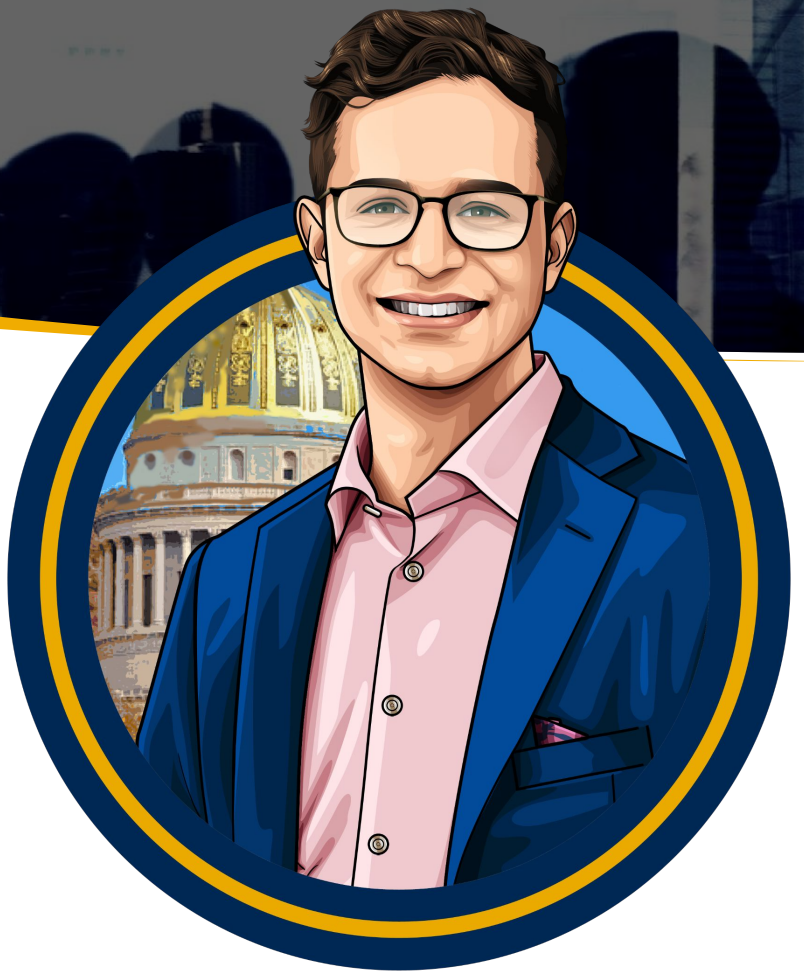
Threat Hunting for Dummies

Nate Hicks

\whoami

- Lead Threat Hunter - Global Payments
- Eight years of experience in security analysis
- Husband, Hacker, Internet Introvert
- Missing Persons CTF Judge/Contestant

#osint4good



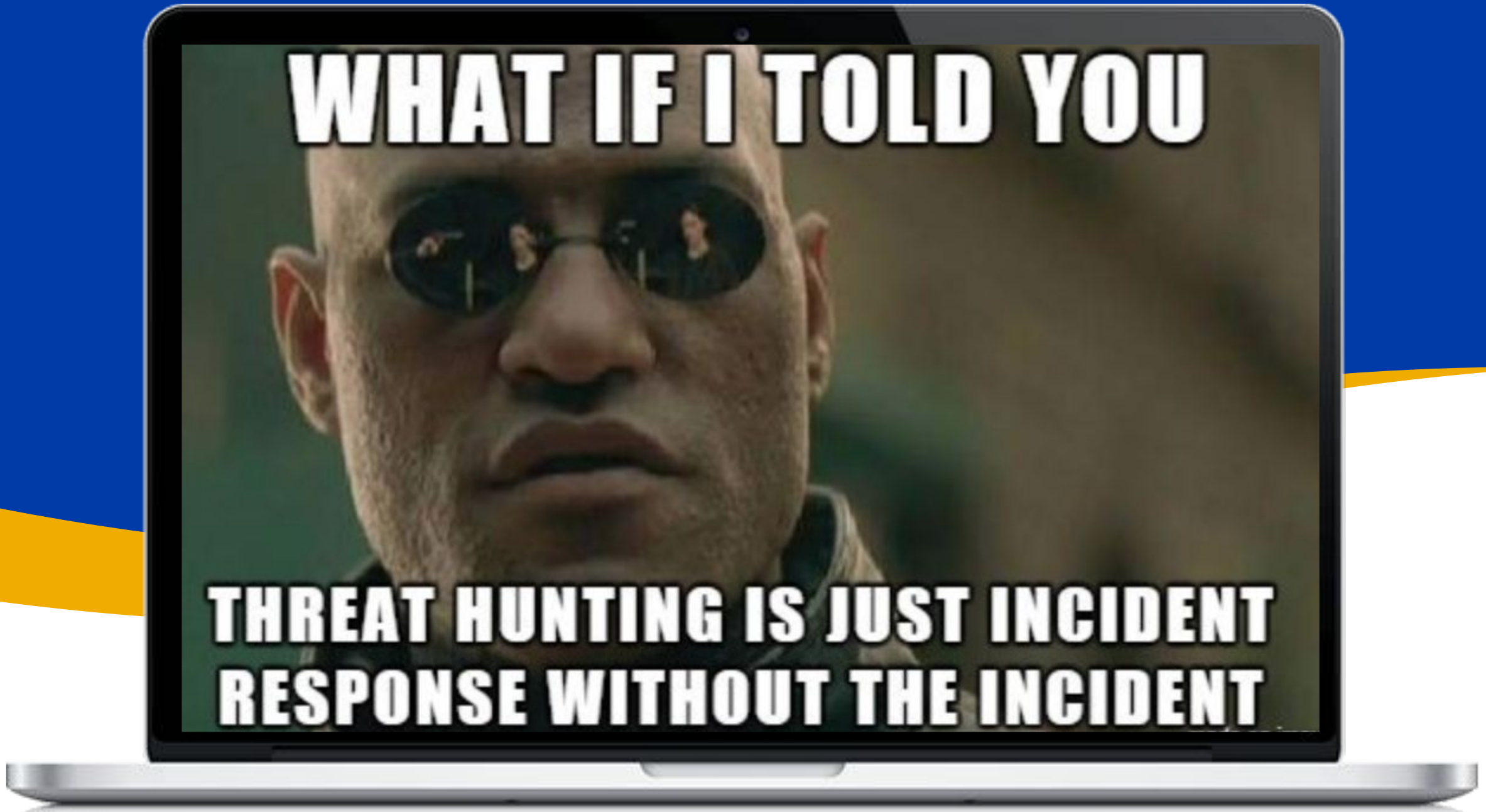
Agenda

1. What is Threat Hunting?
2. Why Threat Hunt?
3. Common Pitfalls and Mistakes
4. Questions

“It's easy to mistake familiarity with computers for intelligence, but computer literate certainly doesn't equal smart. And computer illiterate sure doesn't mean stupid.

Which do we need more: computer literacy or literacy?”

- Cliff Stoll, The Cuckoo’s Egg


WHAT IF I TOLD YOU
THREAT HUNTING IS JUST INCIDENT RESPONSE WITHOUT THE INCIDENT

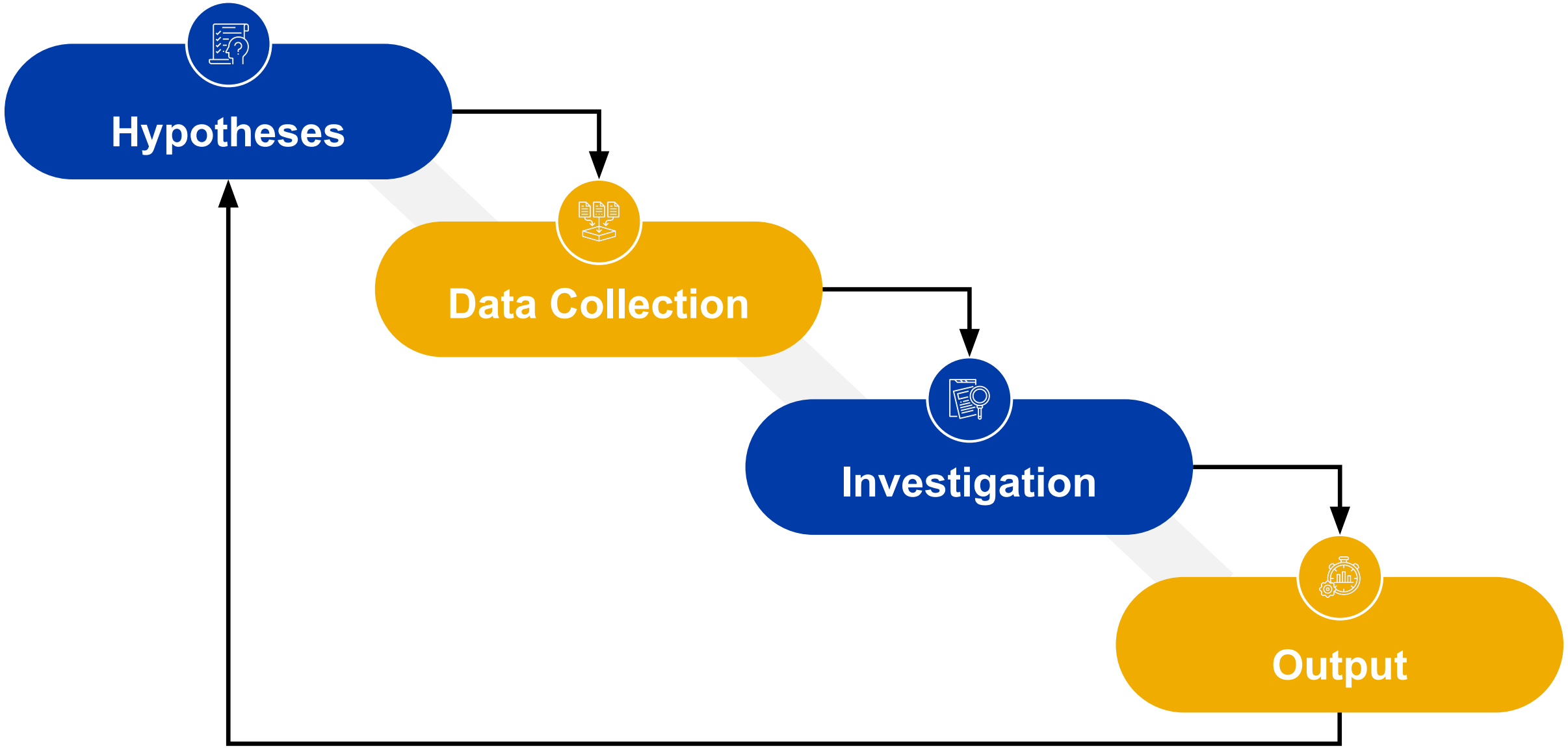
What is Threat Hunting?

Proactive vs Reactive

Validation of Compromise

Human Driven & Tool Oriented

What is Threat Hunting?

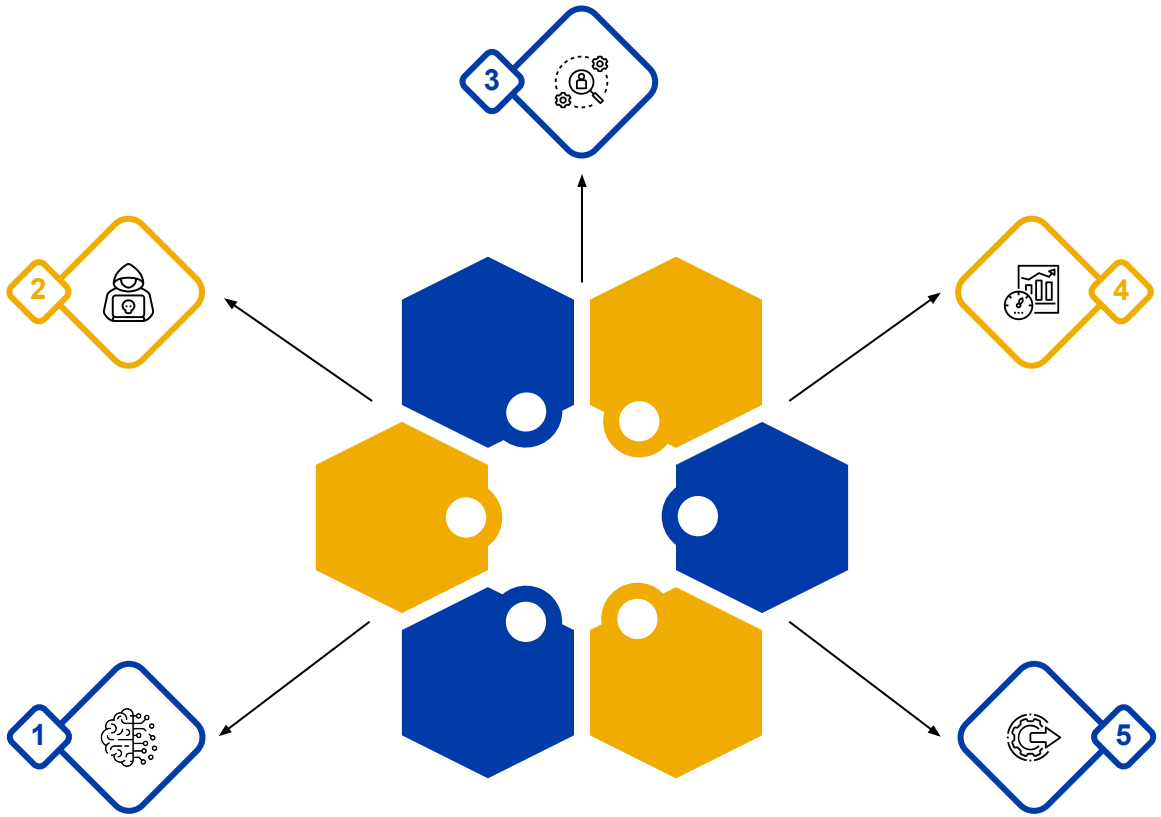


What is important to Threat Hunting?

Characteristics of an Analyst

Adversarial Mindset

Intelligence Driven



TTPs vs IOCs

Outputs

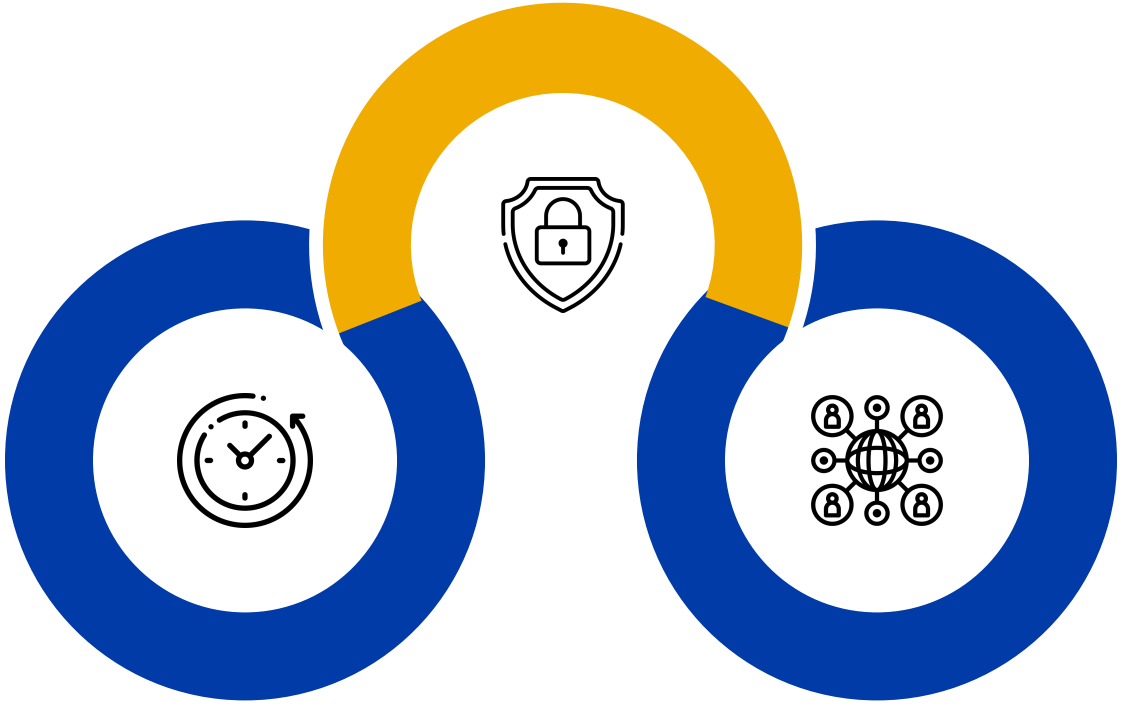
82%

Organizations with a breach involved the human element in **2022**

Why Threat Hunt?

Dwell Time Reduction

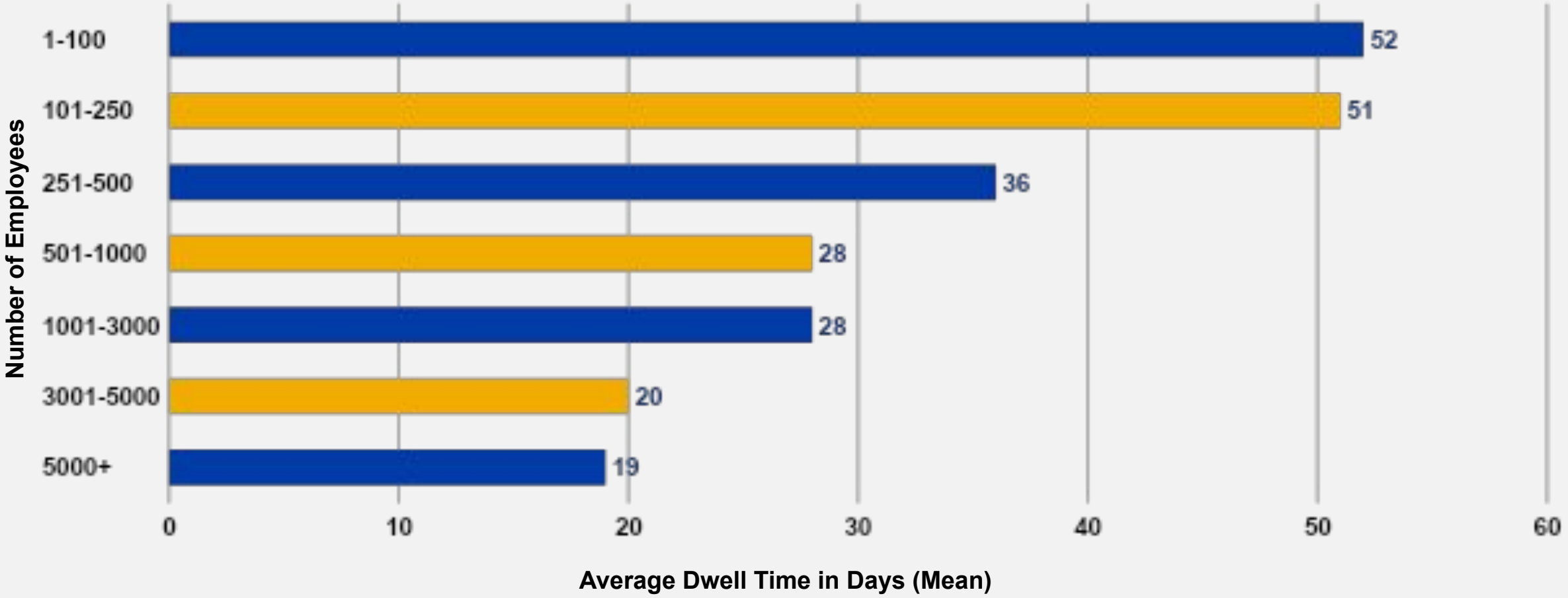
Fills security control gaps



Networks are unique and change

Why Threat Hunt?

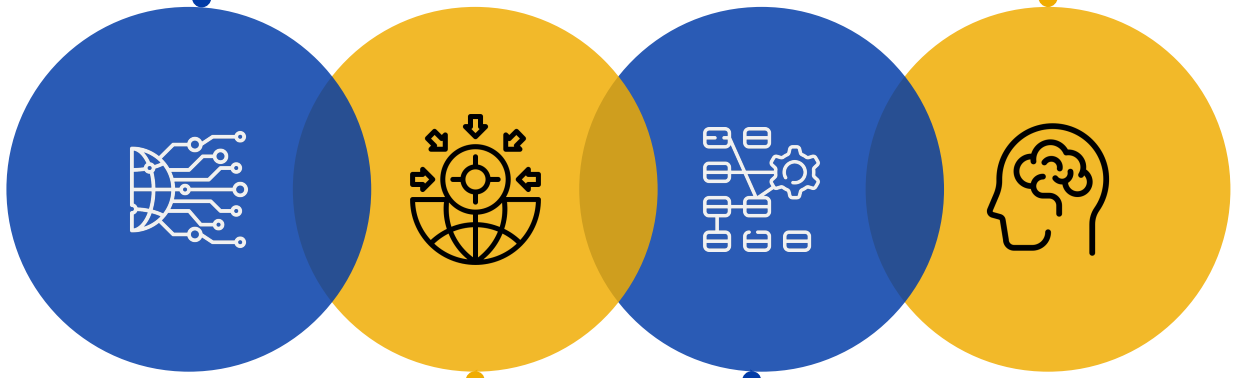
Intruder Dwell Time by Company Size (Mean)



Why Threat Hunt?

People focused security solution

Humans are better at catching humans than computers



Threats can look like legitimate activity

Increase of attack sophistication

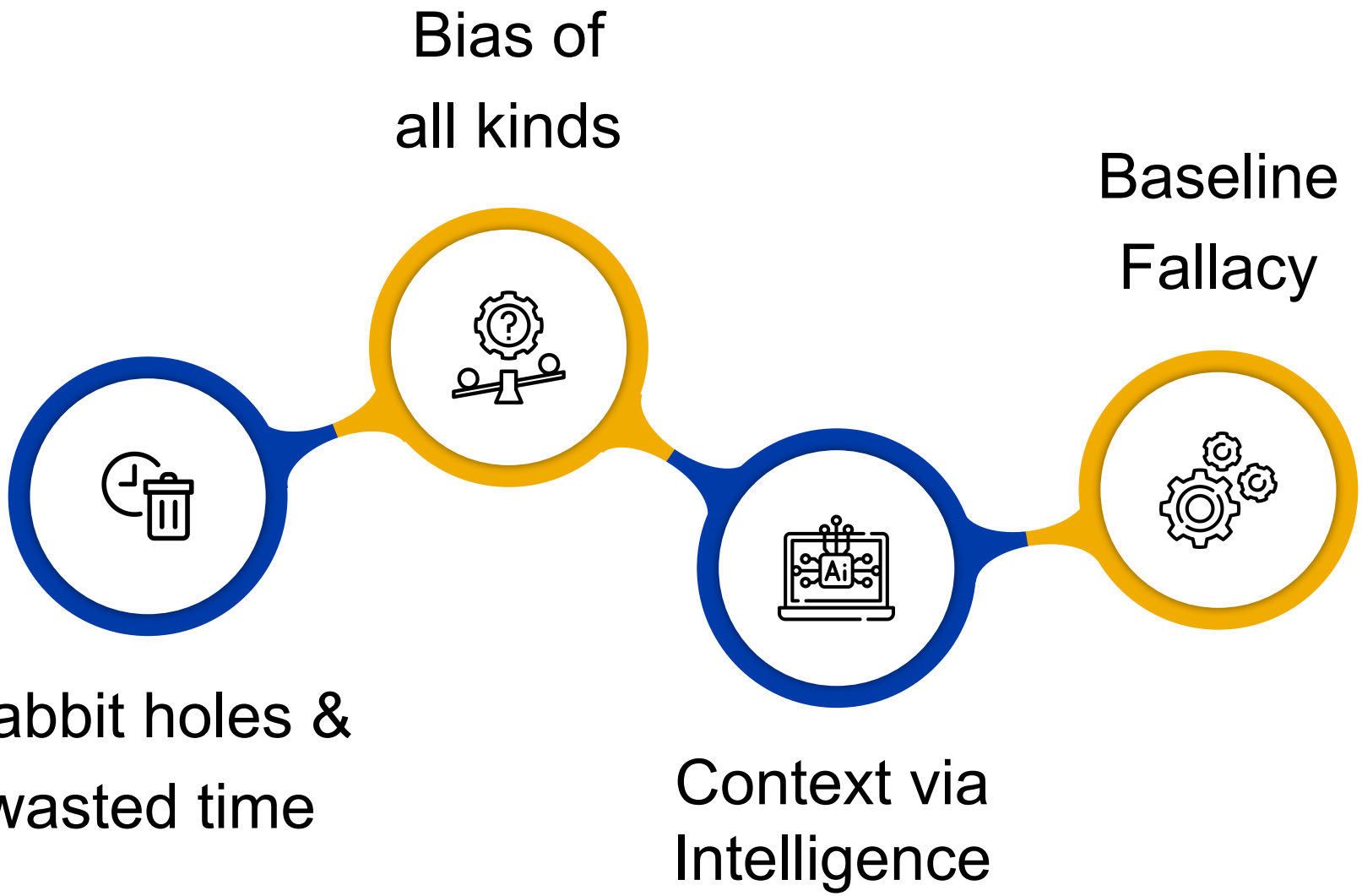
Pitfalls and Mistakes

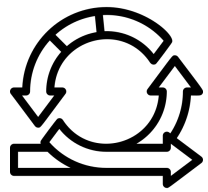
Where do you start?

AI/ML is not a silver bullet

Ad-Hoc hunting

Pitfalls and Mistakes





Different perspectives and backgrounds are more likely to benefit an organization.

A proactive approach to security analysis is required to accurately detect and get ahead of attacks.

Questions?

Thanks!

Links/Contact Information

Email:

nph1016@hotmail.com

LinkedIn:

www.linkedin.com/in/nathan-hicks-33027762/

GitHub:

github.com/goghoti/

Citations

Hylender, Dave. Verizon, New York, NY, 2022, pp. 8–9, *Verizon 2021 Data Breach Investigations Report*.

Sqrrl Team. Sqrrl, pp. 2–3, *A Framework for Cyber Threat Hunting - The Hunting Loop*.

Shier, Written by John. “The Active Adversary Playbook 2022.” *Sophos News*, 7 June 2022, https://news.sophos.com/en-us/2022/06/07/active-adversary-playbook-2022/.

Magma: A Framework for Threat Hunting, https://www.betaalvereniging.nl/wp-content/uploads/FI-ISAC-use-case-framework-verkorte-versie.pdf.

Lee, Robert M, and Rob Lee. “The Who, What, Where, When, Why and How of Effective Threat Hunting.” *SANS Institute*, 2016, https://www.sans.org/white-papers/who-what-where-when-why-how-effective-threat-hunting/.