

ENDSIGHT.NET

Cybersecurity Office Hours

Stephen Hicks, Security Practice Manager

Q2 2026



endsight



Stephen Hicks
**Security Practice
Manager**
CISSP, CCSP, CISM

Phone Number: (510) 280-2036

Email: shicks@endstight.net



MBA from St. Mary's University.



Over 25 years in IT (over a decade in
Cybersecurity).

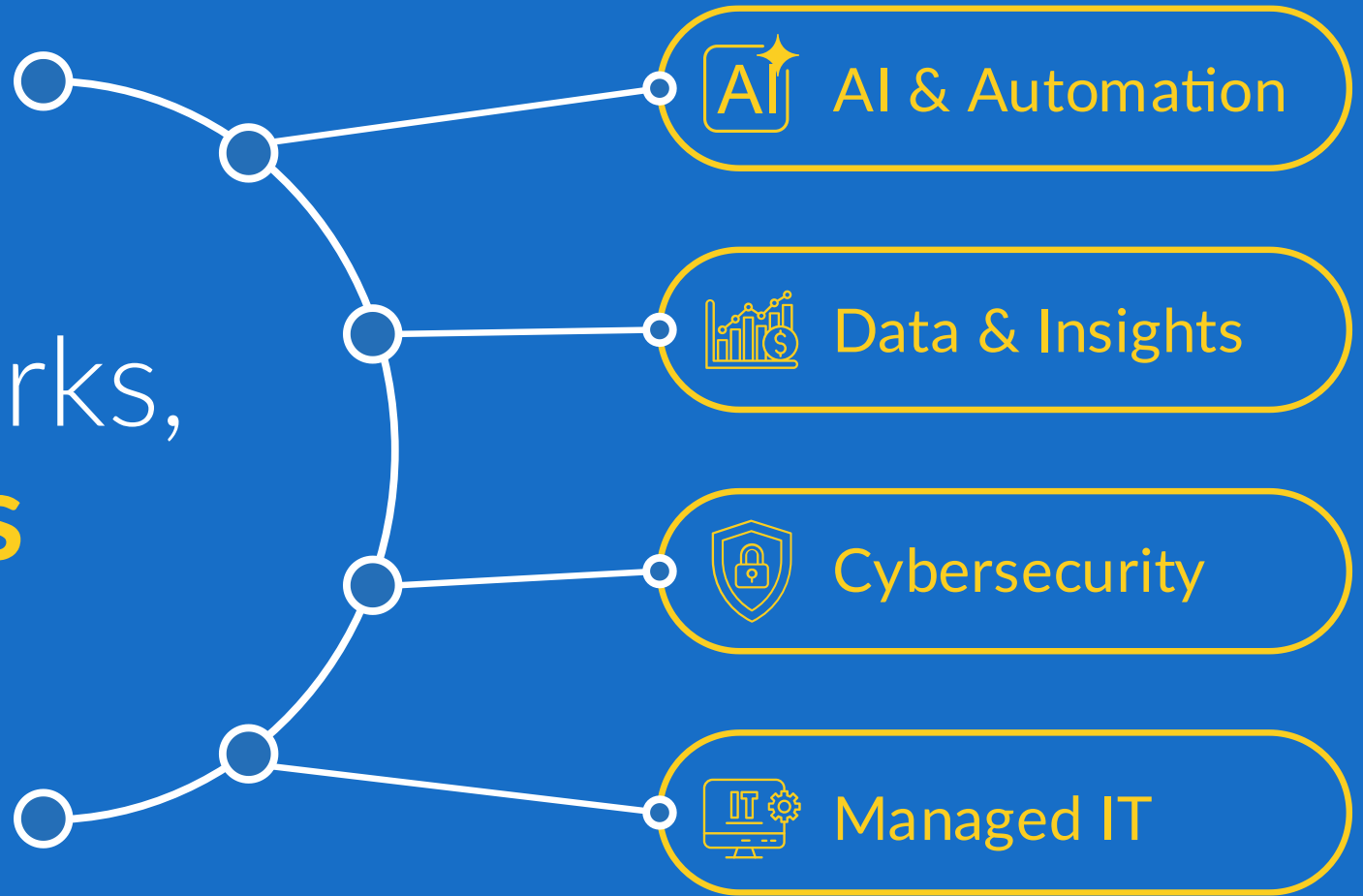
Majority of career working with SMBs.



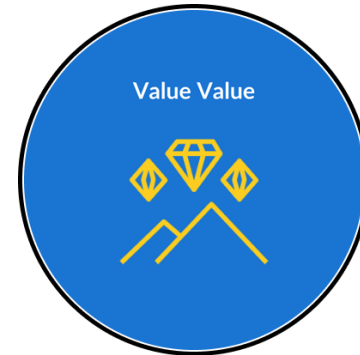
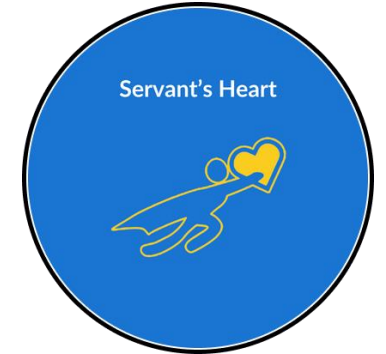
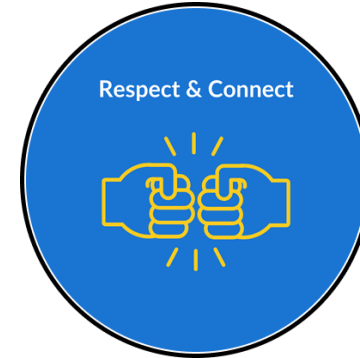
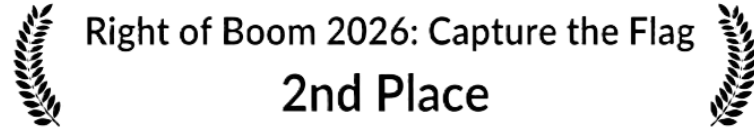
Over a dozen technical certificates.

**We live in the darkness, ”
so you don't have to.**

When your
technology Works,
**Your work gets
easier.**

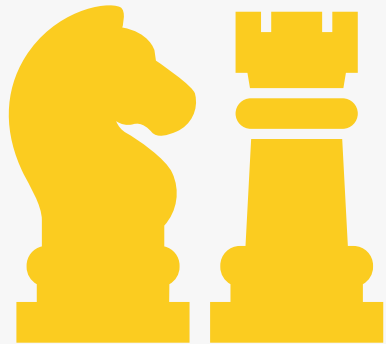


ABOUT



WHAT THIS IS INTENDED TO BE

High level,
strategic discussion



Suitable for
C-Suite



Not tactical,
not user focused



Agenda

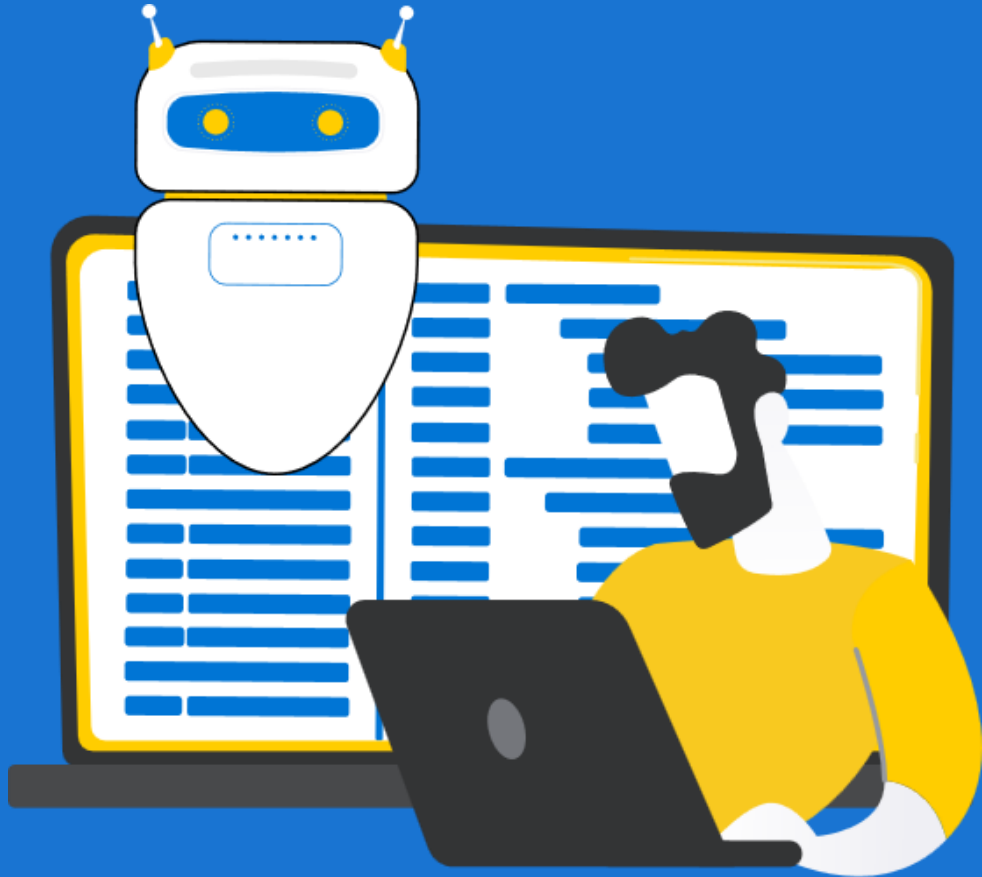
- 01 CISA Shutdown
- 02 Anthropic and Claude Code
- 03 Aura Identity Provider Breach
- 04 Another AI attack - Fortinet
- 05 Scam Centers
- 06 The Approach to Scammers
- 07 Summary
- 08 Q&A

CISA Shutdown



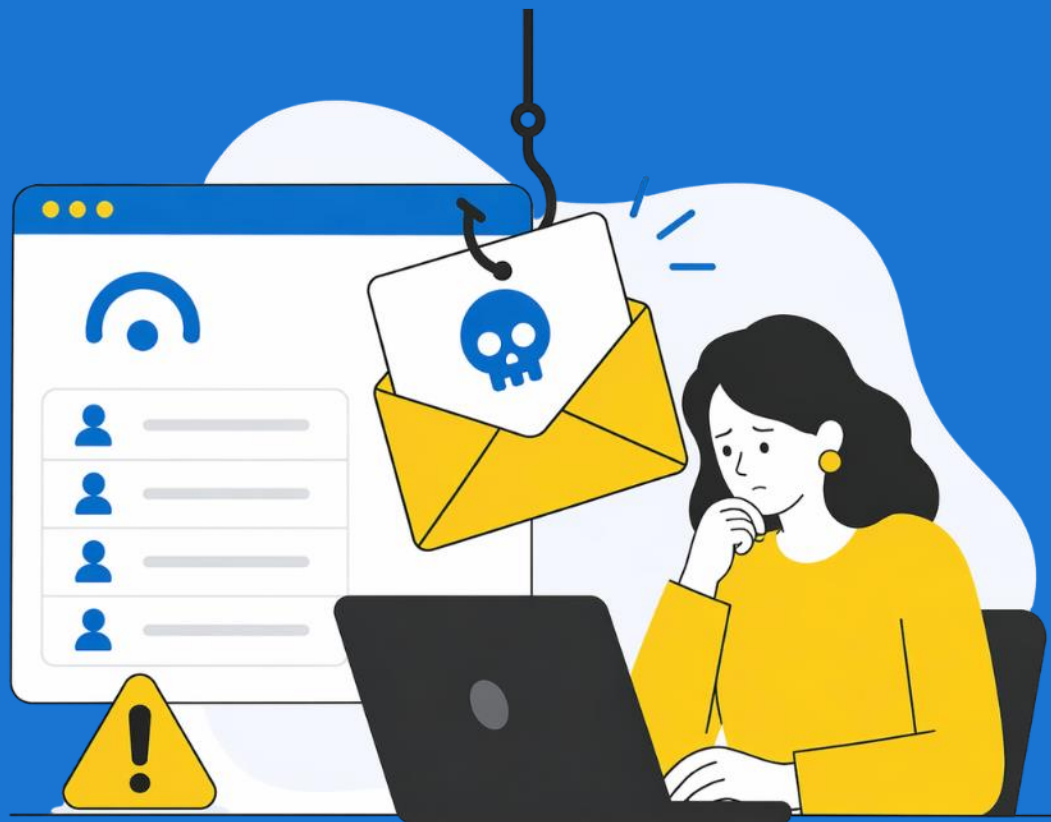
- CISA currently shut down
 - Like all government 'shutdowns', this means varying things
- What do we get from CISA?
- What does this mean specifically for American SMBs

Anthropic and Claude Code



- What happened?
 - Claude, Anthropic's AI assistant, had the portion of its code leaked that assists developers in programming.
 - [Anthropic accidentally exposes Claude Code source code](#)
 - [The Register](#) (link provided on the recording page)
- This is not the entire AI source code; only a portion of it (though it's a useful portion)
- This was not a security incident; this was human error
 - A phishing attack
- What does this mean for us? What does this mean for vendor validation?
 - "Commercially reasonable efforts"

Aura Identity Provider Breach



- Aura (an identity protection service) had a marketing list breached
 - <https://www.pcmag.com/news/no-the-aura-data-breach-did-not-expose-your-ssn-password-heres-what-happened>
- This came from a phishing attack, again.
- Aura says no customer information was accessed.
 - Like Oracle said [Oracle Tells Clients of Second Recent Hack, Log-In Data Stolen](#)
 - Like Co-Op said [Co-op forced to shut down part of IT system after hack attempt | Co-operative Group | The Guardian](#)
 - Like Marks and Spencer said [M&S apologises after 'cyber incident' hits contactless payments and online orders | Marks & Spencer | The Guardian](#)
- What does this mean for our personal information? What does this mean for our business information?

Another AI attack - Fortinet



- Attackers leveraged AI to compromise 600+ Fortinet devices
 - <https://cybersecuritynews.com/600-fortigate-devices-hacked/>
- Why is this different than normal 'scanning'?
- Security and its ever-changing nature, and what that means.
- Why no vendor is safe and what this will evolve into

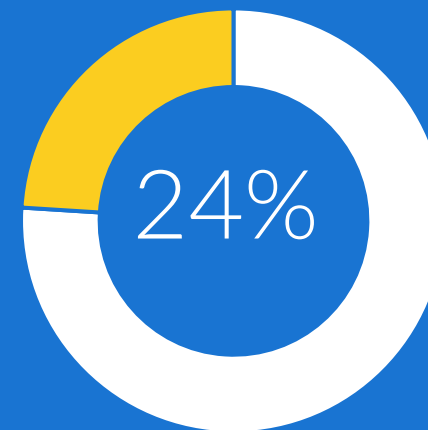
Article

Scam Centers

- The NYT did a spectacular article on a scam center in Myanmar
 - <https://www.nytimes.com/2026/01/13/world/asia/myanmar-scam-center.html>
- Highlights from the article
 - Target profile
 - Scamming methods
- How to help your friends and family

\$10B

stolen in 2024 alone from people who admitted it



Nearly 1 in 4 Americans have been manipulated into sharing personal information through scam emails, texts, or calls.

Pew Research Center

<https://www.pewresearch.org/internet/2025/07/31/online-scams-and-attacks-in-america-today/>

The Approach to Scammers

- There have been several takedowns
 - <https://www.pbs.org/newshour/world/myanmars-military-says-it-has-raided-a-second-major-online-scam-center>
- ...but not all of them appear to be useful
 - <https://www.wired.com/story/myanmar-kk-park-scam-compound-destruction/>
- What can governments do? What can we do?
 - Training, support for loved ones, awareness, and legal angles

Summary



Claude Code
and AI use in
business



Personal
information leaks,
and what to do

*Your information's on the Dark
Web*



AI in attacks
and what the
difference is
from the past



Scams and their
place in the
world

Summary Continued

People

The single most important piece



Process

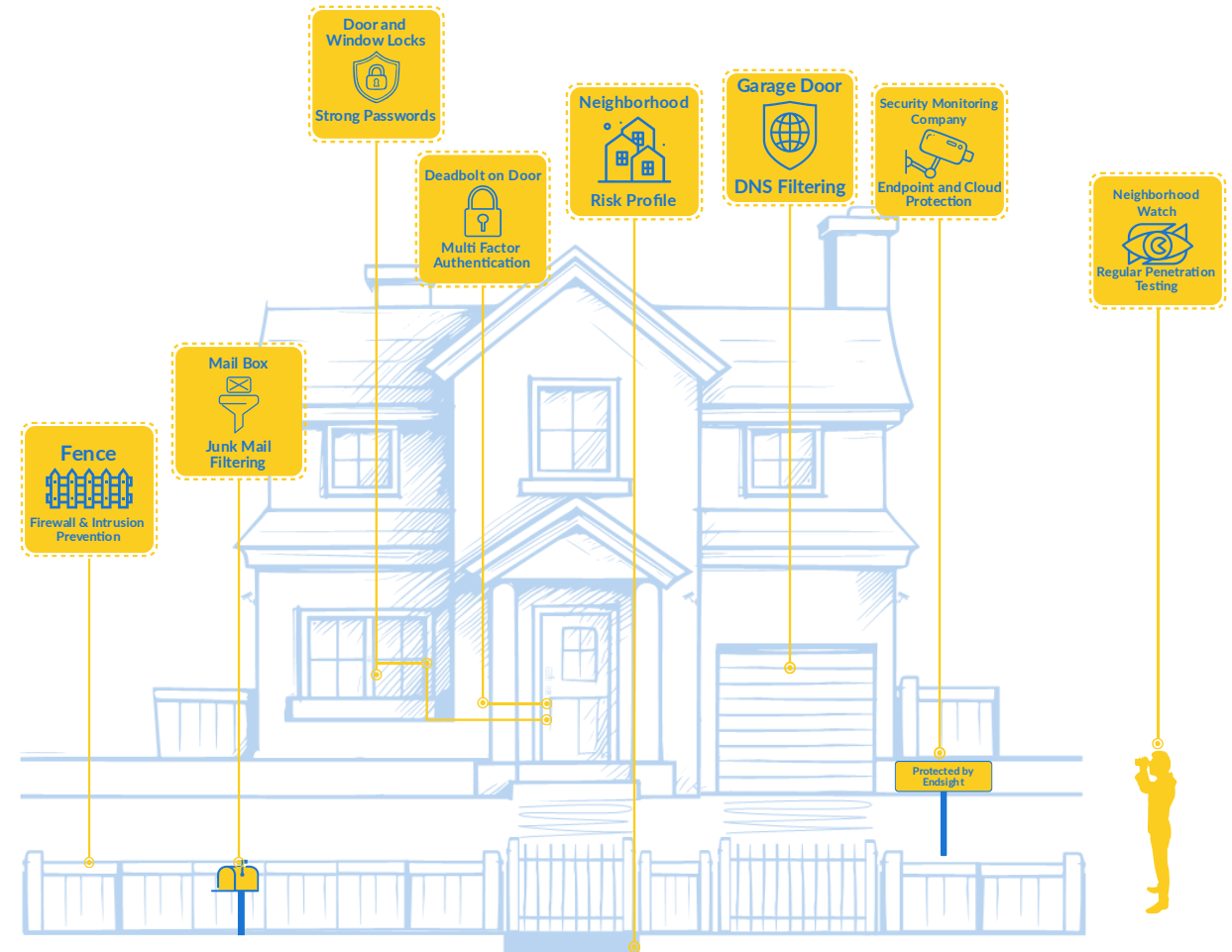


Technology



Defense in Depth

(People, Process, Technology)



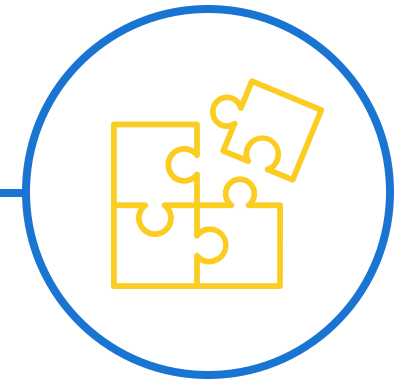
Is Your House in Order?



Contact your Client Strategy Manager or Sales Rep to schedule a call or fill out the form to meet now or later. **Note: If you choose “later,” we will reach out in mid-June.**



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



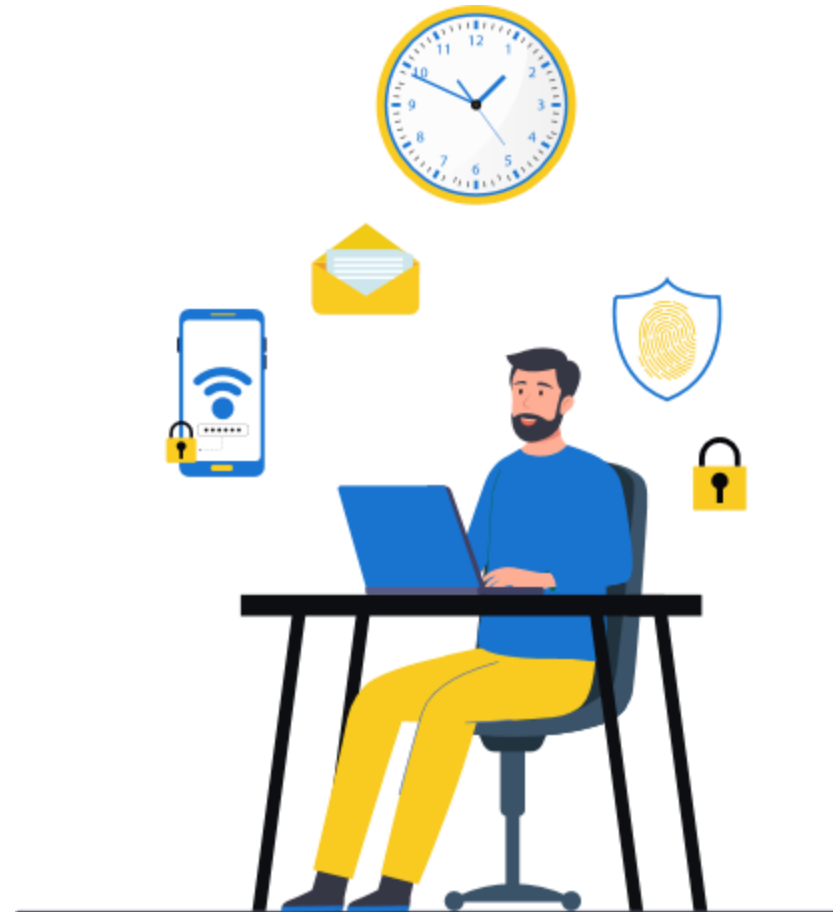
Work with us to remediate and mitigate the risks

Next Sessions

Q3: July 23rd @ 1 PM PST

Q4: October 22nd @ 1 PM PST *Tentative

- To register:
 - Scan the barcode
 - Go to: <https://get.endsight.net/cybersecurity/office/hours>
 - Email akreps@endsight.net to register
 - We can register you for the next one.
 - To register for all of the remaining 2026 sessions, please email akreps@endsight.net

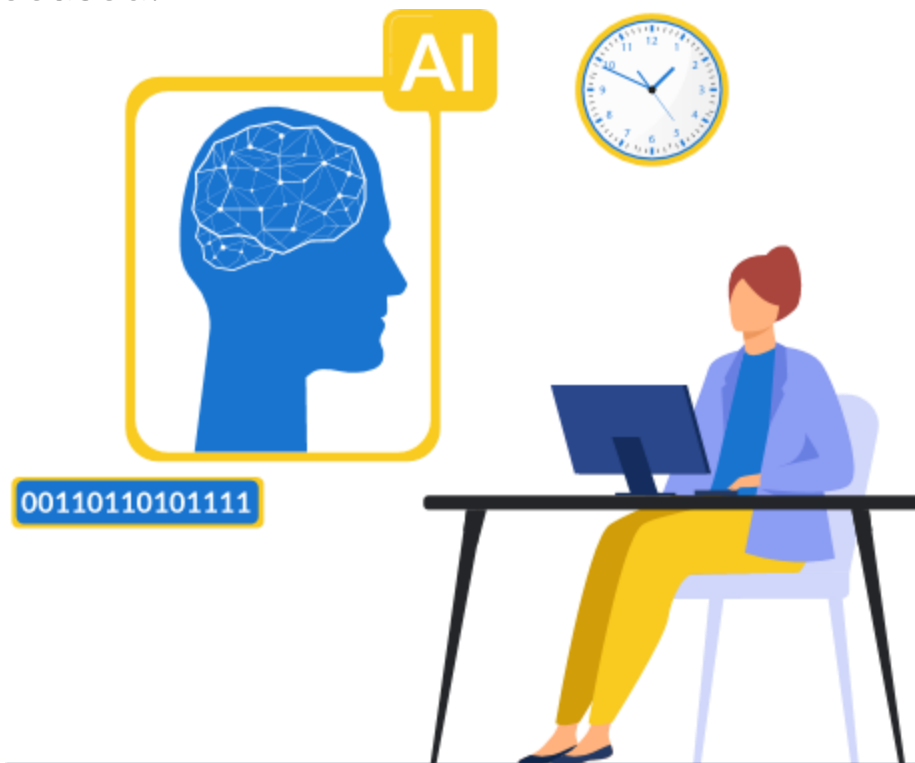


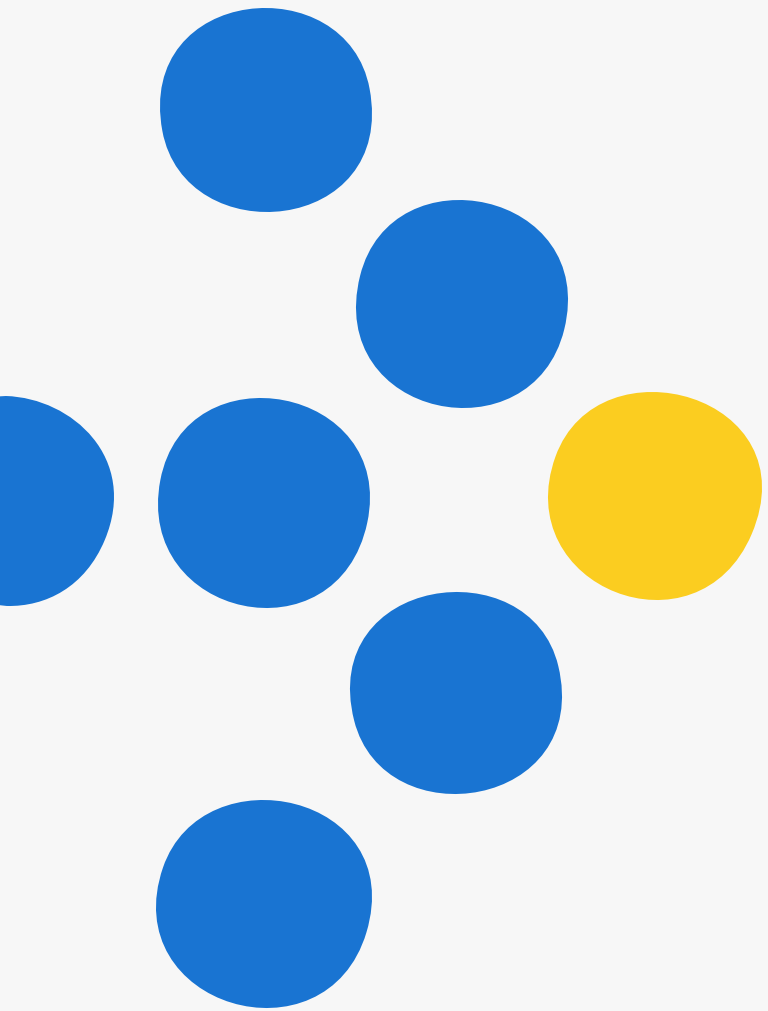
AI Office Hours

June 30th @ 1 PM PST.

Similar format to Security Office Hours, but AI focused.

- To register:
 - Scan the barcode
 - Go to: <https://www.endsight.net/development/webinar>
 - Email akreps@endsight.net to register





Q&A



Q&A

- AI websites and whether those websites can be redirected to enterprise subscriptions only, or is it sending users directly to the free versions of these software applications?
- For the past year or so I am getting a larger amount of spam/junk/etc. making its way into my yahoo email account Inbox. I've tried blocking and/or marking as junk, but the rate of the unwanted emails don't appear to abate much. Any suggestions? As for emails that have an unsubscribe link, I am reluctant to even press the unsubscribe link.



Stephen Hicks

CISSP, CCSP, CISM

Security Practice Manager

@ Endsight

Thank
you!

endsight