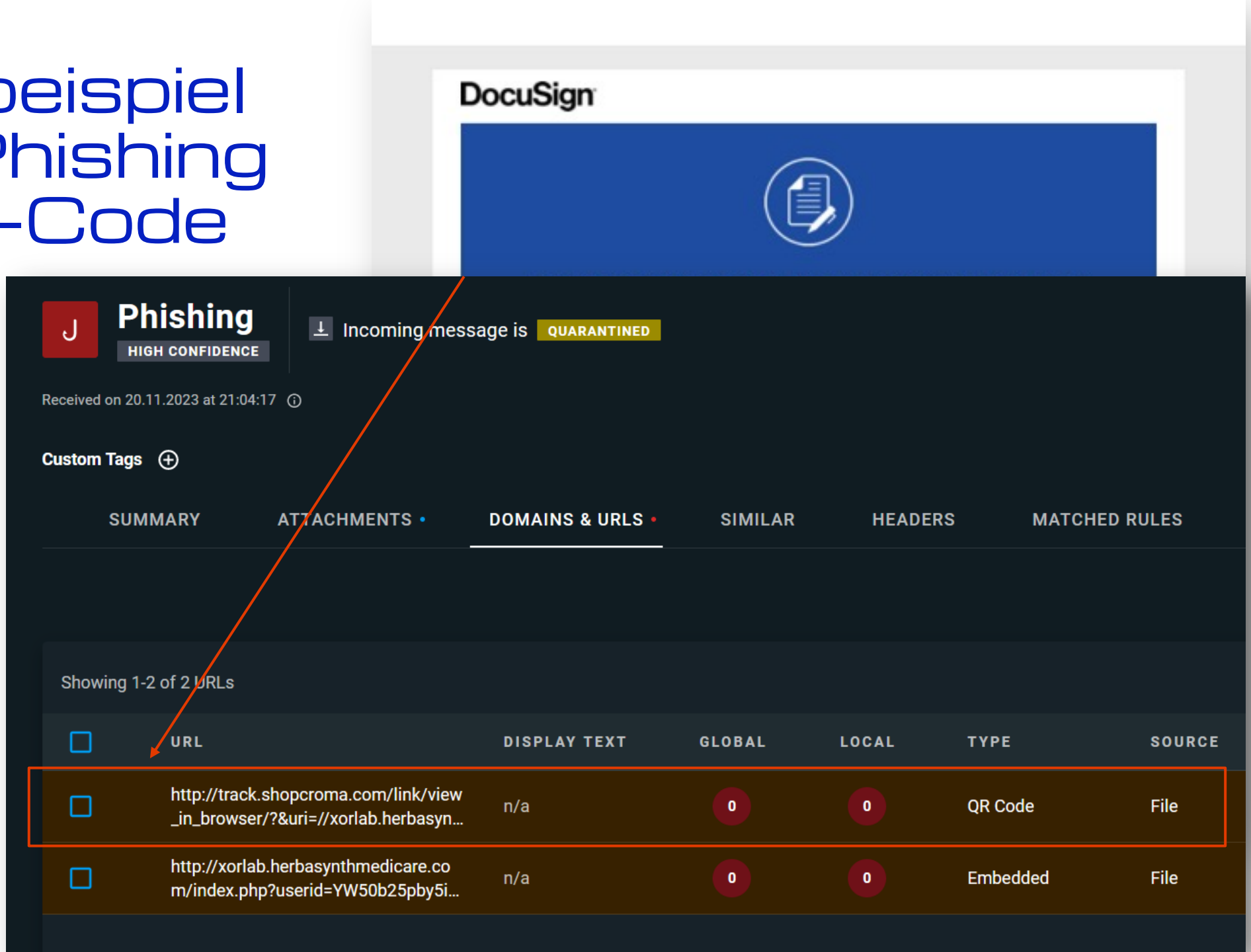
bitkom

Eine erste Einordnung

- Payload – Phishing / «Zero-Hour Phishing»
  - Zugangs- oder Zahlungsdaten
  - Schadcodeübermittlung über Anhänge oder Links
- Kein Payload – Social Engineering
  - Business Email Compromise / VIP Fraud
- Speziell – Spearphishing & Account Compromise

Praxisbeispiel (1/2): Phishing mit QR-Code

(aka. Quishing)



Praxisbeispiel (2/2): Business Email Compromise aka. VIP Fraud

Good morning [redacted]

Did Mr. [redacted] attorney at Baker McKenzie Law Firm, already contact you on my behalf, by telephone or by email regarding the [redacted] file currently managed at the Headquarters ?

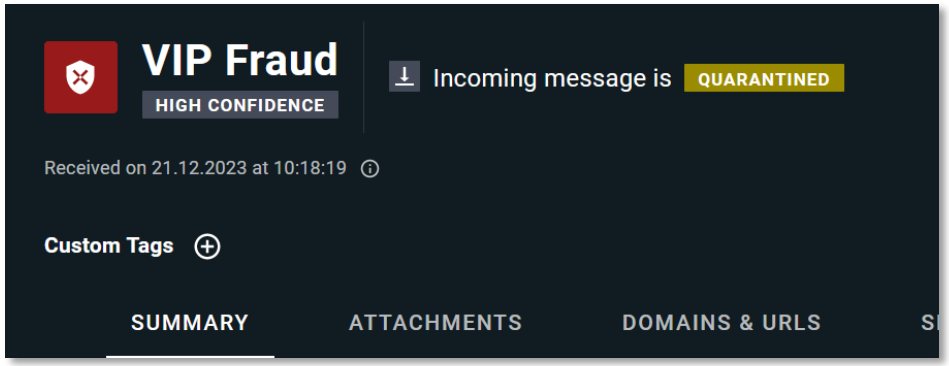
If he has not done it yet, contact him immediately on my behalf, **from your private e-mail** at the following address:
[redacted]@legal-bakermckenzie.com
The file reference [redacted] must be specified in your e-mail and also a phone number where you are reachable so that he explains to you what we are expecting from you.

I will get back to you once you have spoken to him, to give you my further instructions for the day.

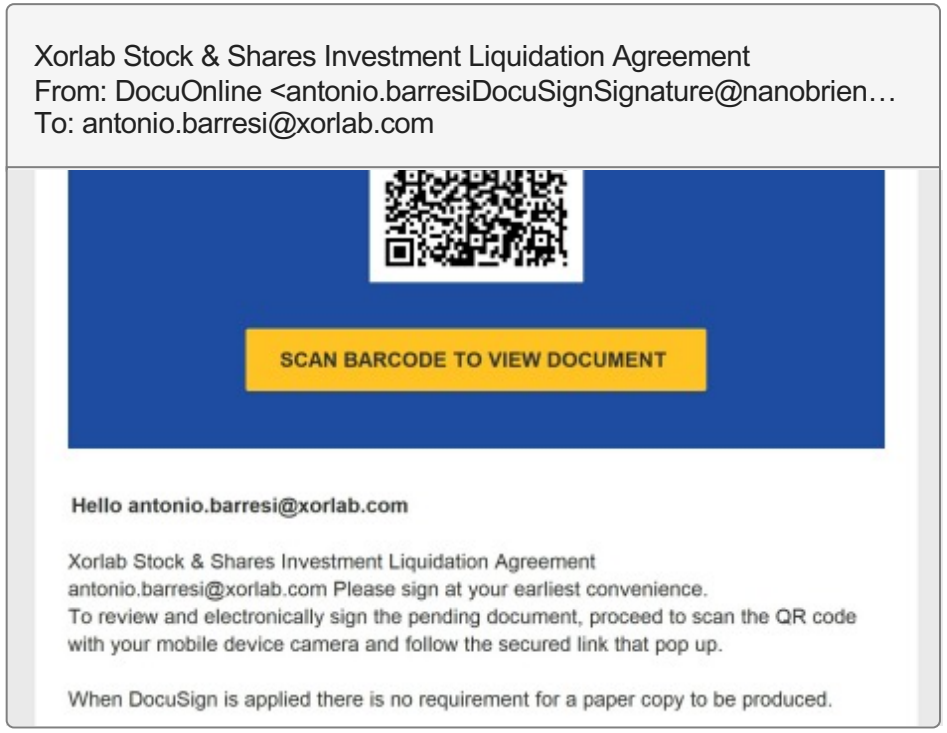
Freundliche Grüße / Best Regards,

[redacted]
CEO [redacted]

von meinem iPhone gesendet



Mögliche Gründe für die Häufung der Schäden



proofpoint. Microsoft cisco FORTINET

Beobachtete Probleme:

- Link wird nicht erkannt
- Link ist kein bekannter ”Indicator of Attack”
- URL Sandbox Analyse war OK
- Point-of-click Analyse war OK
- «Zero Hour Auto Purge» (ZAP) erfolglos

Fazit: statische Analyse bringt am meisten.

* Quelle: Analyse xorlab Januar 2024

Unseren Analysen nach sind die Phishing-Links in >80% der Fälle unbekannt

Frage: wie viele Phishing-E-Mails haben Eigenschaften eines Zero-Hour Angriffs?

Zero-Hour: der Phishing-Link ist in keiner «known malicious URL»-Datenbank enthalten.

Untersucht wurden die als Phishing klassifizierten E-Mails bei einem mittelgrossen Kunden während einem Zeitraum von 90 Tagen.

81% der Phishing-E-Mails sind sog. "Zero-Hour" Angriffe

Anzahl Phishing-E-Mails	12 461 (100%)
Davon «Zero-Hour»	10 147 (81%)
Davon »Known-Malicious»	2 314 (19%)

Solange E-Mail existiert, werden wir uns gegen Phishing etc. schützen müssen.

Die kriminelle Motivation bleibt, nur die Techniken werden sich ändern.

- Technische Ebene: Quishing, Shortener-Dienste, Google AMP, Open Redirects, HTML Smuggling, usw.
- Menschliche Ebene: «Message Injection», Account Compromise, LLMs, Deepfakes, usw.

LLMs senken die Angriffskosten und machen es Menschen gleichzeitig noch schwieriger, Angriffe zu erkennen

An early experiment with ChatGPT revealed powerful new attacker capabilities:

- Create phishing campaigns with completely unique emails
- Dynamically generate campaigns in multiple languages
- Have automated conversations in parallel and at scale
- Classify human responses to adjust and generate better answers
- Improve campaign effectiveness by feeding back the click or response rate
- Launch AI-Powered BEC attacks
- Use open-source intelligence to further customize phishing emails

xorlab

AVANITEC
Competence. Security. Trust.

2. Context Matters: Der xorlab-Ansatz

E-Mail Security neu gedacht | CISO Roundtable

Antonio Barresi, antonio.barresi@xorlab.com

Who am I

Antonio Barresi

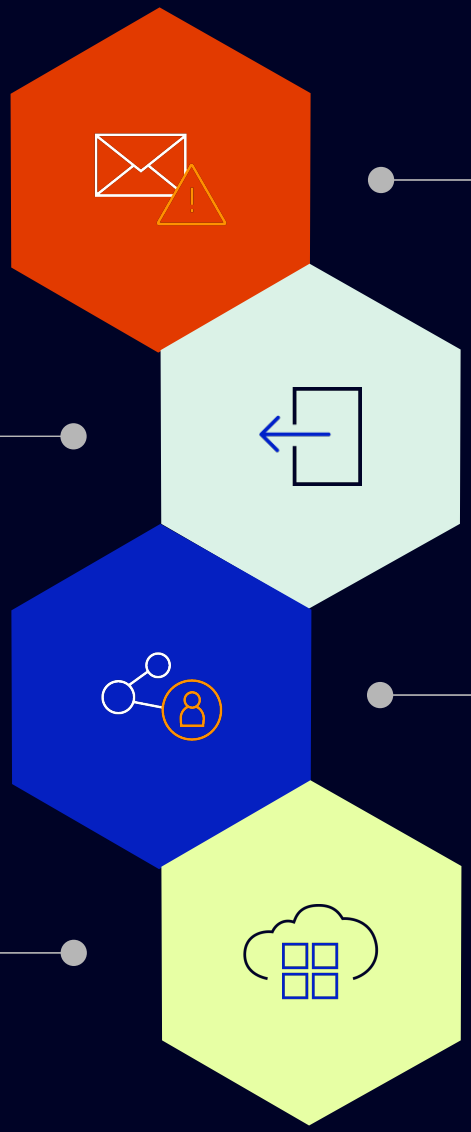
CEO & Gründer xorlab

- Security nerd and former security researcher
- Software exploitation and defense
- Mobile security
- Cloud side-channels
- Started with offensive security as a teenager
- Co-founded xorlab, an ETH Zurich Spin-off in cybersecurity

About us

Founded & based	Employees	Email accounts protected	Processed emails per day	Attacks prevented in 2023*
2015 in Zurich	**37**	**290 000+**	**20 Mio+**	**10 Mio+**

E-Mail Security braucht neues Angreifermodell



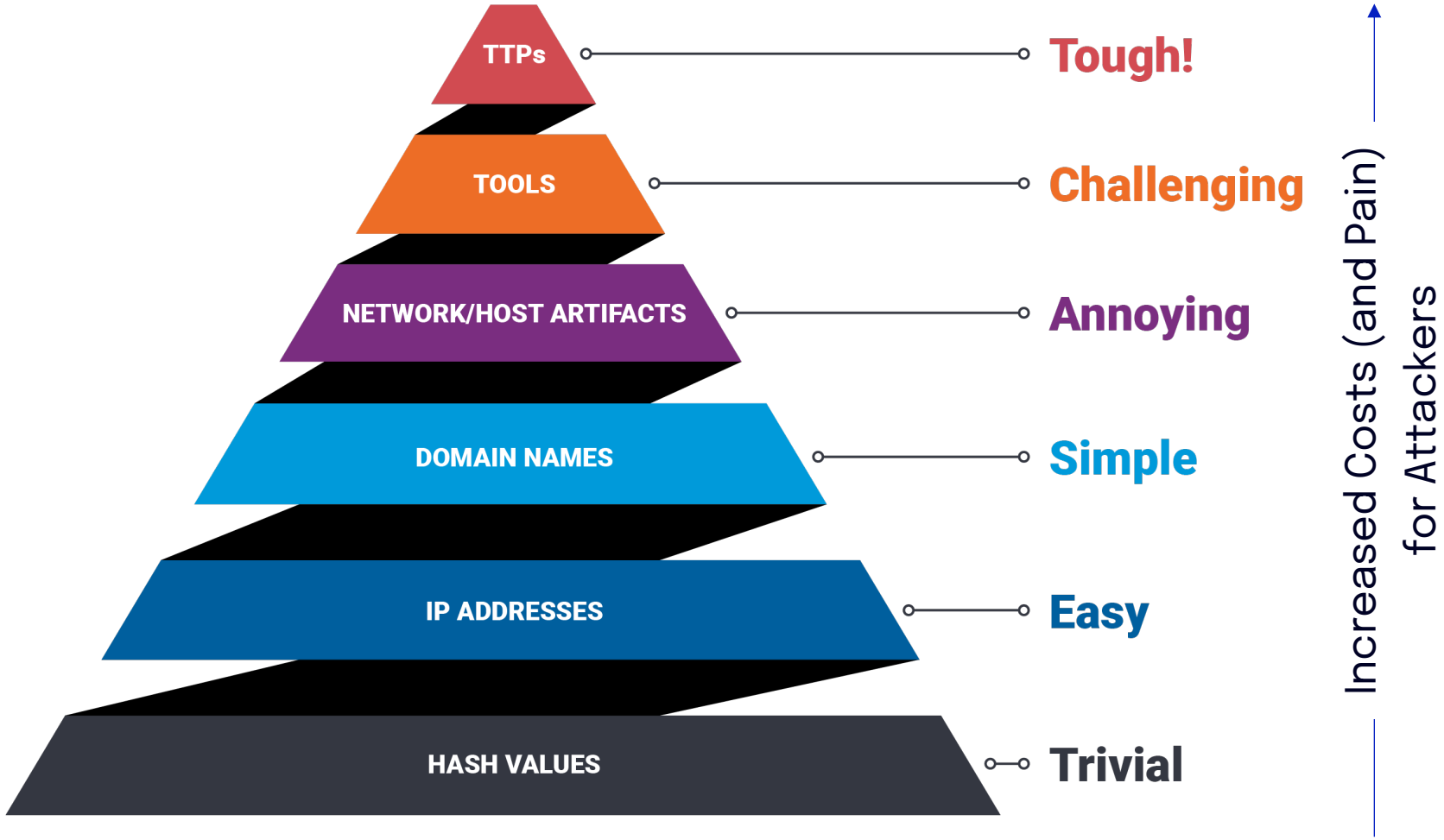
Angriffe sind “zero-hour”

Der Angreifer kann Sandbox-Checks umgehen (URL & Dateien)

Der Angreifer kontrolliert E-Mail Accounts vertrauter Parteien

Der Angreifer nutzt legitime Infrastruktur (z.B. M365)

Pyramid of Pain in Email Security

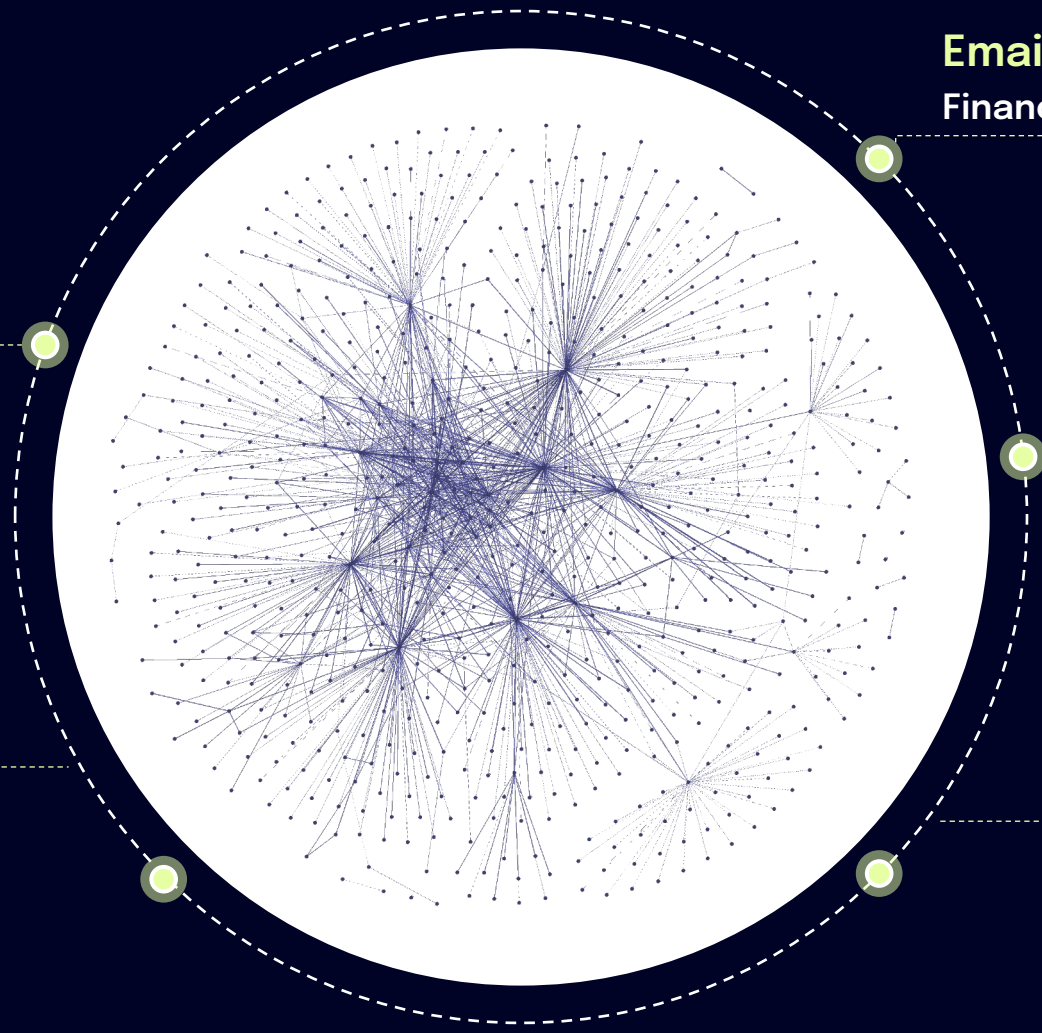


Die Pyramid of Pain gilt auch für E-Mail-basierte Angriffe

Context-Intelligence

Email content topics
Financial transactions | password reset | etc.

Relationships
Vendors | Customers | etc.



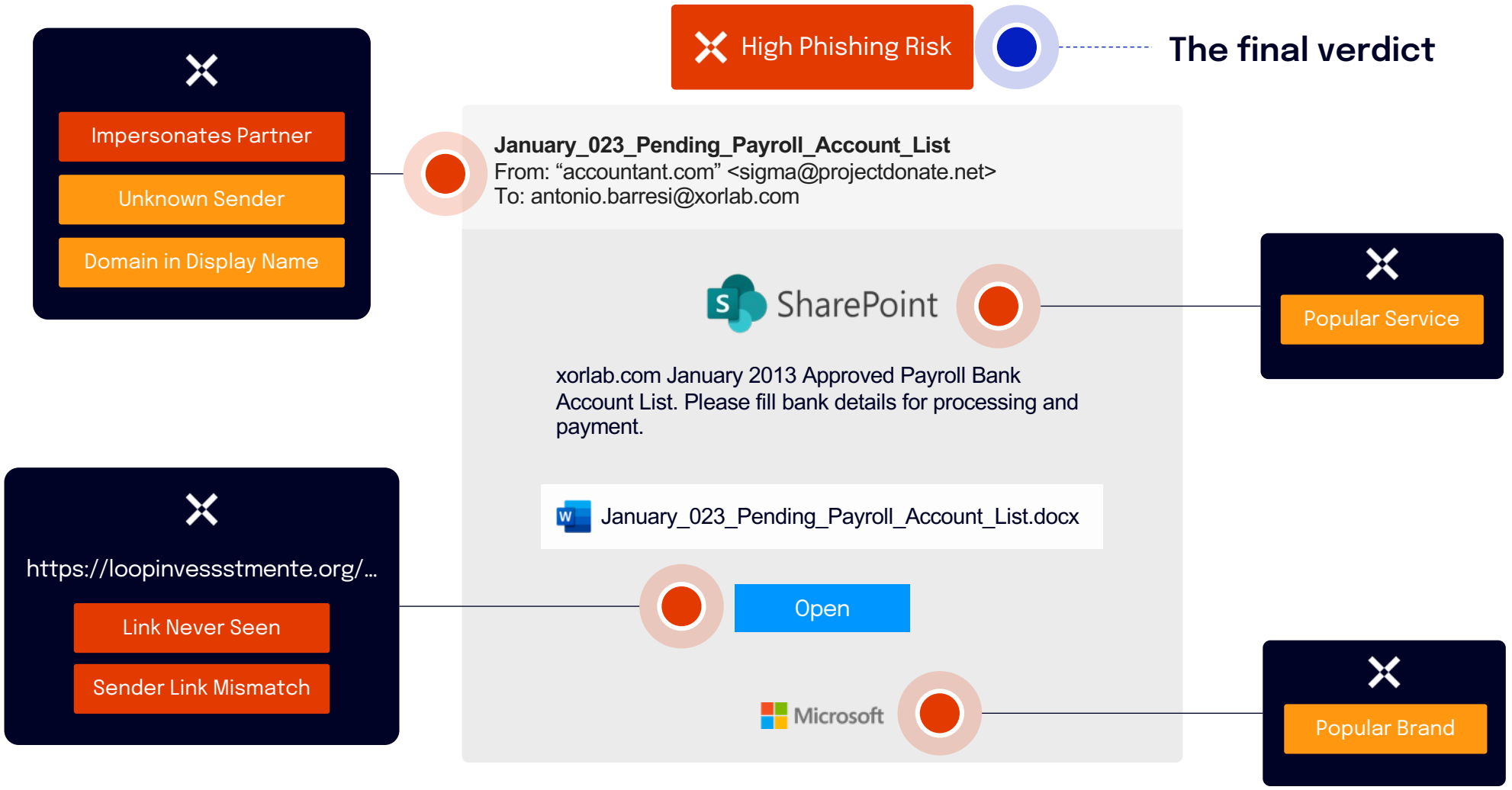
Sentiment
Urgency
| authority
| etc.

File types & attributes
Macros & active content |
encrypted archives | etc.

Links & domains
Cloud services | shadow IT | etc.

Plot: Visualizing the relationships from 3 months worth of xorlab email communication

Example


High Phishing Risk
The final verdict
Impersonates Partner
Unknown Sender
Domain in Display Name
January_023_Pending_Payroll_Account_List
From: “accountant.com” <sigma@projectdonate.net>
To: antonio.barresi@xorlab.com
SharePoint
Popular Service
xorlab.com January 2013 Approved Payroll Bank Account List. Please fill bank details for processing and payment.
January_023_Pending_Payroll_Account_List.docx
https://loopinvessstmente.org/...
Link Never Seen
Sender Link Mismatch
Open
Microsoft
Popular Brand

xorlab

Demo

Unsere Vision

1st line of defense	Tech | E-Mail Security Filter	• Stoppt Bedrohungen proaktiv • Reduziert Angriffsfläche • Ist transparent (keine Blackbox)
2nd line of defense	Mensch | Mitarbeiter + SecOps	• Sinnvolle Warnungen (Banner) • Alles wird gemeldet und triagiert • Isolation bei Verdacht
3rd line of defense	Tech | SIEM + SOAR + XDR	• Datenaustausch in Echtzeit • Korrelation mit anderen Daten • Integration mit E-Mail Security Filter

Vontobel

3. Mehr Kontrolle in der E-Mail Security

Erfahrungen nach 3 Jahren xorlab

Lukas Kellenberger
IT Security Engineer
Platform Security

Ausgangslage 2021

E-Mail Gateway als Managend Service bei Open Systems

- «Abhängigkeit» vom Support & Engineering
- Sinkende Service-Qualität, keine Innovationen
- Schlechte Filter-Qualität insbesondere bei Phishing-Attacken

Wohin wollen wir?

- On-Prem Lösung – mehr Transparenz für Administratoren
- Verbesserung der Filter-Qualität
- Unabhängigkeit

Potentielle Kandidaten

- Proofpoint
- Symantec Messaging Gateway
- Cisco ESA
- Trustwave Mail Marshal
- xorlab Security Platform

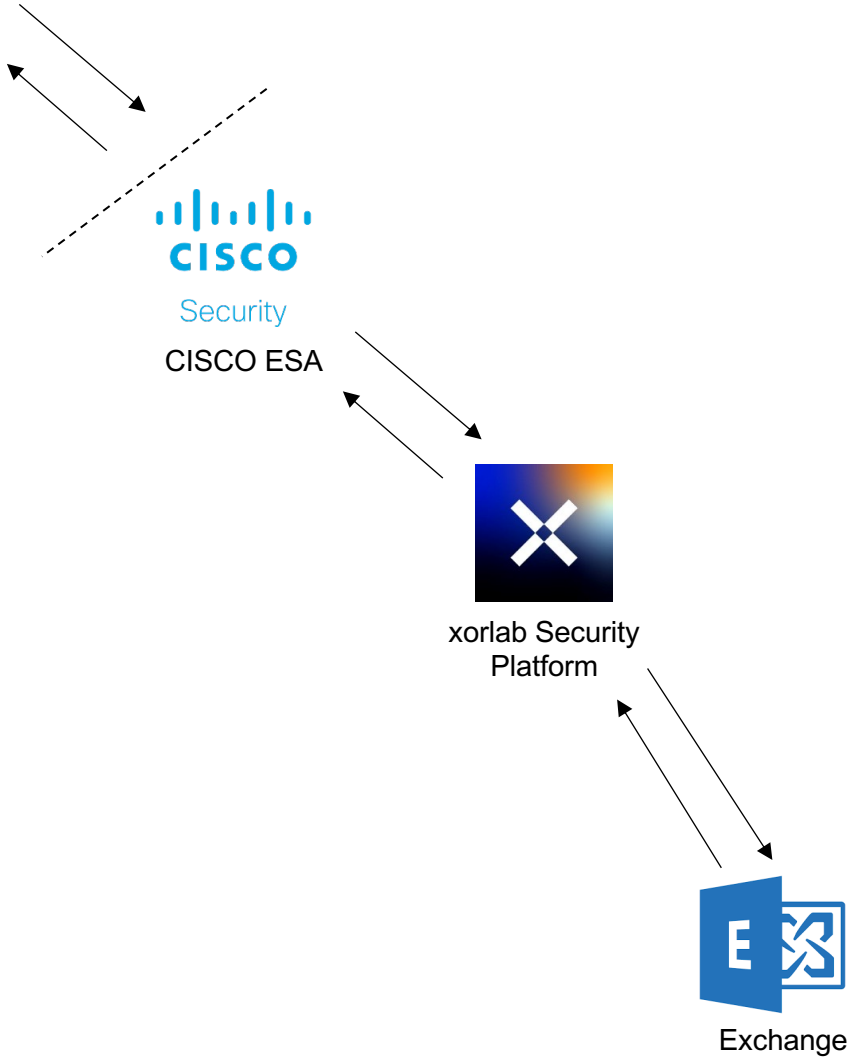
Wo wir heute stehen

Rollen, Funktionen & Prozesse

- User – Self-Service Quarantäne
- Analyst – Cyber Defense Team
- Helpdesk – 1st & 2nd Level Support
- Admin – Platform Security Team

Resultate

- Mehr Kontrolle
- Stabile Upgrades
- Mehr Transparenz für User
- Zeitersparnisse für Supporteinheiten, SOC und Administratoren
- Verbesserte Filter-Qualität
  - Rückgang der gemeldeten Phishing E-Mails um ca. 70%



Persönliche Erfahrungen

Zusammenarbeit

- Enge Zusammenarbeit
- Offene Kommunikation
- Spannende und lehrreiche Meetings
- Hilfsbereit

Produkt

- Sehr detaillierte Konfigurationsmöglichkeiten
- Campaigns erlauben es schnell, präzise Massnahmen zu treffen
- Das Tool macht Spass! :)

xorlab

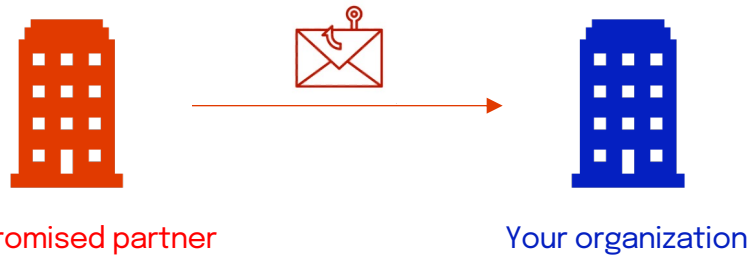
AVANITEC
Competence. Security. Trust.

4. Third-Party Risk Management

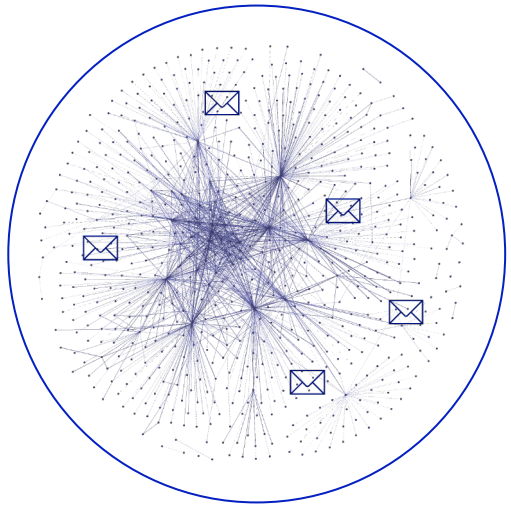
E-Mail Security neu gedacht | CISO Roundtable

Antonio Barresi, antonio.barresi@xorlab.com

Was hat Email mit 3rd-Party Risks zu tun?

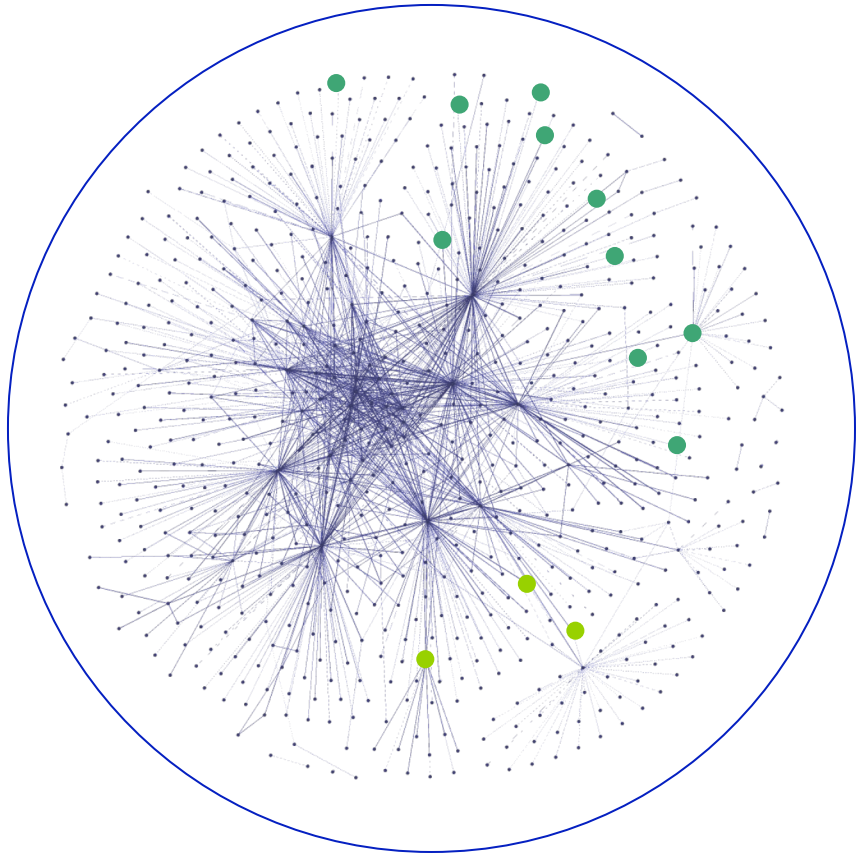


Attack vector



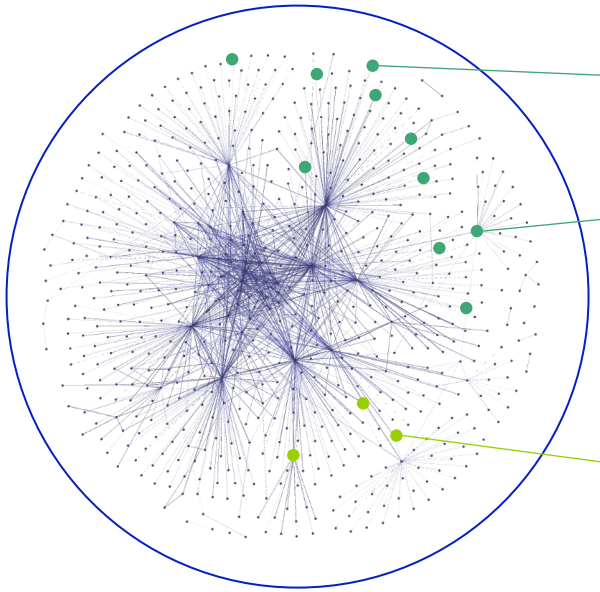
Intelligence

Identifikation der Third-Parties



	RELEVANCE
NexaWealth Partners	100
LegalPeak Associates	82
SkywardTech Cloud Solutions	67
Datalogix	42
BuildCraft Contractors	30

Anreicherung mit Threat Intelligence



NexaWealth Partners — Recent Ransomware incident

joe@nexawealth.com — Recently leaked credentials found

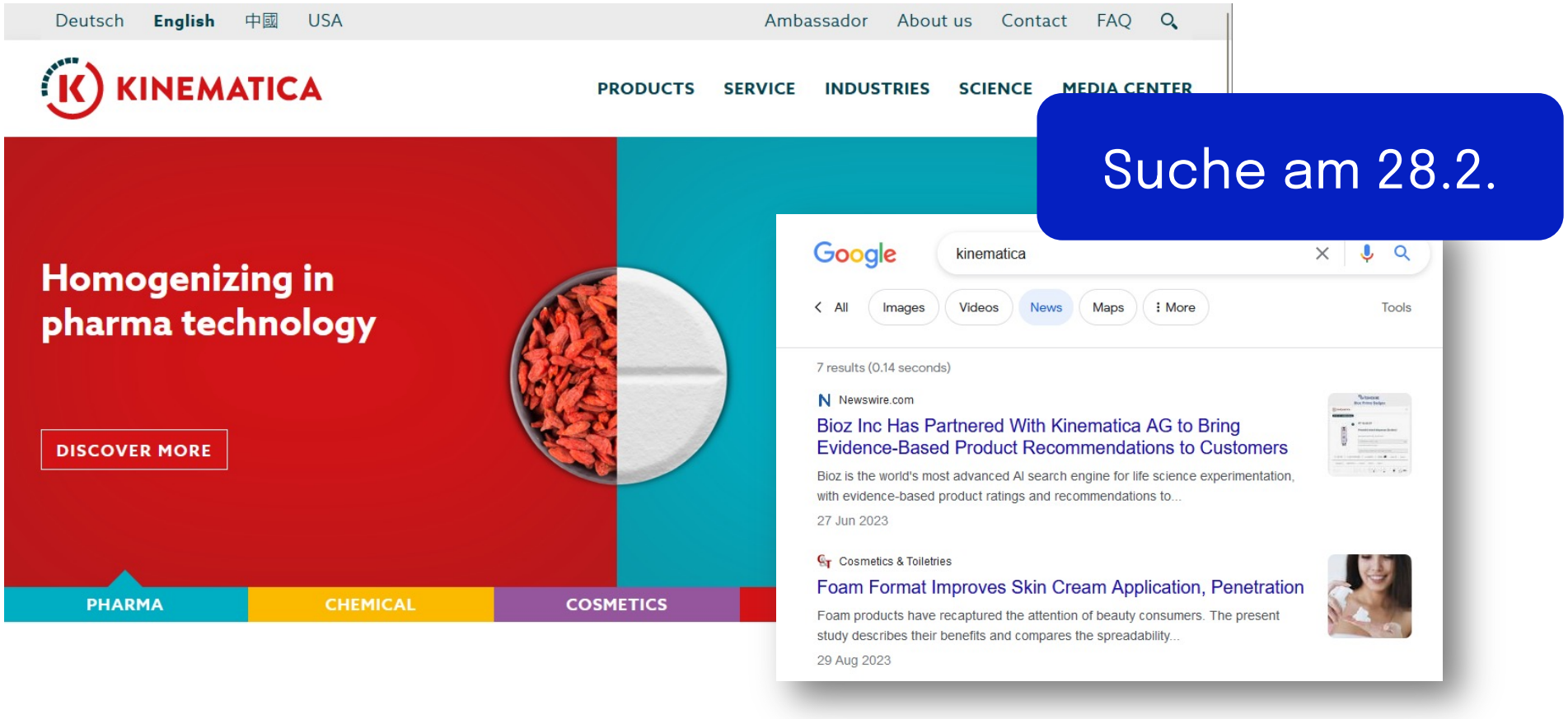
bob@nexawealth.com — Recently leaked credentials found

LegalPeak Associates

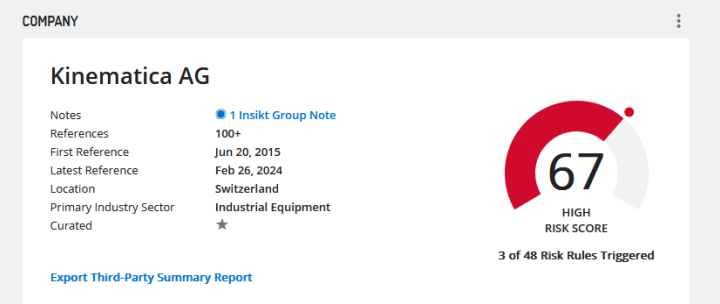
alice@legalpeak.legal

Threat Intelligence

KINEMATICA

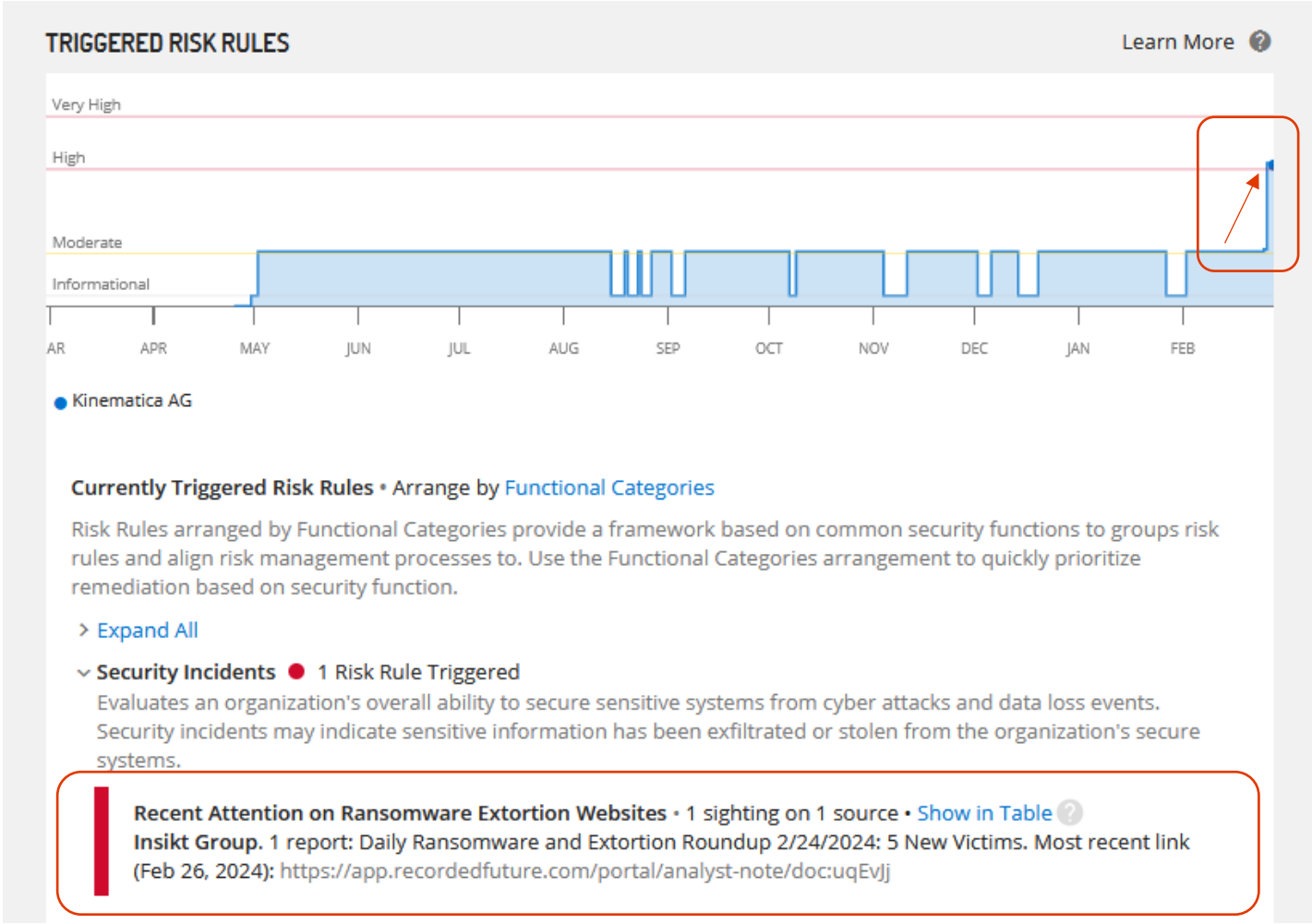


Threat Intelligence (Recorded Future)

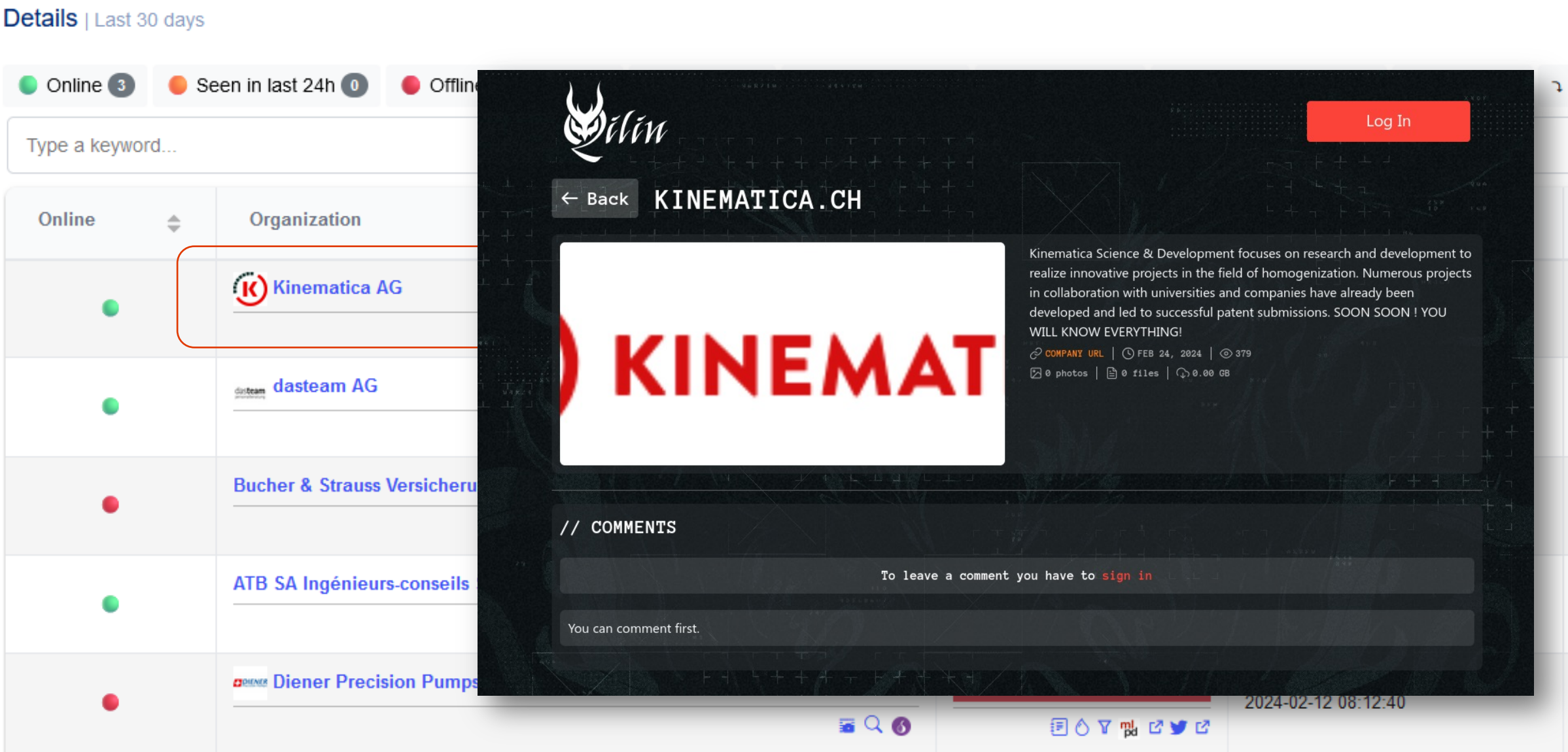


On 26.2.2024 the Risk Score went from 27 to 68

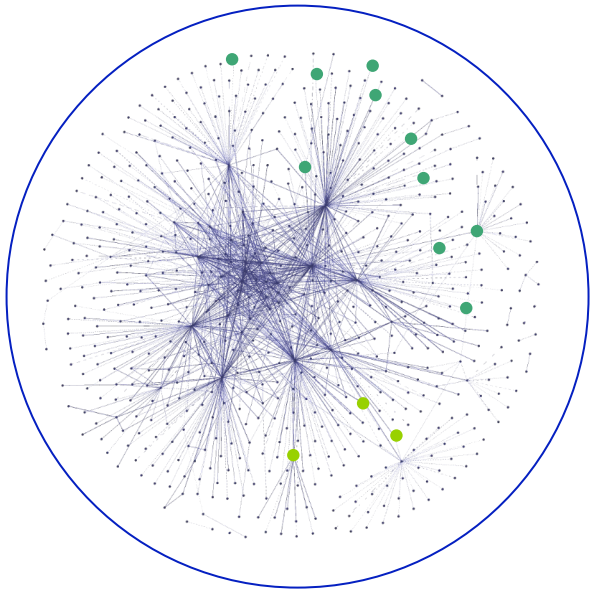
27 → 68



Threat Intelligence (eCrime.ch)



Third-Party Risiken zeitnah erkennen



KINEMATICA + 27 → 68

Potenzielles Risiko
wird erkannt und kann
zeitnah adressiert werden!

Qualität der Threat Intelligence

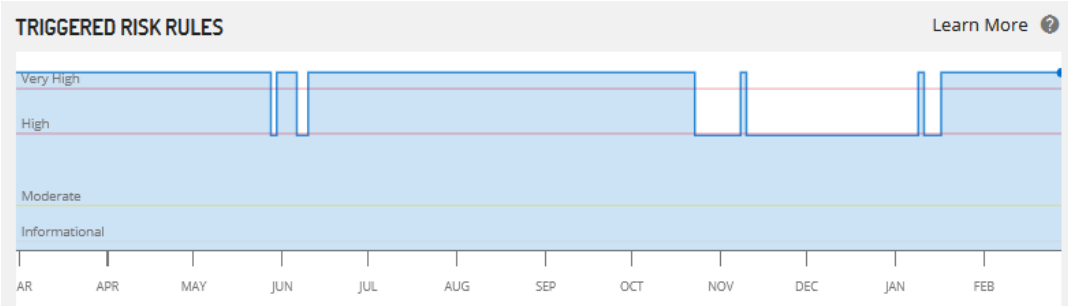
Microsoft

Notes	2891 Insikt Group Notes
References	1 000 000 000+
First Reference	Jan 28, 2009
Latest Reference	Feb 28, 2024
Location	United States
Primary Industry Sector	Software
Curated	★

39 of 48 Risk Rules Triggered

Used in List
- Companies Susceptible to Ivanti Connect Secure and Ivanti Policy Secure
- Companies susceptible to CVE-2022-41040 and CVE-2022-41082
- Companies Susceptible to Ivanti EPMM Vulnerability

Export Third-Party Summary Report



Malicious Network Activity ● 9 Risk Rules Triggered

Evaluates an organization's ability to implement security controls that protect against machine compromise and external communications to known bad indicators of compromise. Observed malicious network activity may indicate an organization's machine is compromised or infected with malware.

Hosts Recently Communicating With C&C Server • 214 sightings
Active command and control communication on uncommon ports related to malware from 17 hosts including **3.120.253.178**, **52.11.171.106**, **15.181.145.235**. 3 related malware families: Cobalt Strike, PlugX, Quasar. Last observed on Feb 25, 2024.

Likely IT Policy Violations • 4 sightings
Recent Tor Node seen for 4 IP Addresses on company infrastructure including **52.214.94.163**, **13.127.5.47**, **18.233.162.212**

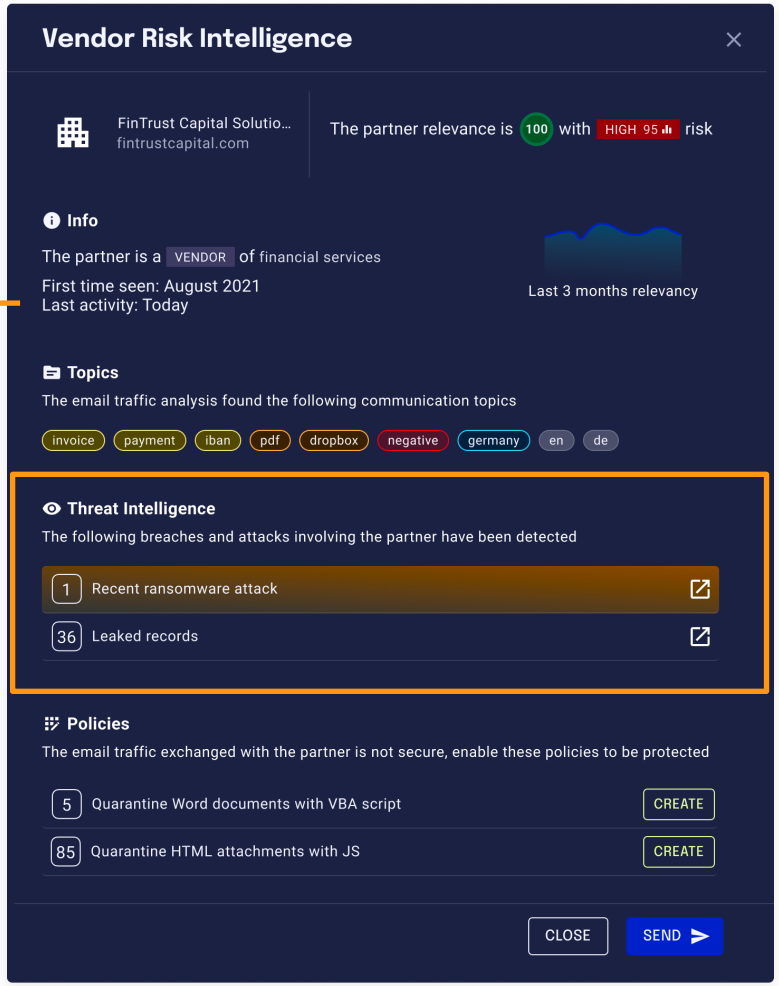
Possible IT Policy Violations • 10000+ sightings
Honeypot Host seen for 31,477 IP Addresses on company infrastructure including **51.17.62.122**, **13.208.56.168**, **13.40.168.17**

Infections Recently Reported in Company Infrastructure • 100+ sightings
Resolution of Fast Flux DNS Name seen for 217 IP Addresses on company infrastructure including **18.141.146.247**, **13.212.175.108**, **54.169.183.167**. Recent Host of Many DDNS Names seen for 111 IP Addresses on company infrastructure including **54.207.241.159**, **3.21.245.172**, **3.236.167.187**. Suspected Malicious Packet Source seen for 96 IP Addresses on company infrastructure including **3.8.6.16**, **18.130.104.69**, **18.130.50.26**. Recent Botnet Traffic seen for 808 IP Addresses on company infrastructure including **78.13.48.172**, **18.212.86.39**, **18.167.17.158**

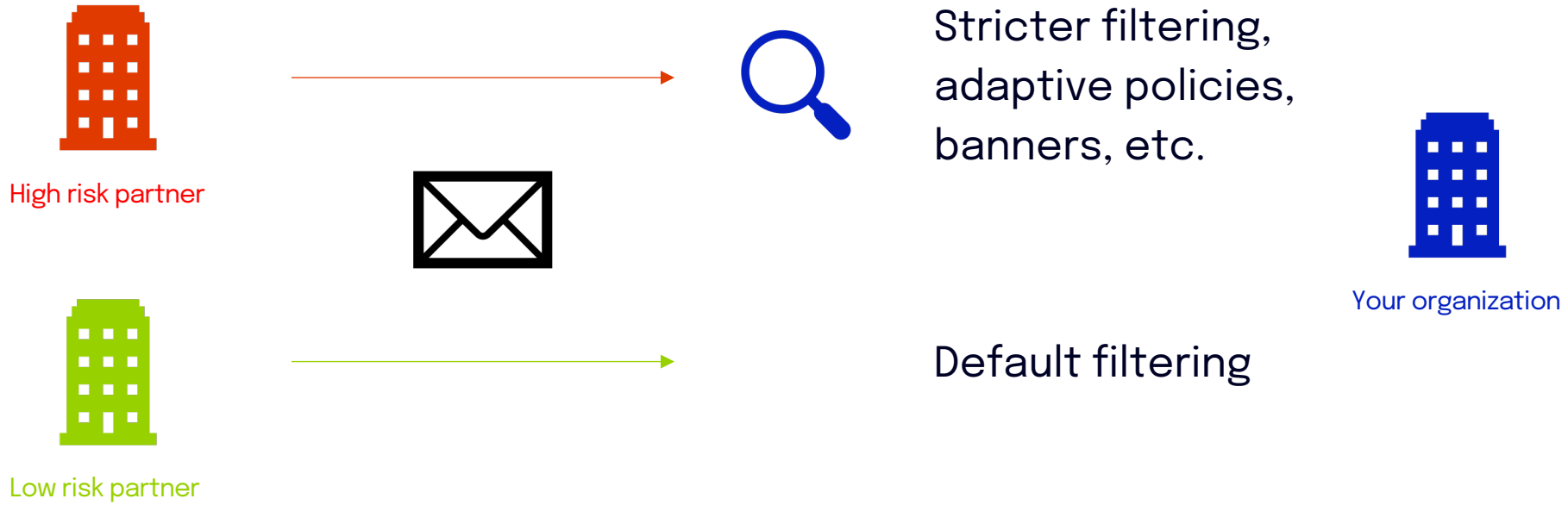
Recent High-Impact Abuse of Company Infrastructure • 10+ sightings
Validated C&C Server seen for 6 IP Addresses on company infrastructure including **3.66.38.117**, **3.121.139.82**, **18.198.77.177**. Recently Reported C&C Server seen for 30 IP Addresses on company infrastructure including **3.126.37.18**, **18.158.249.75**, **3.68.171.119**. Mitigated by being in Amazon Web Services Infrastructure (Allow List), Multi-Domain IP Addresses (Allow List).

Recent Possible Malware in Company Infrastructure • 10+ sightings
Recent Positive Malware Verdict seen for 48 IP Addresses on company infrastructure including **100.25.39.123**, **18.239.63.203**, **35.171.144.152**

Identifikation der Third-Party Risks



Erhöhte E-Mail Sicherheit



E-Mail ist eine wertvolle Informationsquelle, um **zeitnah** und **dynamisch** 3rd-Parties zu identifizieren.

- Angereichert mit der richtigen Threat Intelligence können so Risiken erkannt werden.
- Richtig reagiert kann zusätzlich die Sicherheit erhöht werden, in dem die E-Mails von Partnern mit hohem Risikopotenzial strikter beurteilt werden.

xorlab

AVANITEC
Competence. Security. Trust.

6. Trends & Ausblick

E-Mail Security neu gedacht | CISO Roundtable

Christine Hakenjos, christine.hakenjos@xorlab.com

Who am I

- Start-up and product marketing enthusiast
- With xorlab since January 2024
- Product Marketing: Customer Success Stories / Product Roadmap / Value and Benefits

Christine Hakenjos

Product Marketing

Awareness is not enough

ETH Study Findings

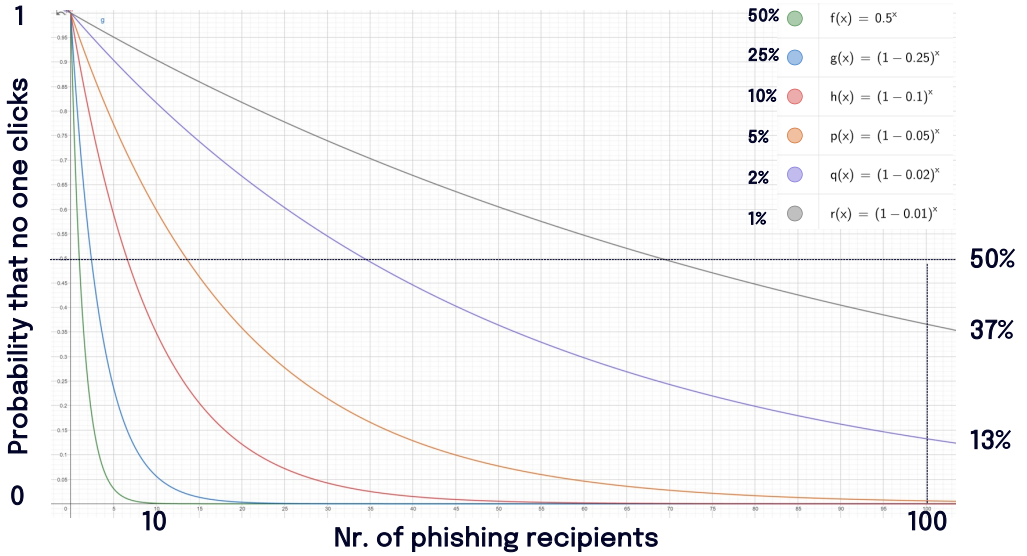

Phishing in Organizations: Findings from a Large-Scale and Long-Term Study

Daniele Lain, Kari Kostiainen, and Srdjan Čapkun
Department of Computer Science
ETH Zurich, Switzerland
{daniele.lain, kari.kostiainen, srdjan.capkun} @inf.ethz.ch

ETH zürich

- There are several “repeated clickers” in a large organization.
- Voluntary embedded training in simulated phishing exercises is not effective.
- Many employees will eventually fall for phishing if continuously exposed.

Assuming that 1% falls for any given phishing attack, the chance that no one clicks is less than 10% if more than 230 people receive the phish (.99^230 = .099)



https://arxiv.org/abs/2112.07498

External sender banners

CAUTION: This e-mail originated from outside the organisation. Do not click on links or open attachments unless you recognise the sender and know the content is safe.

Be aware: This is an external email.

ELSEVIER

Decision Support Systems
Volume 92, December 2016, Pages 3-13

Your memory is working against you: Ho
eye tracking and memory explain
habituation to security warnings

Bonnie Brinton Anderson [a]
C. Brock Kirwan [b c], Davi

people unconsciously scrutin
that habituation sets in after
with further repetitions. Using guidelines from the warning science literature, we design

frontiers in Psychology

Front Psychol. 2020; 11: 528079.
Published online 2020 Dec 7. doi: 10.3389/fpsyg.2020.528079

PMCID: PMC7751389
PMID: 33364992

Repetition of Computer Security Warnings Results in Differential Repetition Suppression Effects as Revealed With Functional MRI

C. Brock Kirwan,[1,2,*] Daniel K. Bjornn,[2] Bonnie Brinton Anderson,[3] Anthony Vance,[4] David Eargle,[5] and Jeffrey L. Jenkins[3]

▸ Author information ▸ Article notes ▸ Copyright and License information PMC Disclaimer

https://www.ncbi.nlm.nih.gov/pmc/articles/PMC7751389/
https://www.sciencedirect.com/science/article/abs/pii/S0167923616301592

Contextual banners

Alert

New external sender and organization

The sender including its organization is not known to us. If you have not expected this message please ignore or report it.

Warning

New external sender

The external sender is not known to us but the organization is. If you have not expected this message please ignore or report it.

Info

Weak relationship with external sender

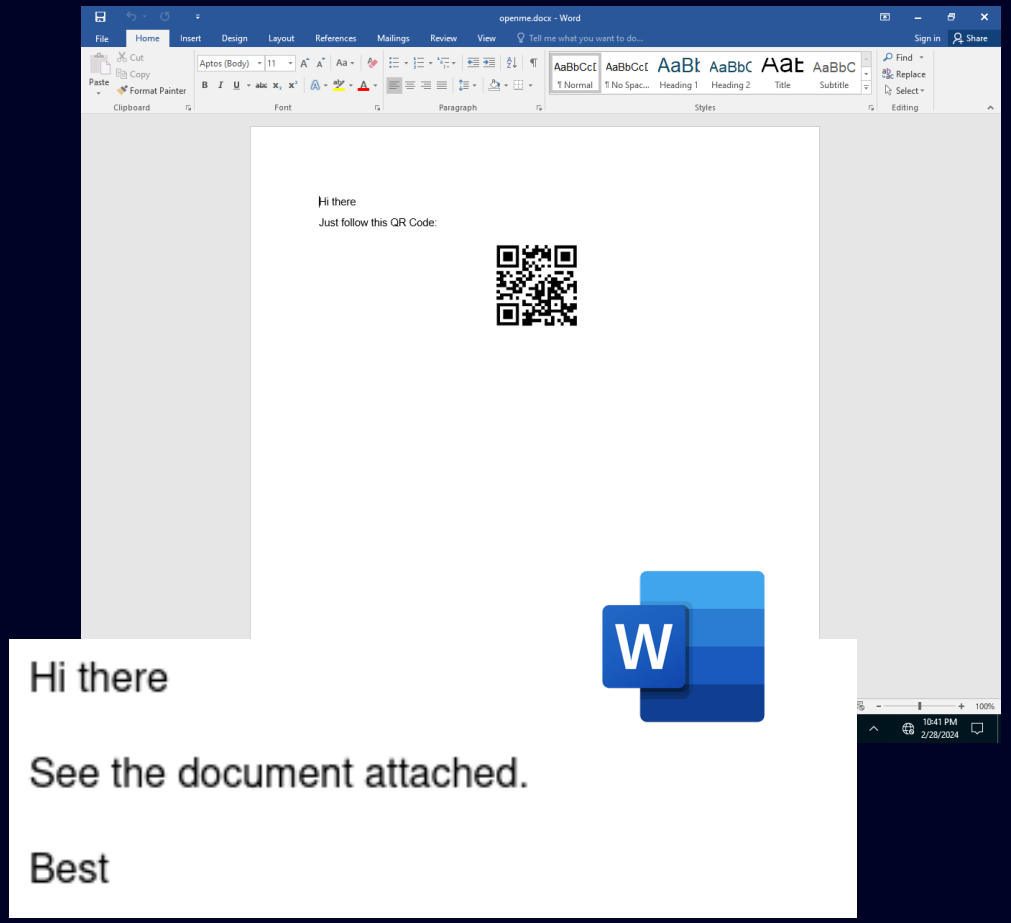
Be cautious with new relationships in new communication channels. When in doubt, please report the message.

£ r ï ŪęŪʕēЦЄŒŪħ

- Invoice from never seen before organization
- Invoice from known organization
- Graymail
- Potential Phishing, BEC, Spam
- Dangerous file types

Goal: no banners with most legitimate emails!

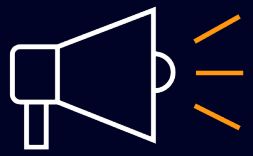
Stay in control with adaptive policies




```
1  // Sets tags #untrusted #youngsender
2
3  messages.inbound
4  and not(sender.is_tusted)
5  and sender.domain.registered_date < 5d
6  and link.in_document: {
7    link.relevance <= 5
8    and (link.is_shortened
9          or link.is_in_qr_code)
10 }
11
```

Sharing of policies across customers

Trends we observe and support



Support the human factor

Stay in control

Benefit from collaboration