KnowBe4
Human error. Conquered.

A Look Behind The Curtain: Open Source Intelligence (OSINT) Hacking Data Sources That Bad Guys Use!

A conversation with Kevin Mitnick

Kevin Mitnick
Chief Hacking Officer
KnowBe4, Inc.

Perry Carpenter
Chief Evangelist & Strategy Officer
KnowBe4, Inc.

About today's format…

This is not your typical webinar

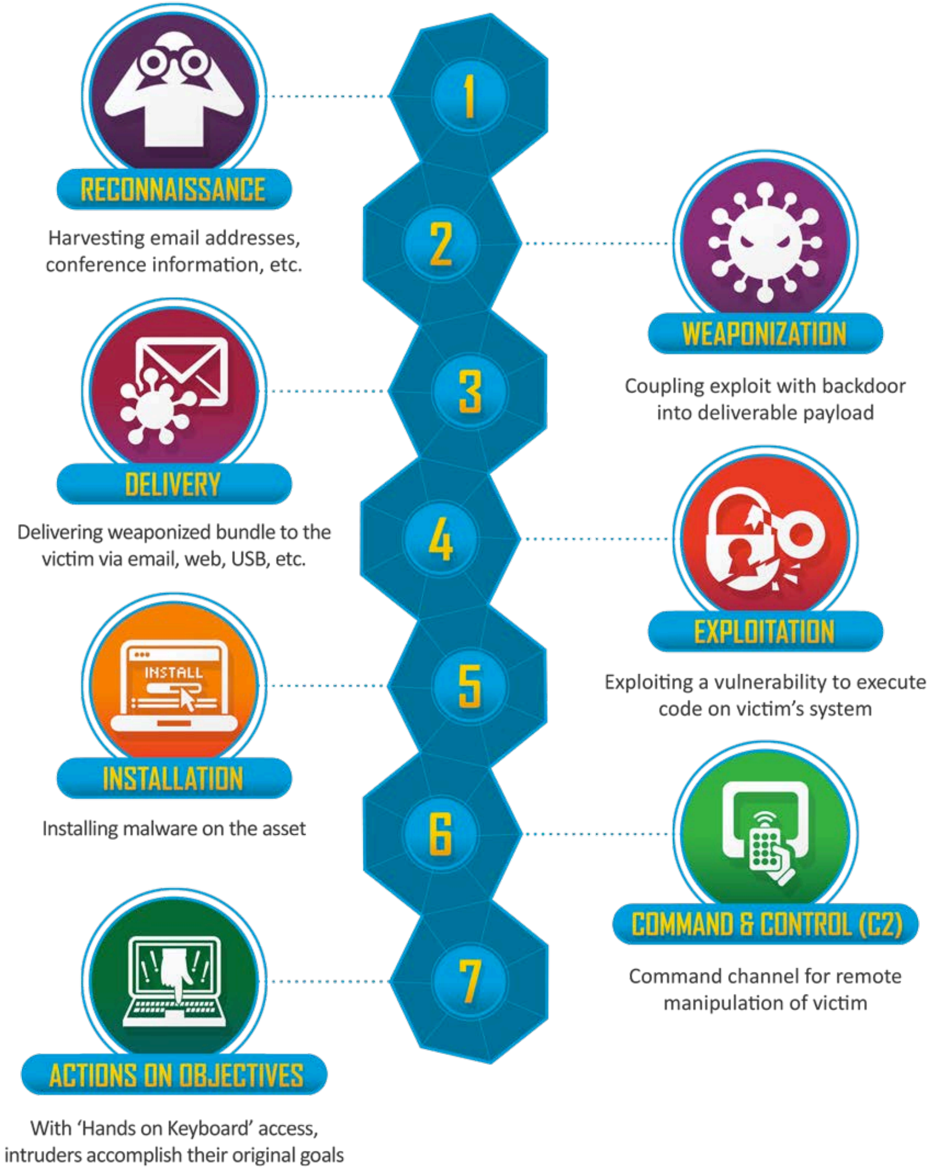
Kevin Mitnick
Chief Hacking Officer
KnowBe4, Inc.

Perry Carpenter
Chief Evangelist & Strategy Officer
KnowBe4, Inc.

KnowBe4
Human error. Conquered.

Understanding the Cyber Kill Chain

Attackers generally follow these steps to compromise an organization



1 RECONNAISSANCE
Harvesting email addresses, conference information, etc.

2 WEAPONIZATION
Coupling exploit with backdoor into deliverable payload

3 DELIVERY
Delivering weaponized bundle to the victim via email, web, USB, etc.

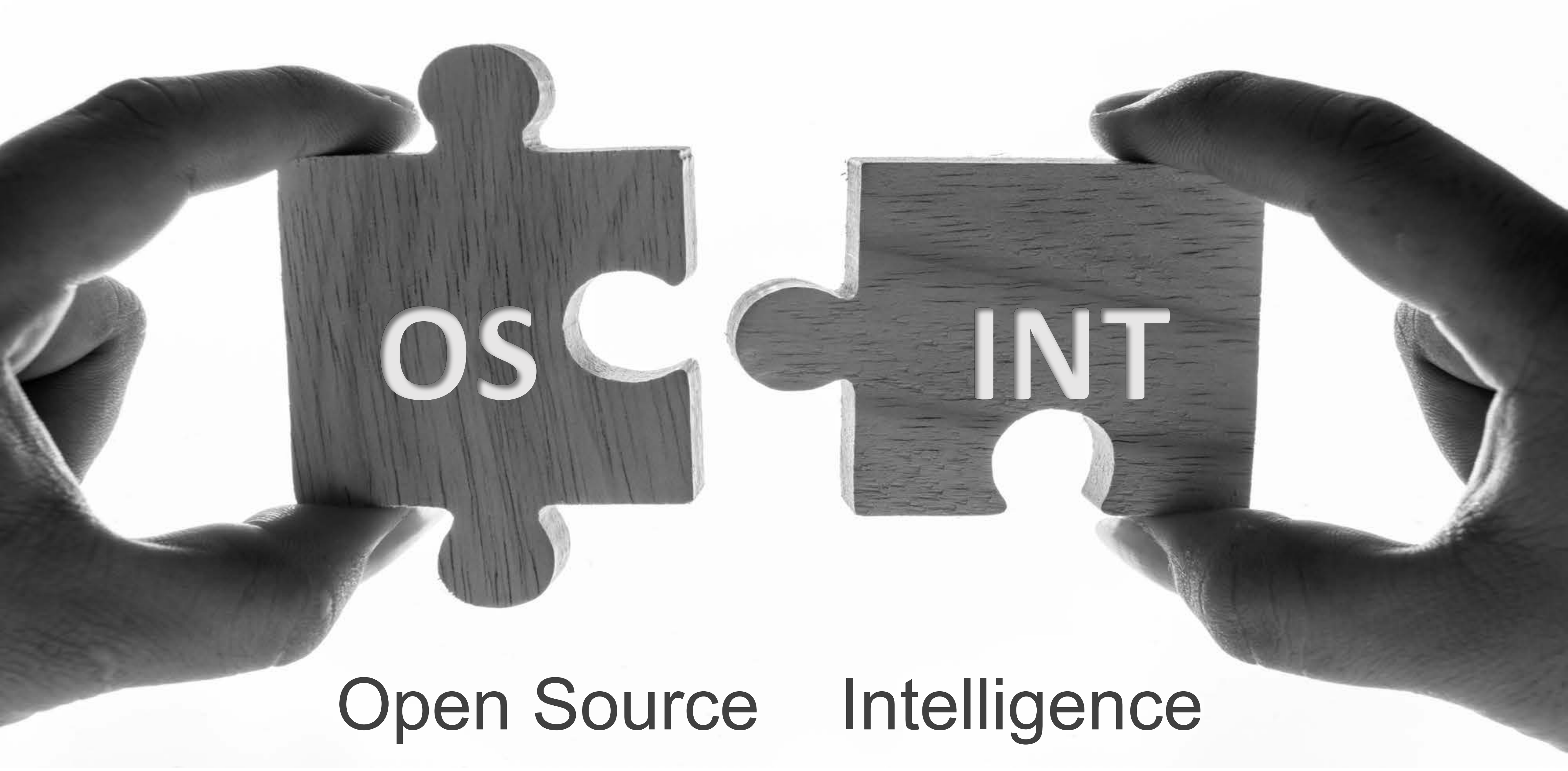
4 EXPLOITATION
Exploiting a vulnerability to execute code on victim's system

5 INSTALLATION
Installing malware on the asset

6 COMMAND & CONTROL (C2)
Command channel for remote manipulation of victim

7 ACTIONS ON OBJECTIVES
With 'Hands on Keyboard' access, intruders accomplish their original goals

http://www.lockheedmartin.com/us/what-we-do/aerospace-defense/cyber/cyber-kill-chain.html



Open Source Intelligence

OSINT 101:

- Why use it?
- Where does it fit in with a pen-test or a real attack?
- What data is available?
- Where can I go to collect OSINT?
- What are the best tools?

OSINT in Action

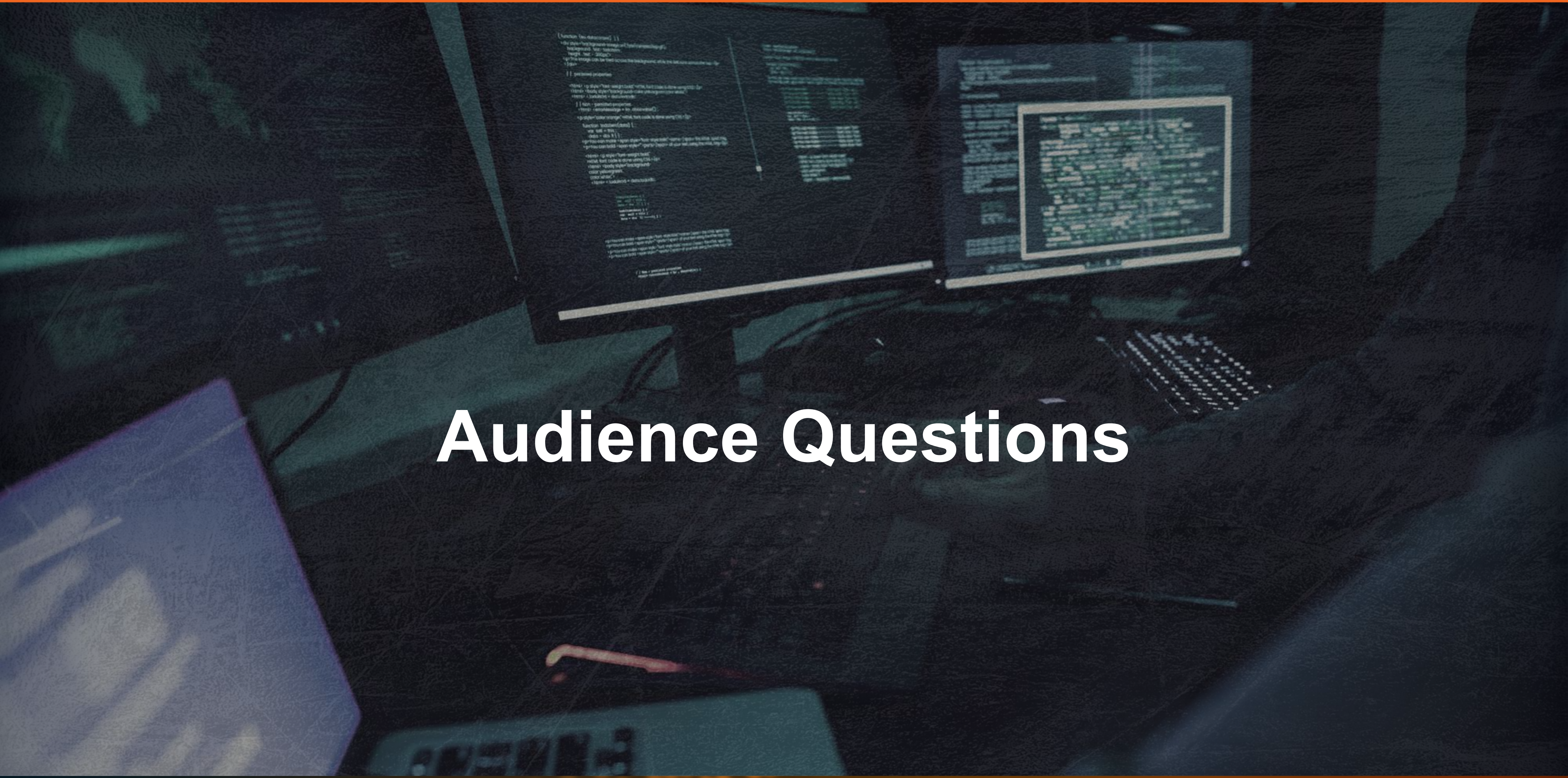
Demonstrating the Reality

- LinkedIn scraping
- Gitrob – code repositories
- Pipl search – personal public data
- Intel Techniques – public databases (MelissaData)
- WeLeakInfo.com – leaked passwords
- Vital Search - mother's maiden name

Protect Your Organization’s Secret Credentials

- Never store any credentials in code or in configuration files that you commit to Github.
- Don’t forget that hardcoded passwords, credentials, API keys, or other secret tokens may be stored in deleted branches or files. You must audit deleted commits as well.
- Require 2FA (two-factor authentication) for all GitHub console access.
- Remove any unused personal GitHub access tokens
- Rotate ssh private keys and Github personal tokens on a periodic basis.

How can organizations protect their users?



Audience Questions

Final Thoughts & Takeaways

Thank You

KnowBe4

Human error. Conquered.