ENDSIGHT.NET

Cybersecurity **Office Hours** ***Chick-fil-A Edition***

Stephen Hicks, Security Practice Manager

Q3 2026

endsight

Stephen Hicks

Security Practice Manager

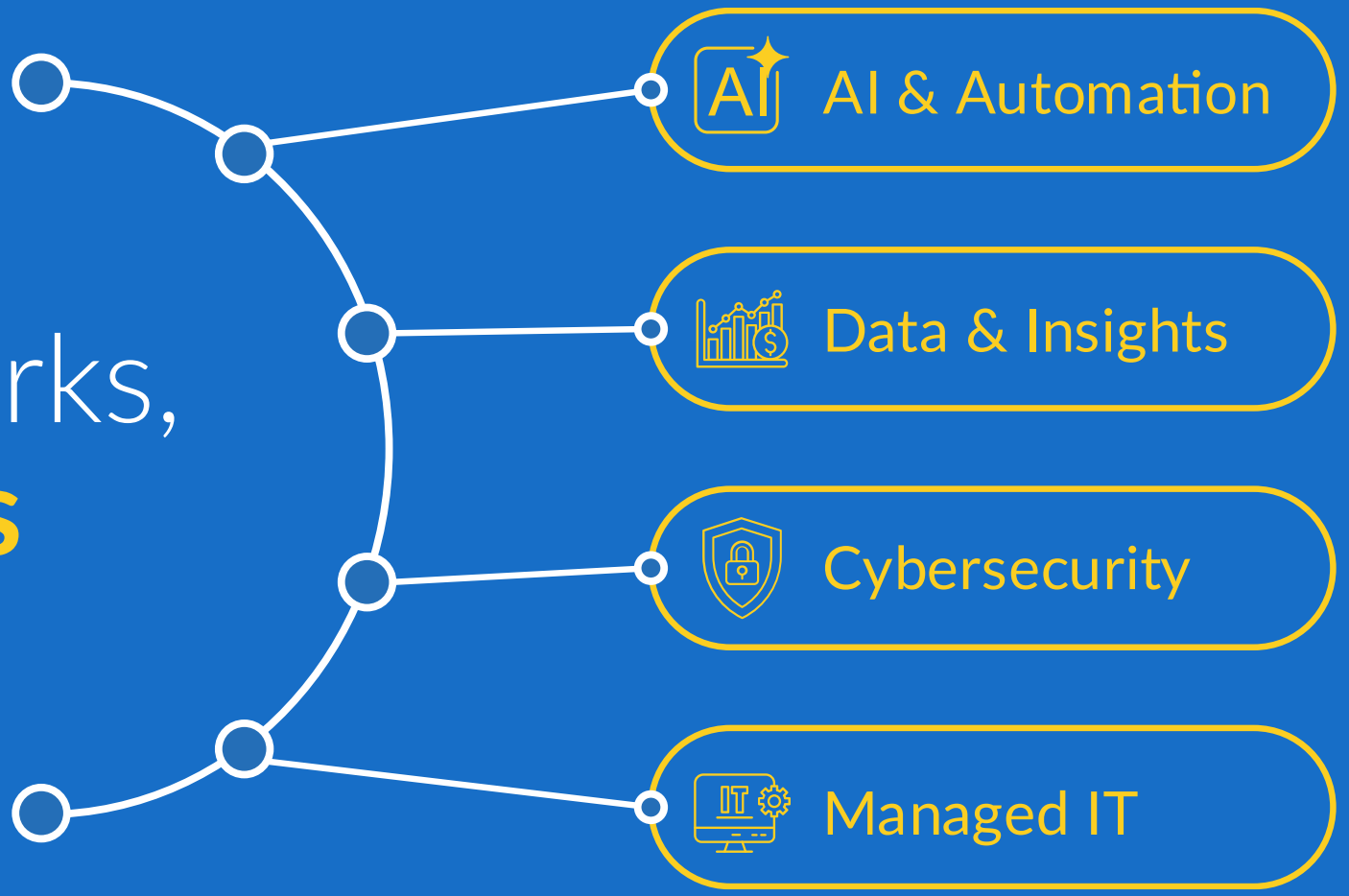
CISSP, CCSP, CISM

Phone Number: (510) 280-2036

Email: shicks@endsight.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.

When your technology Works,
Your work gets easier.



endsight

ABOUT

WINNER
Outstanding Growth Partner
endsight
PARTNER IMPACT AWARDS 2025

Right of Boom 2026: Capture the Flag
2nd Place

MSP 501
Channel Futures 2025

San Diego Business Journal
2025 TOP
TECHNOLOGY SOLUTION PROVIDERS

THE CHANNEL CO.
CRN FAST GROWTH 150
2025

THE CHANNEL CO.
CRN SOLUTION PROVIDER 500
2025

Respect & Connect

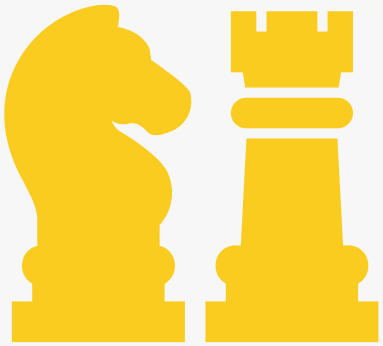
Servant's Heart

Value Value

Progress Over Comfort

WHAT THIS IS INTENDED TO BE

High level,
strategic discussion



Suitable for
C-Suite

Not tactical,
not user focused

Agenda

01 Anthropic and the US Government

02 Canvas Ransomware Attack

03 Windows Defender Zero-Day

04 Huntress and Breach Response

05 Summary

06 Q&A

Anthropic and the US Government

- What happened?
  - Anthropic was ordered to restrict usage of its two frontier models, Mythos and Fable, to only US citizens.
    - https://www.anthropic.com/news/fable-mythos-access
- Motivation for doing this aside, this is still a supply chain threat
- The CIA triad: Confidentiality, Integrity, and Availability
  - The main data attributes security is trying to protect
  - This is an Availability threat
    - ...and some would say AI is a confidentiality threat (they're correct)
- How do we handle and plan for this?

Planning for Supply Chain Risks

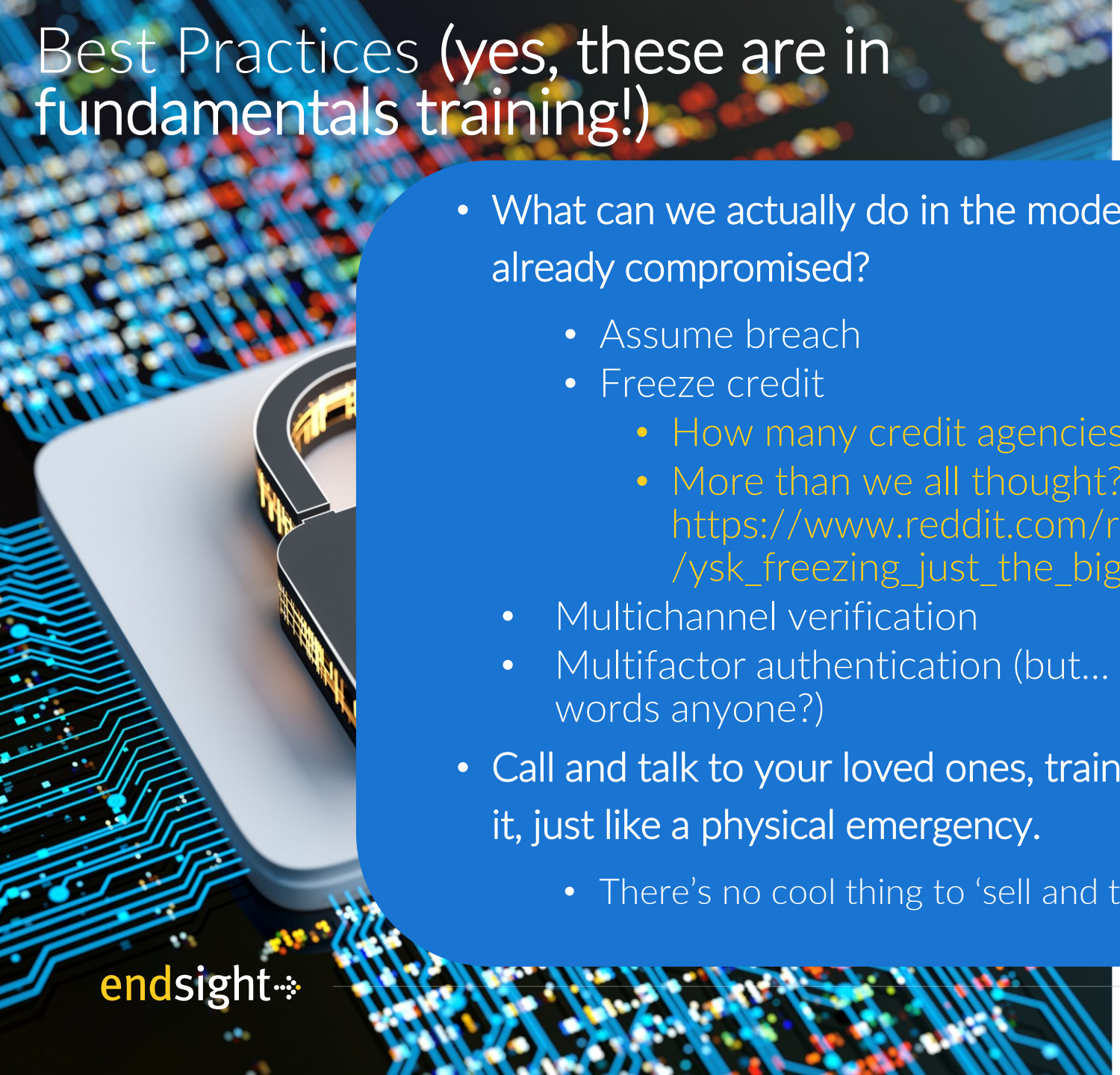
- Addressing risk:
  - Avoid
  - Mitigate
  - Transfer
  - Accept
- This is also known (tangentially) as TPRM – Third Party Risk Management
  - Frequently disregarded or postponed
- There are many inexpensive ways to plan for third party risks:
  - Tabletop exercises
  - Live failure demonstrations
  - Alterative suppliers (sometimes, but not always feasible)
- What risks are you accepting at your organization without knowing it?

Canvas Ransomware Attack

- Canvas suffered a major ransomware attack in May
  - https://www.staysafeonline.org/articles/canvas-data-breach (For parents/teachers/students)
- What did they get?
  - https://www.fisherphillips.com/en/insights/insights/the-canvas-breach-what-educational-institutions-need-to-know-and-how-you-can-respond quite a bit.
    - Student IDs (ever use your SSN for an ID?)
    - Names
    - Addresses
    - Personal messages
- What does this mean?
  - Downtime, obviously
  - Compromised PII
  - Credit monitoring
- Why am I even telling you this?
  - What can we actually do? Third party breaches are commonplace.

endsight

Best Practices (yes, these are in fundamentals training!)



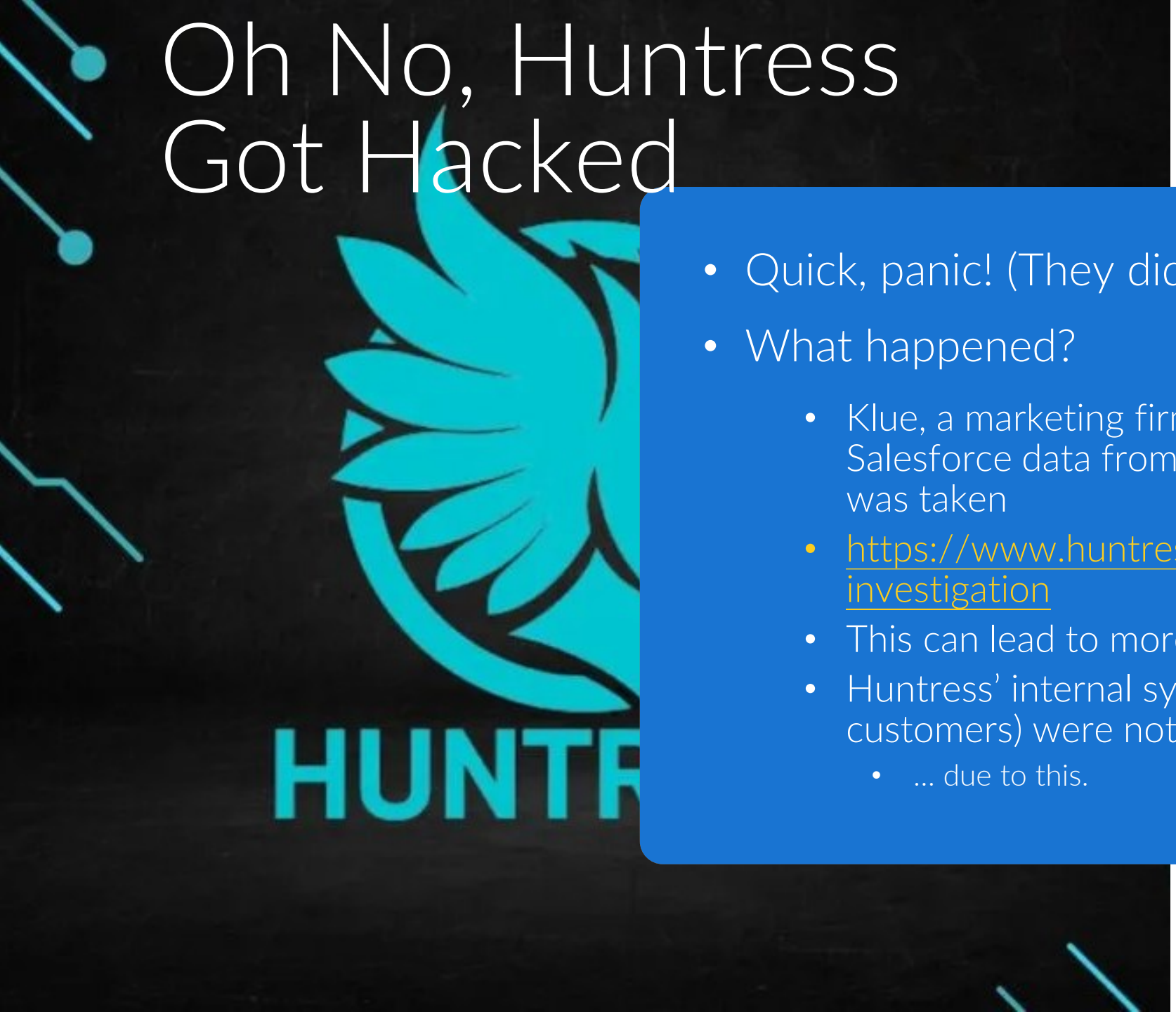
- What can we actually do in the modern world when our information is already compromised?
  - Assume breach
  - Freeze credit
    - How many credit agencies are there?
    - More than we all thought? https://www.reddit.com/r/YouShouldKnow/comments/1qfiyrd/ysk_freezing_just_the_big_3_credit_bureaus_isnt/
  - Multichannel verification
  - Multifactor authentication (but… maybe not technologically. Code words anyone?)
- Call and talk to your loved ones, train your employees, make a plan and test it, just like a physical emergency.
  - There's no cool thing to 'sell and turn on' that fixes this

Maybe Don’t Upset the Hackers

- The backstory – an upset researcher with a vendetta
  - *https://labs.cloudsecurityalliance.org/research/csa-research-note-defender-zero-days*
  - https://www.youtube.com/watch?v=phsRA-_DDwE
- What is ‘responsible disclosure’?
- Is my company vulnerable?
- Is Endsight pivoting solutions based on this?
- What does ‘vulnerability management’ mean?
- Who would like to know what your company is using AI for?

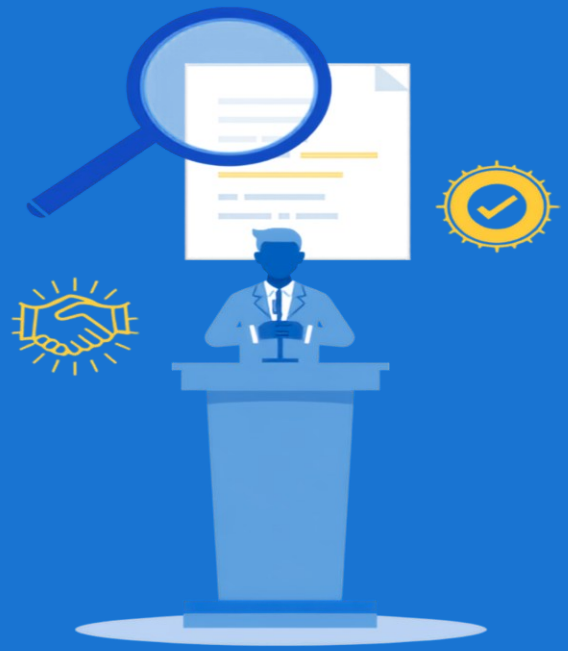
endsight

Oh No, Huntress Got Hacked



- Quick, panic! (They didn't get hacked)
- What happened?
  - Klue, a marketing firm, was compromised, and Salesforce data from Huntress, and other vendors, was taken
  - https://www.huntress.com/blog/klue-breach-investigation
  - This can lead to more social engineering attacks
  - Huntress' internal systems (and other Klue customers) were not breached
    - … due to this.

How to Deal with a Breach



- Huntress told us about this before anyone else did
  - That's huge, and generates trust
- They have fully detailed their approach publicly
- A third-party investigation firm was enlisted to assist
- They've kept us up to date and have even done interviews
- This is a model for how we evaluate 'good' companies during vendor analysis
  - What is OSINT?

Summary

Anthropic, AI, and supply chain risk

Canvas and third-party breaches

Best practices when your data is already out there

Microsoft and responsible disclosure

Huntress and how to handle a breach well

Summary Continued

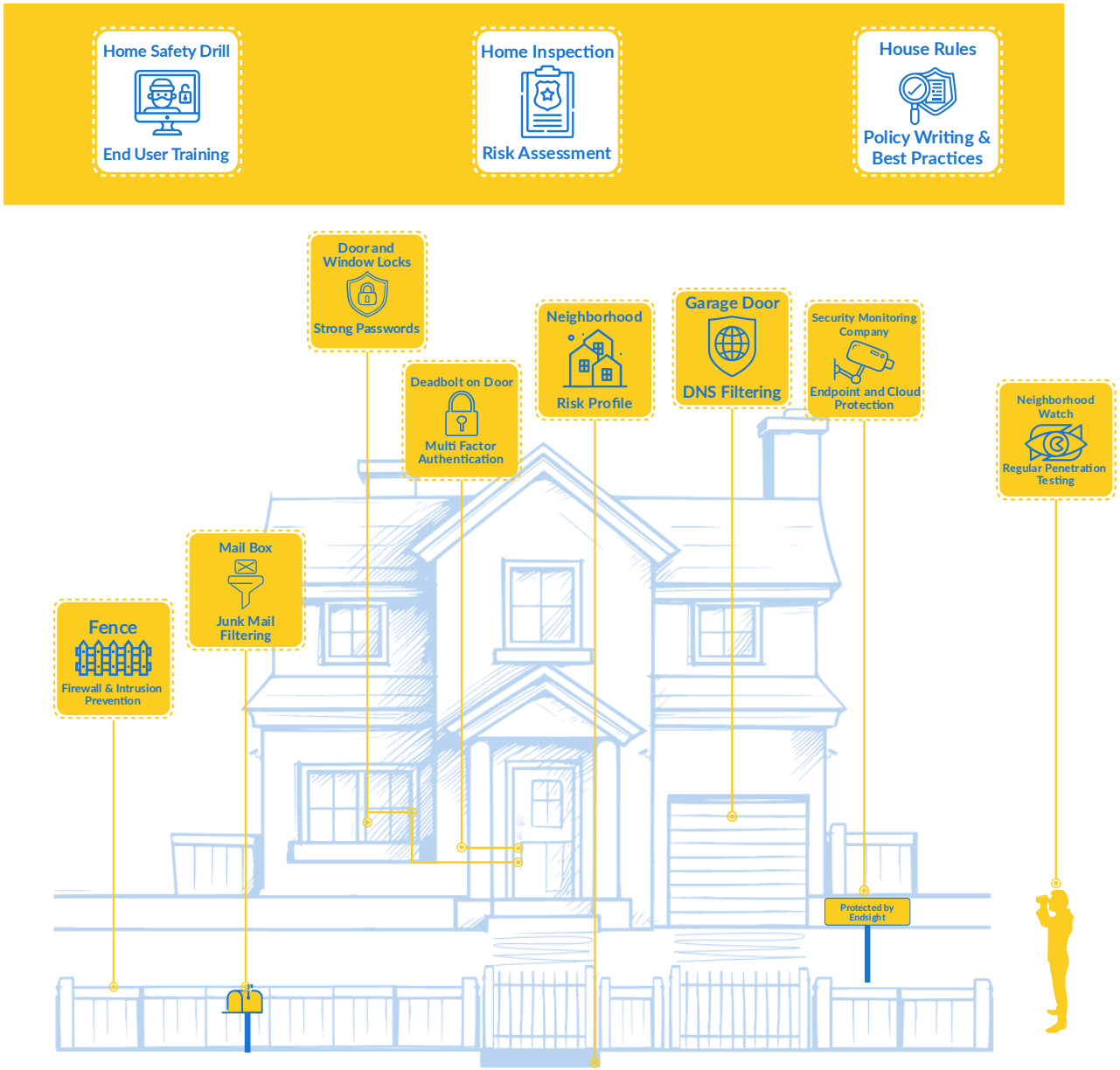
People
The single most important piece

Process

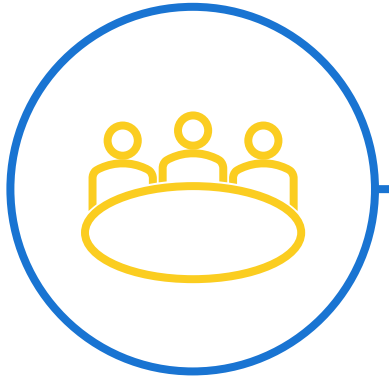
Technology

Defense in Depth

(People, Process, Technology)

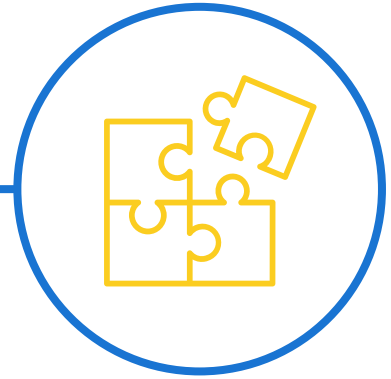


Is Your House in Order?



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’ll reach out in 45 days.

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 Session

October 22nd @ 1 PM PST.

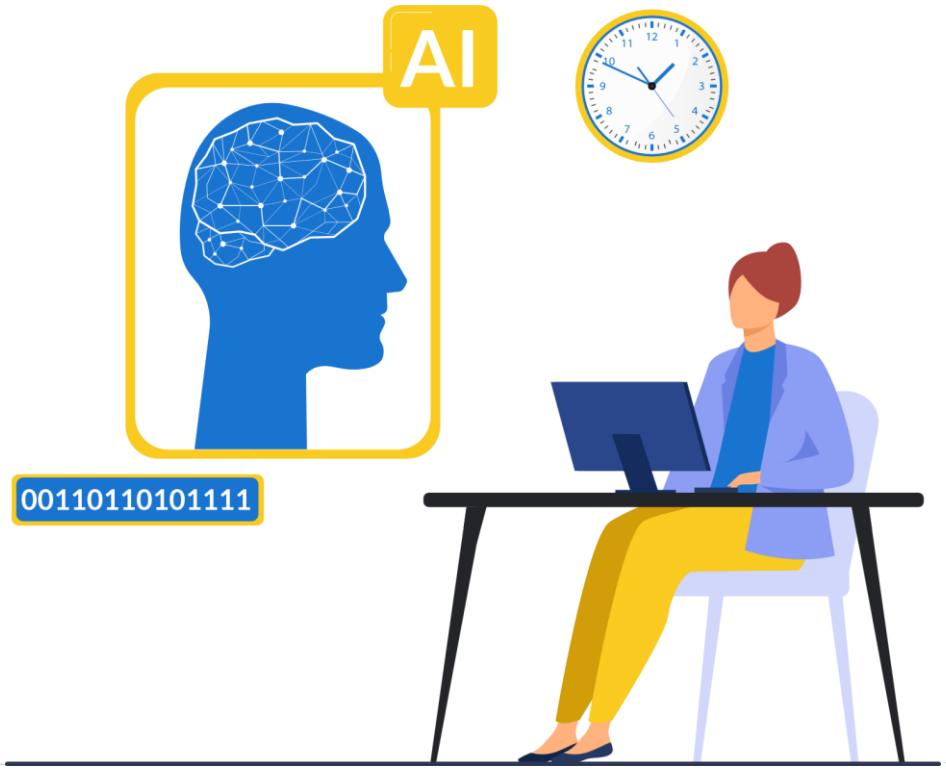
- To register:
  - Scan the barcode
  - Go to: https://get.endsight.net/cybersecurity/office/hours
  - Email akreps@endsight.net to register
    - We can register you for the next one.

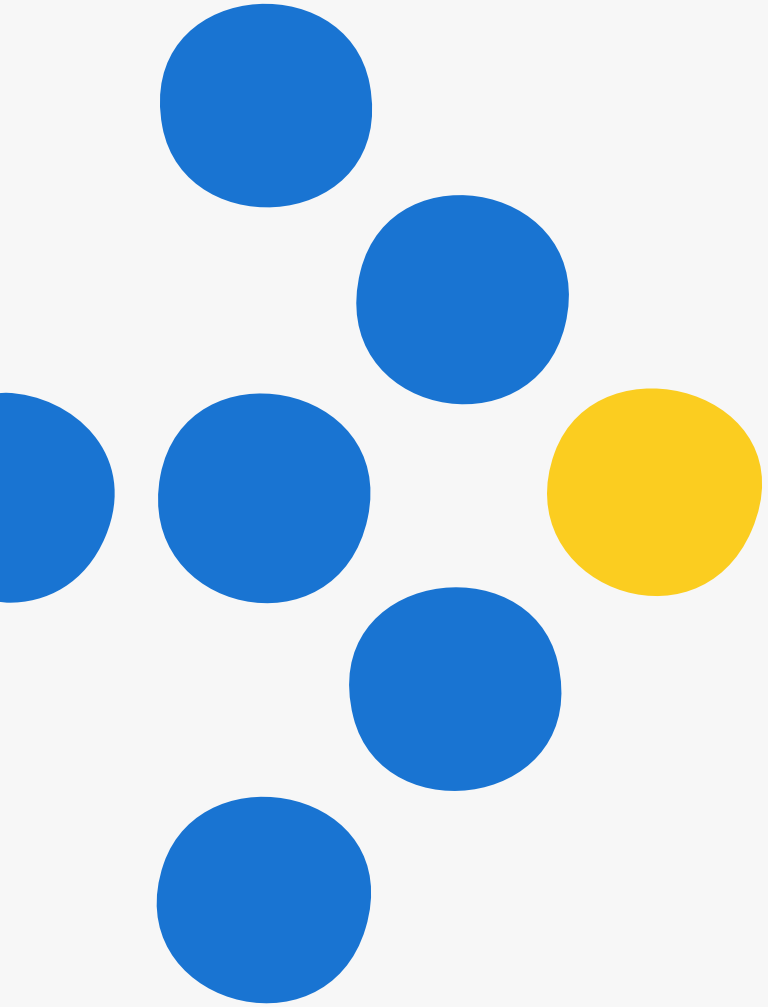
AI Office Hours

September 10th @ 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

1) Are videos and quizzes really the best way to train end users on cybersecurity these days?
2) I saw that OpenAI accidentally hacked another company without any human involvement. How worried should we be about this kind of thing?

Stephen Hicks

CISSP, CCSP, CISM

Security Practice Manager

@Endsight

Thank you!

endsight