CYBERSECURITY OFFICE HOURS

endsight

www.endsight.net | info@endsight.net | (833) 363-7444

endsight

About Stephen Hicks

Stephen Hicks

CISSP, CCSP, CISM

Security Practice Manager @ Endsight

- Over 25 years in IT (over a decade in cybersecurity).
- Over a dozen technical certifications
- MBA from Saint Mary's college
- Majority of career working with SMBs

☎ (510) 280-2036

✉ shicks@endsight.net

ABOUT

San Diego Business Journal
2024 TOP
TECHNOLOGY SOLUTION PROVIDERS

MSP 501
Channel Futures 2024

THE CHANNEL CO.
CRN
SOLUTION PROVIDER 500
2024

SAN FRANCISCO BUSINESS TIMES
2024 BEST PLACES TO WORK IN THE BAY AREA
2024 BEST PLACES TO WORK
B P t W
Endsight
RANKED #24

THE CHANNEL CO.
CRN
FAST GROWTH 150
2024

Gold: Best Computer Services
2024 - Best of Napa County

Respect & Connect

Servant's Heart

Value Value

Progress Over Comfort

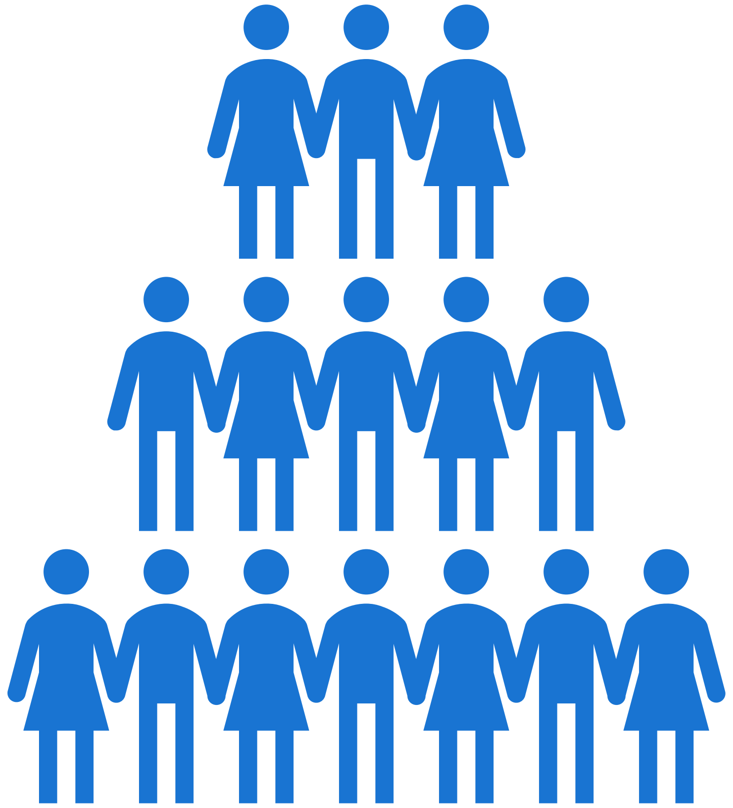
endsight

WHAT THIS IS INTENDED TO BE

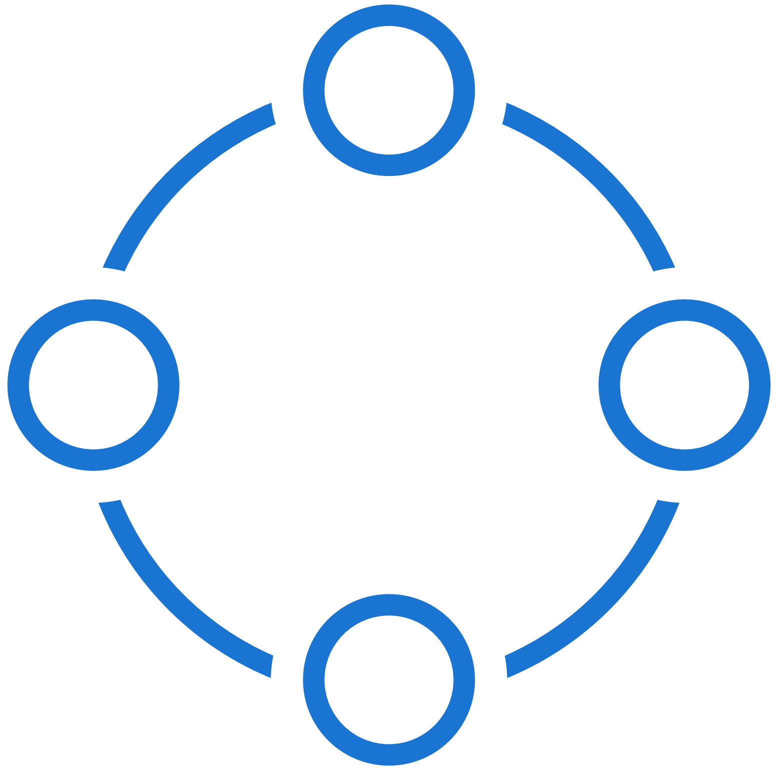
- High level, strategic discussion
- Suitable for C-Suite
- Not tactical, not user focused

The Three Pillars

People



Process



Technology

In that order

If you reach this point, 2/3 of your process has failed.

Topic for this quarter

5

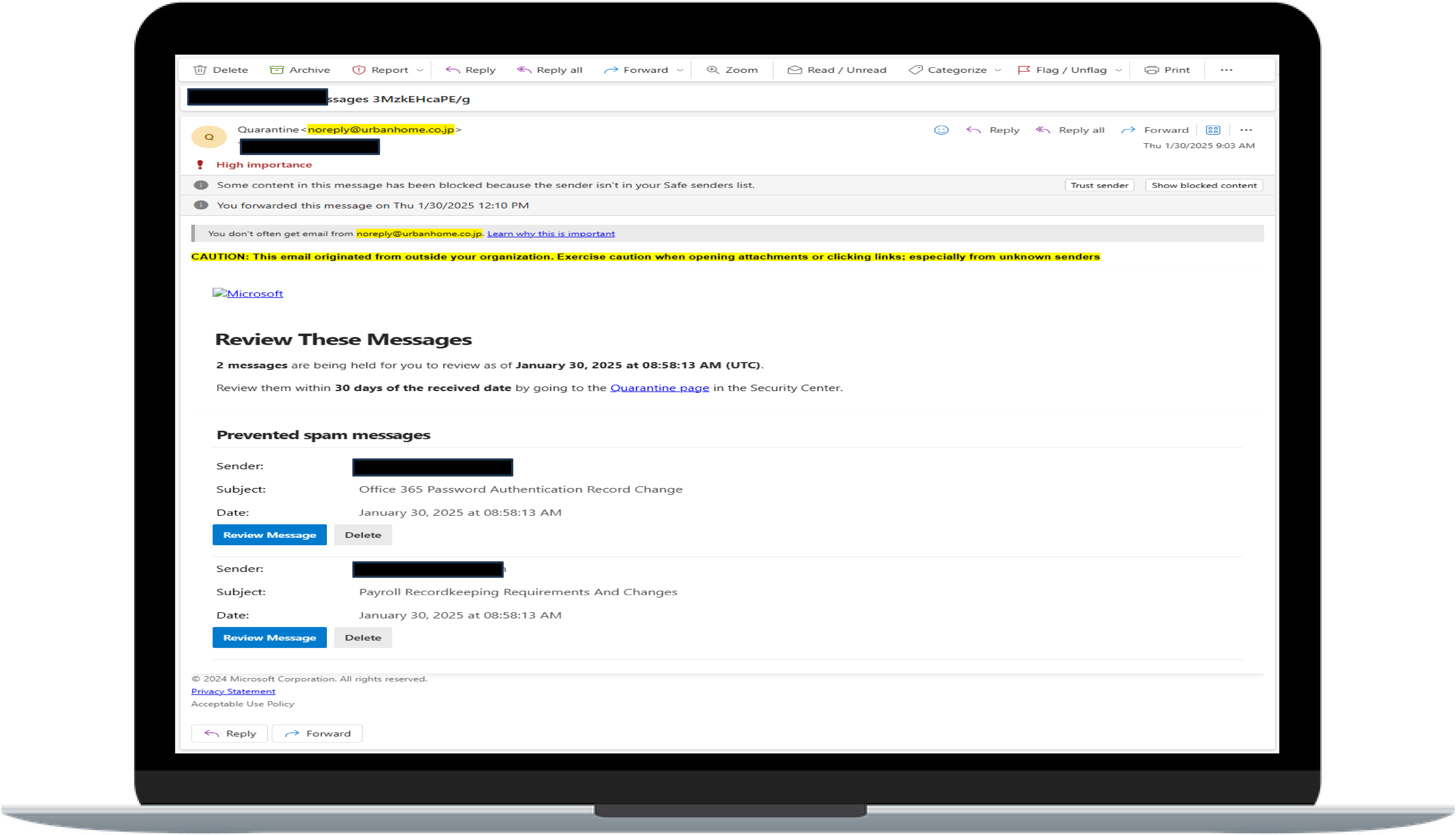
Phishing Emails

3 Endsight gets roughly 3 reported attacks per day, despite asking clients not to send us phishing emails

Phishing comes in many forms, and AI is making them much better

? What do we do about phishing attacks?

endsight



[redacted]ssages 3MzkEHcaPE/g

Quarantine <noreply@urbanhome.co.jp>

[redacted]

Thu 1/30/2025 9:03 AM

High importance

Some content in this message has been blocked because the sender isn't in your Safe senders list.

You forwarded this message on Thu 1/30/2025 12:10 PM

You don't often get email from noreply@urbanhome.co.jp. Learn why this is important

CAUTION: This email originated from outside your organization. Exercise caution when opening attachments or clicking links; especially from unknown senders

Microsoft

Review These Messages

2 messages are being held for you to review as of **January 30, 2025 at 08:58:13 AM (UTC)**.

Review them within **30 days of the received date** by going to the Quarantine page in the Security Center.

Prevented spam messages

Sender:	[redacted]
Subject:	Office 365 Password Authentication Record Change
Date:	January 30, 2025 at 08:58:13 AM

Review Message | Delete

Sender:	[redacted]
Subject:	Payroll Recordkeeping Requirements And Changes
Date:	January 30, 2025 at 08:58:13 AM

Review Message | Delete

© 2024 Microsoft Corporation. All rights reserved.
Privacy Statement
Acceptable Use Policy

Financial Fraud

Financial Fraud is the most common reason to use a phishing attack

$1.2M

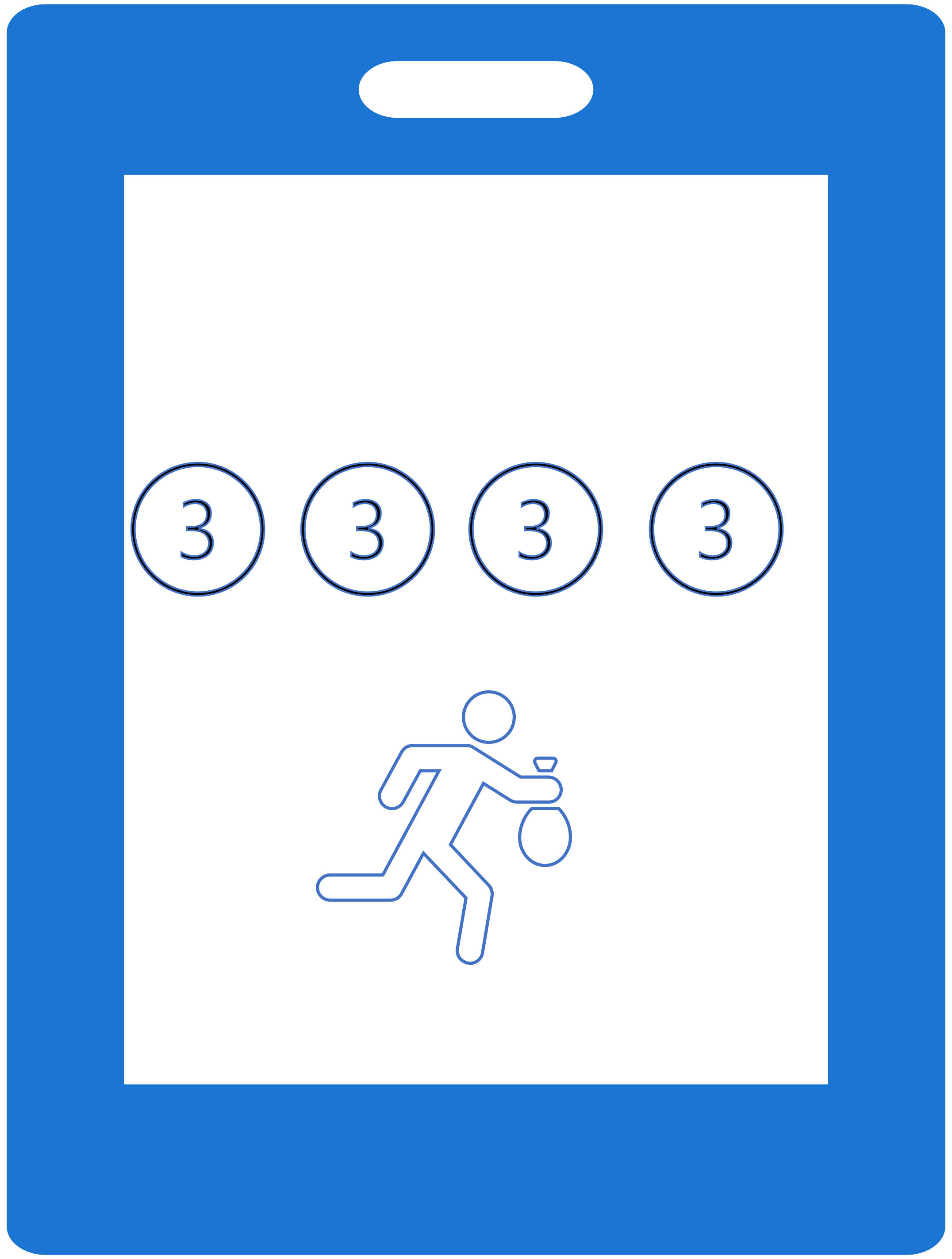
Endsight clients lost roughly $1.2 million in the last two years from financial fraud attacks

... and 3 jobs

Why we can’t just ‘sell something’ to fix this.

endsight

Fake Logins



Attackers have found a way around MFA – and it’s humans

It's always humans

Man in the middle attack

How common is this and how do we deal with it?

…And how do we do so without upsetting everyone?

Supply Chain Attack

Multiple firewall zero days for SSL VPN exploits in the past year

What is ZTNA (Zero Trust Network Access) and why is it important?

Okta, Lastpass, Microsoft attacks

US Government attacks and data leakage.

Process Breakdown

Multiple signers for payment changes

Documentation and review of said process

How can process break down? (A discussion)

Email reporting process and evaluation process

When all else fails…
Pick up the dang phone!

Is Your House in Order?

Contact Technical Account Manager or Sales Rep to setup a call with us. (Or answer "Yes" in the form)

Take that information to internal stakeholders and see if that's an appropriate risk profile

Work with us to remediate and mitigate the inappropriate risks

endsight

SUMMARY

- Threat actors focusing on cloud and humans
- People are the single most important piece
  - People
  - Process
  - Technology (in that order)
- There’s no more ‘set it and forget it’ – continual review and invested stakeholders are key in the modern threat landscape.
- Users will always require training, reinforcement, and consequences.
- Endsight has a service (The MSSP) to assist with process, training, and the human element.

Q&A

- Are document library stored in the Office 365 cloud subject to AI crawling?
- I delete items I see in my e-mail without opening them to read any message and they still show as if I did. Is there a way around this?
- Do you have any website security recommendations?
- What are our alternatives if the Authenticator app can now be intercepted by cyber criminals?

endsight

Office Hours

- May 22nd @ 1 PM PST.
  - To register:
    - Scan the barcode
    - Go to: https://get.endsight.net/cybersecurity/office/hours
    - Email akreps@endsight.net to register
    - Answer "Yes" in the poll.
      - We can also auto register you for the remaining 2025 sessions

AI/Copilot Webinar

- March 13th @ 1 PM PST.
- Title - Microsoft Copilot: What You’re Missing and How to Use It Better
- Similar format to Office Hours, but with some training.
  - To register:
    - Scan the barcode
    - Go to: https://www.endsight.net/development/webinar
    - Email akreps@endsight.net to register
    - Answer "Yes" in the poll.

endsight

endsight

Stephen Hicks
CISSP, CCSP, CISM
Security Practice Manager @ Endsight

Thank you!

☎ (510) 280-2036
✉ shicks@endsight.net