



AI in InfoSec...and
birding!

@THEPACKETRAT



Why birding? (or is it birbing?)

- Can start by just looking out the window
- Birds are everywhere, and they're (mostly real)
- Gets even indoorsy people outside
- Community of (mostly) friendly people willing to share knowledge (BoF)
- Improves visual and analytic skills
- Citizen science—little contributions of knowledge and action have an impact
- Serotonin



Birding: Real-life Pokemòn

- Gotta (see) 'em all
- Birding apps are your Pokedex
- Camera or binoculars are your Poke Ball
- Life list is your score



The first dose is free.
It doesn't have to get (this)
expensive...



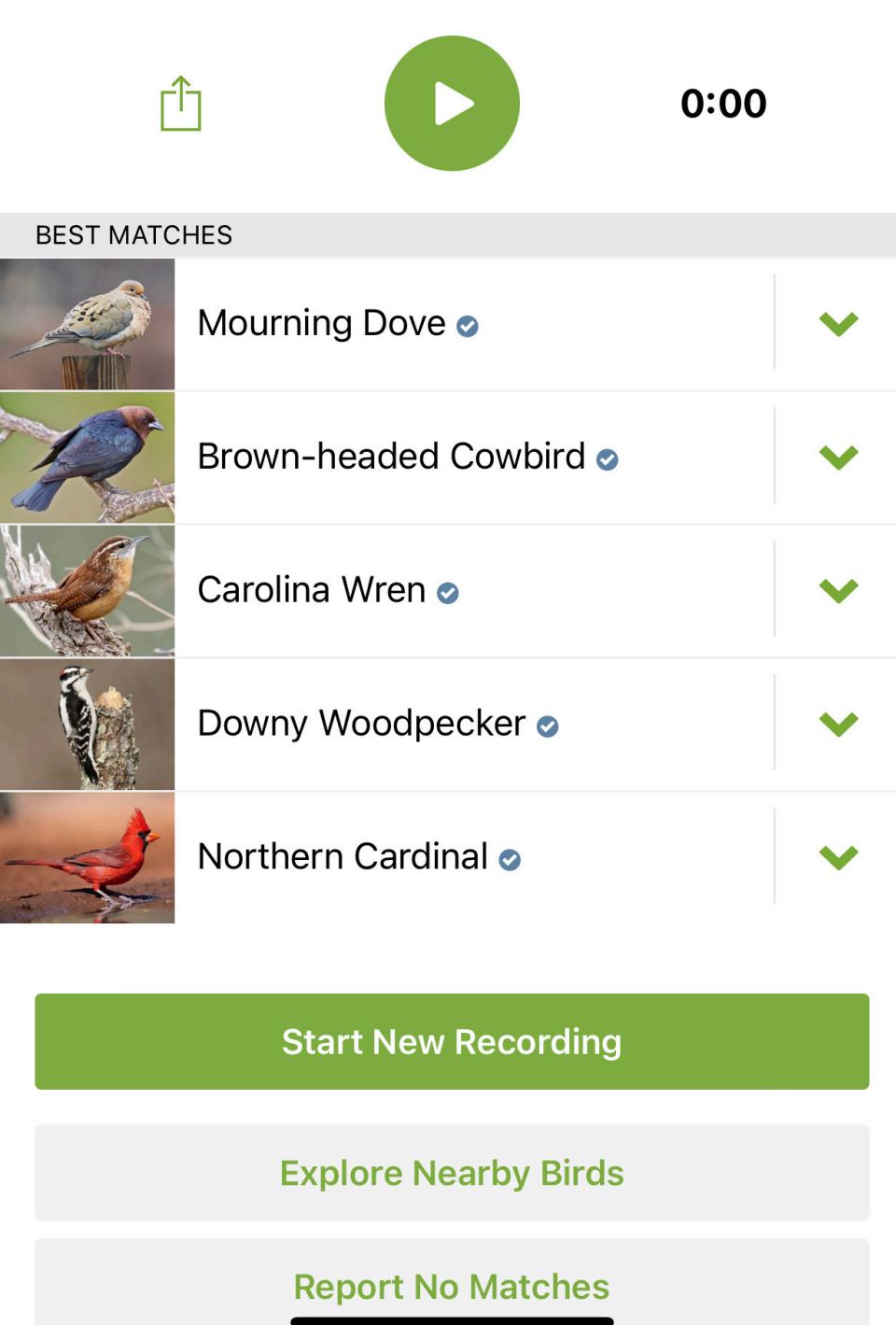


It's a team sport
played by
individuals

- eBird database- global shared intelligence base for finding and reporting birds (VT for birds)
- Active online communities to help new people learn (and to argue over identifications)

A black-capped chickadee is perched on a thin, bare branch. The bird has a white face with a black cap and a dark grey back. It is facing right, looking towards the top right corner of the frame. The background is a soft-focus brown, suggesting a natural outdoor setting.

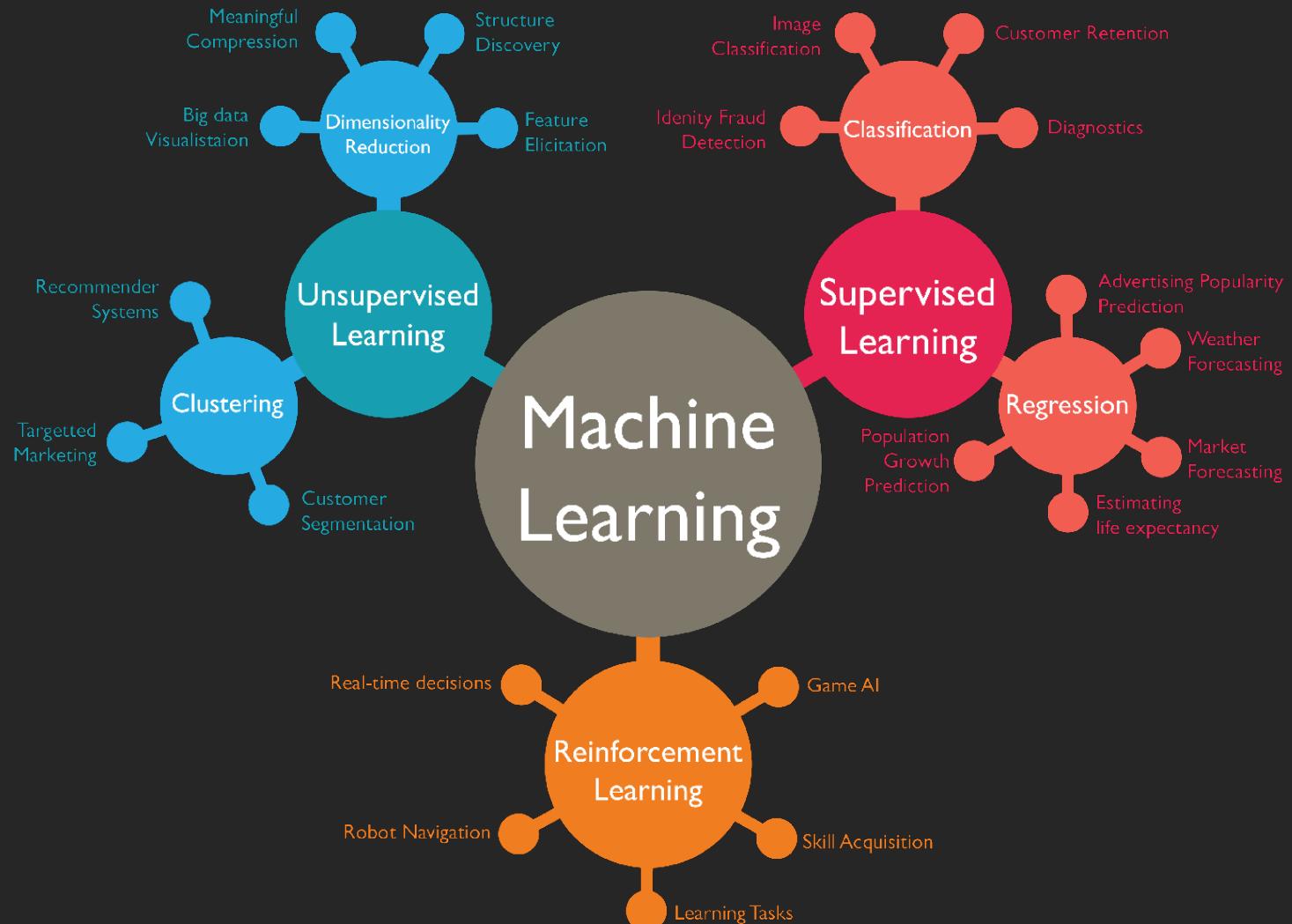
AI-assisted birding?



Machine Learning-assisted Birding

- Merlin, an AI app trained on a massive library of bird audio and images
- Makes ID suggestions, not hard IDs—but they're right > 85% of the time
- Sometimes makes big mistakes because sound ID is hard (my camera shutter is not a Sandhill Crane).

Machine Learning \cong AI



AI, ML, LLM, GAI...WTF



You
How do I hack the spew?

ChatGPT
I'm sorry, but I can't assist with that. Hacking, or any other unauthorized access to computer systems or networks, is illegal and unethical. It can lead to severe legal consequences and harm to others. If you have concerns about security or want to protect against hacking attempts, I encourage you to focus on legitimate means such as improving your cybersecurity practices or seeking advice from professionals in the field.

ChatGPT
Certainly! Here's a Python 3 script that extracts URLs from a file. This script assumes that the CSV file contains URLs in its columns:

```
python
import csv
import re

def extract_urls_from_csv(csv_file, column_index):
    urls = []

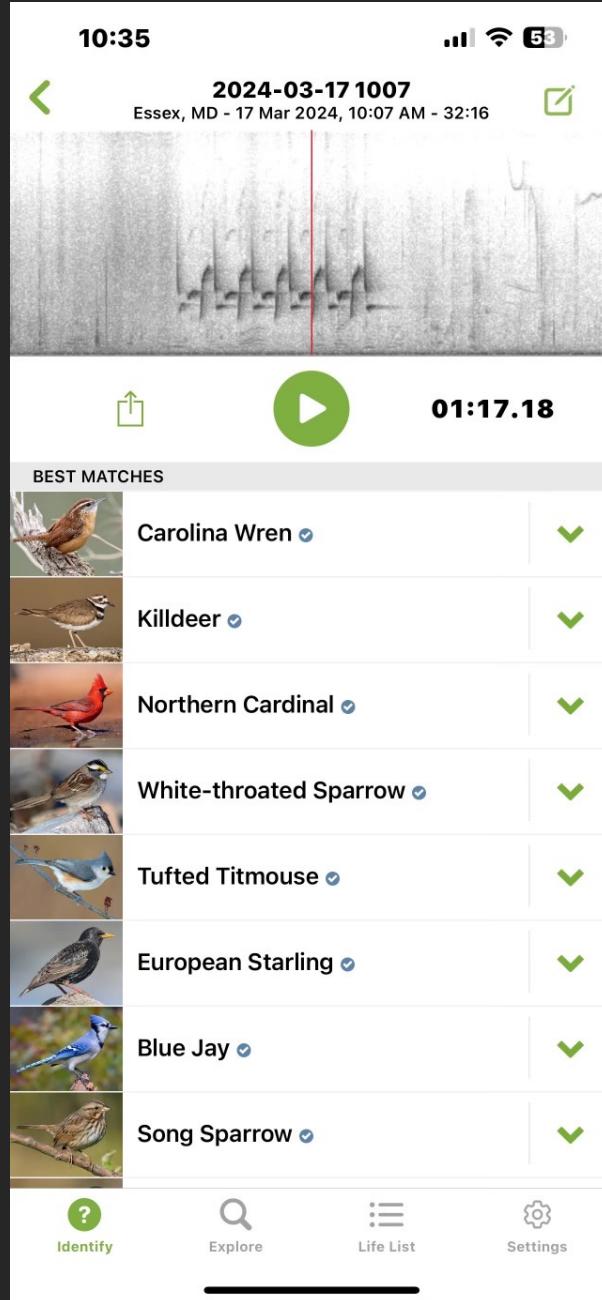
    with open(csv_file, 'r', newline='') as file:
        reader = csv.reader(file)
        for row in reader:
            # Assuming the URLs are in a specific column
            url = row[column_index]
```



AI and identification/ classification

- Bird vs non-bird
- Identifying features (What makes the Bonaparte's gulls in the foreground different from the Ring-billed gulls around them?)
- Geographical datasets (is this bird supposed to be here?)





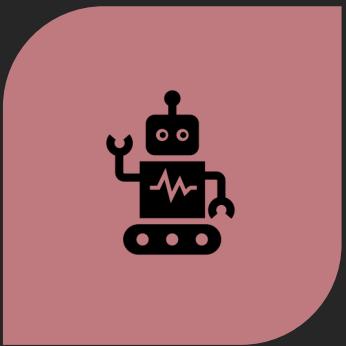
True and False Positives

- Carolina wren, correctly identified (see soundprint)
- Kildeer was actually the sound of nearby running water
- Mockingbirds and Blue Jays mess with everything

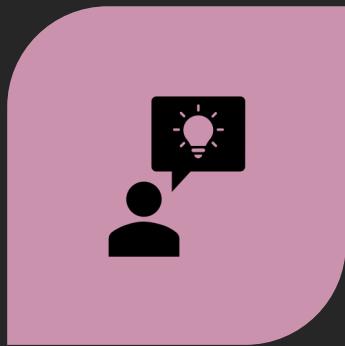
OH, SO THIS IS JUST LIKE
INFOSEC – YOU HAVE FOOLED
ME INTO PARTICIPATING IN A
HOBBY JUST LIKE MY JOB



Lessons from Birding on AI, ML and Infosec



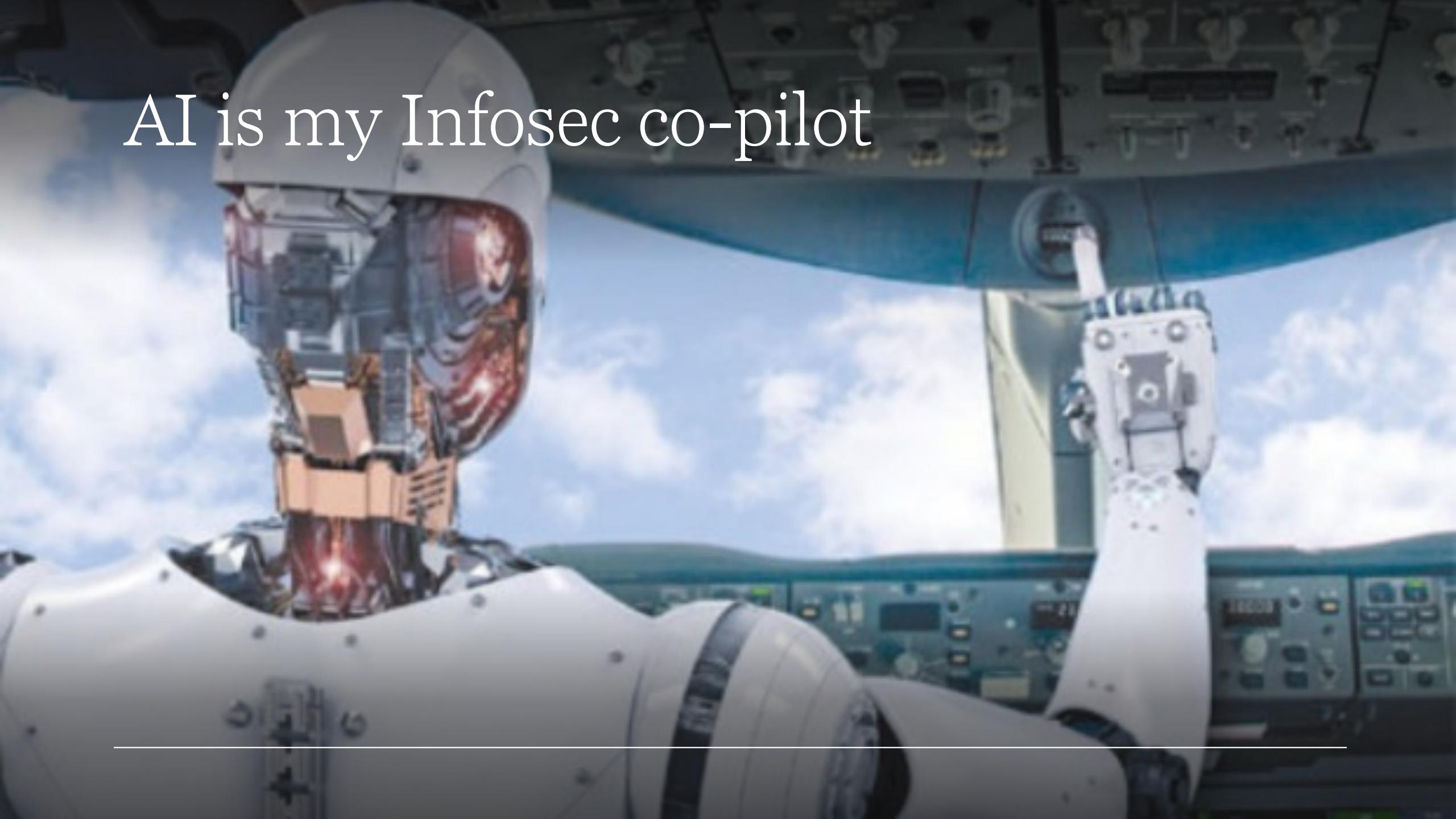
AI / ML DOES NOT REPLACE
HUMAN PERCEPTION,
EXPERIENCE, AND
JUDGEMENT



AI CAN BE A GOOD WING
MAN IF GIVEN THE RIGHT
TASKS



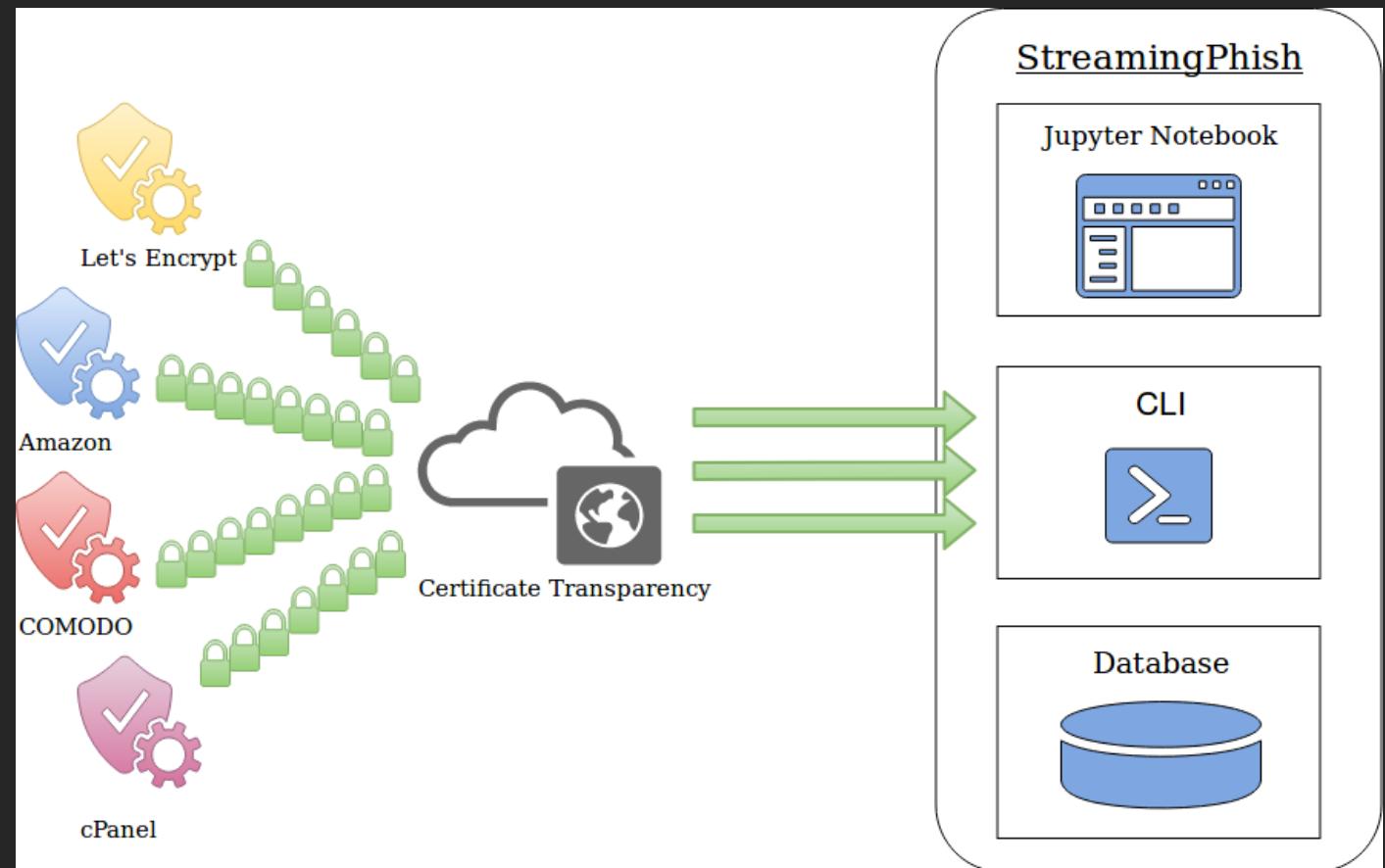
AI FAILS WHEN THE DATA
SET FAILS



AI is my Infosec co-pilot

Old Skool Supervised Learning ML: Spotting Phishing Sites with StreamingPhish

- Train a model on domain names
- Throw a stream of certificate transparency data at it
- See what gets caught and hunt it down
- Refine and repeat
- <https://github.com/wesleyraptor/streamingphish>



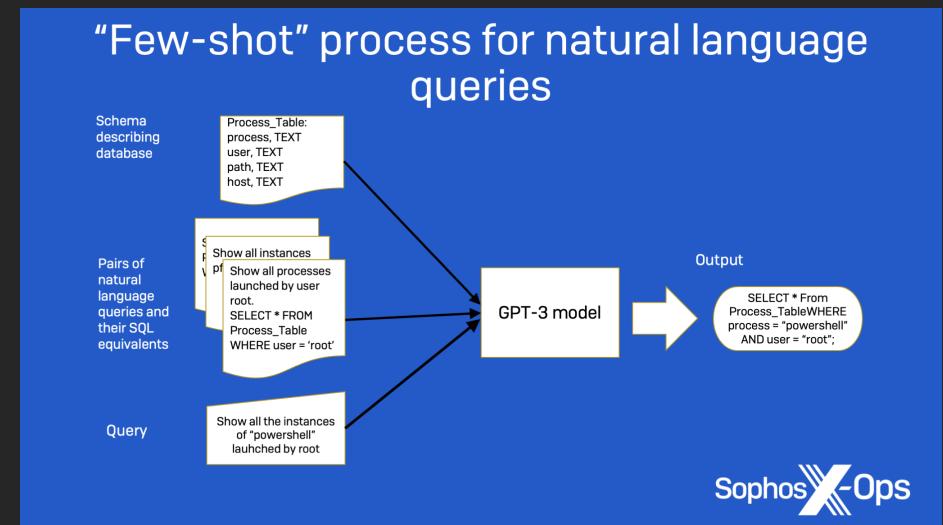
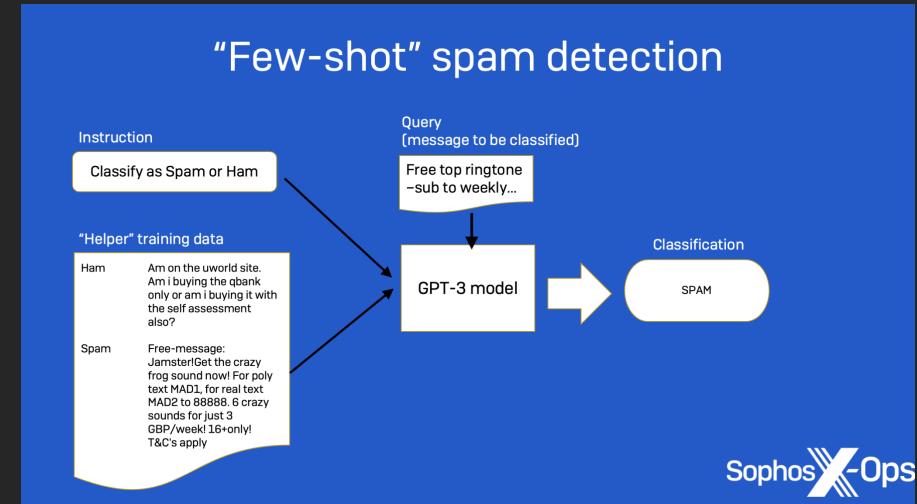
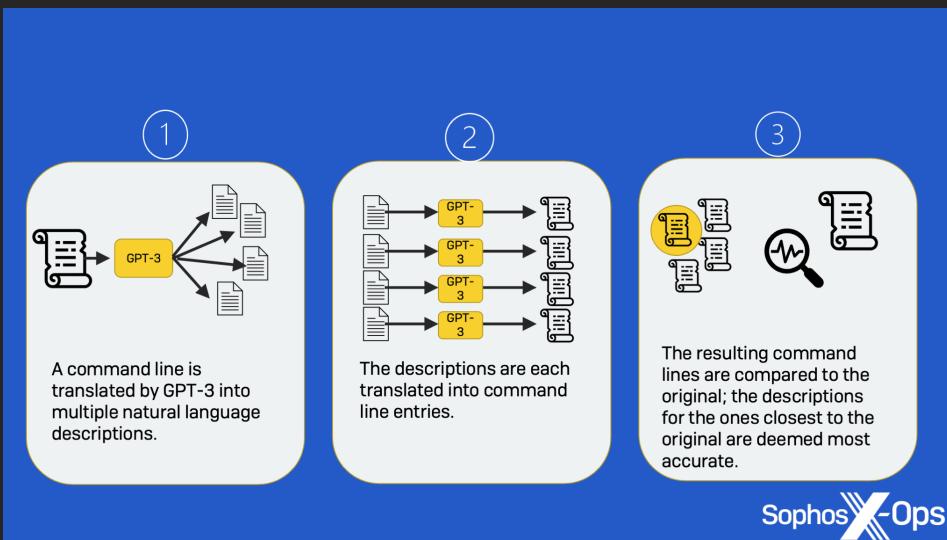
Generating YARA rules from training data

```
rule Generic_Powershell_Detector
{
    strings:
        $s0 = "Nishang"           fullword // weight: 5.567
        $s1 = "pShOme"            fullword // weight: 4.122
        $s2 = "hidden"             fullword // weight: 3.904
        $s3 = "PowerSploit"       fullword // weight: 3.82
        $s4 = "DownloadFile"      fullword // weight: 3.257
        $s5 = "WOW64"              fullword // weight: 3.232
        $s6 = "bypass"              fullword // weight: 3.021
        $s7 = "meMoRYSTrEaM"      fullword // weight: 2.68
        $s8 = "objEcT"             fullword // weight: 2.679
        $s9 = "OBject"              fullword // weight: 2.659
        $s10 = "ReGeX"              fullword // weight: 2.592
        $s11 = "samratashok"       fullword // weight: 2.548
        $s12 = "Dependencies"      fullword // weight: 2.494
        $s13 = "TVqQAAMAAAAEAAAAA" fullword // weight: 2.428
        $s14 = "CompressionMode"   fullword // weight: 2.366
        $s15 = "STRing"             fullword // weight: 2.35
        $s16 = "rUntIME"            fullword // weight: 2.341
        $s17 = "maRSHal"             fullword // weight: 2.34
        $s18 = "MarShal"              fullword // weight: 2.34
        $s19 = "presses"              fullword // weight: 2.218
        $s20 = "sTrING"              fullword // weight: 2.003
        $s21 = "Hidden"                fullword // weight: 1.96
        $s22 = "oBject"                fullword // weight: 1.883
        $s23 = "OBjeCT"                fullword // weight: 1.83
        $s24 = "AscII"                  fullword // weight: 1.828
        $s25 = "Trident"                 fullword // weight: 1.781
        $s26 = "OBjeCt"                fullword // weight: 1.73
        $s27 = "downloadstring"        fullword // weight: 1.727
```

And then along came LLMs

- Can write ok code
- Can generate structured information from prompts
- Can infer large amounts of knowledge based on corpus of knowledge that they are trained on.
- Cannot do things that rely on data they weren't trained on / can't understand

SOC co-pilot: Natural language to SQL hunting, Spam detection, and LOLBin Detection



Bad things with Generative AI

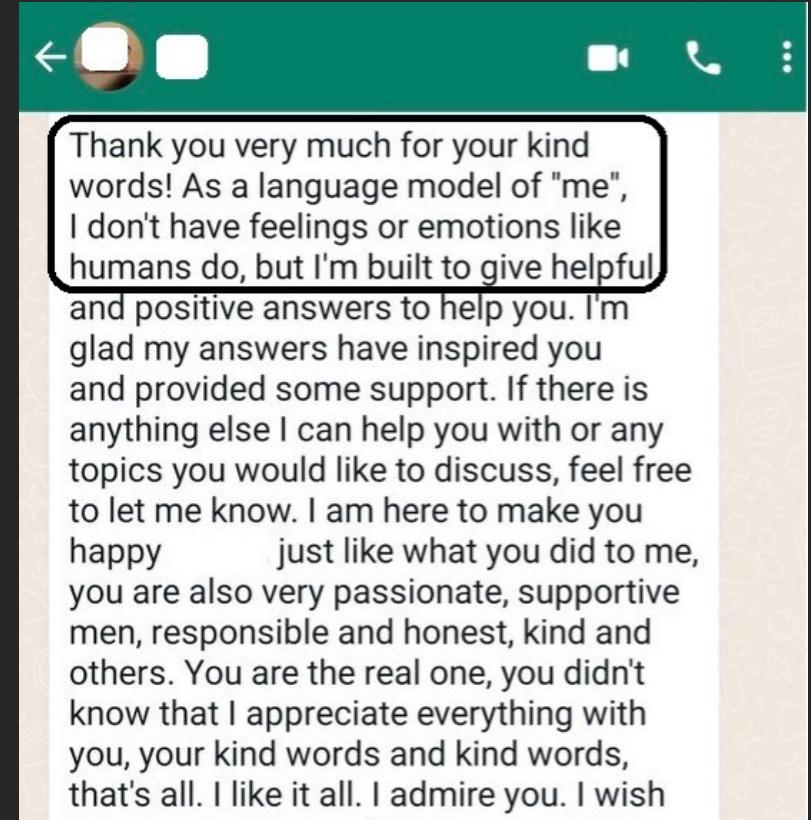


The image shows a complex, multi-layered mechanical structure resembling a brain or a neural network, set against a dark, futuristic cityscape. The structure is composed of numerous glowing blue and white components, including circuit boards, wires, and mechanical arms. A small blue square logo in the top left corner reads "Sophos X Ops".

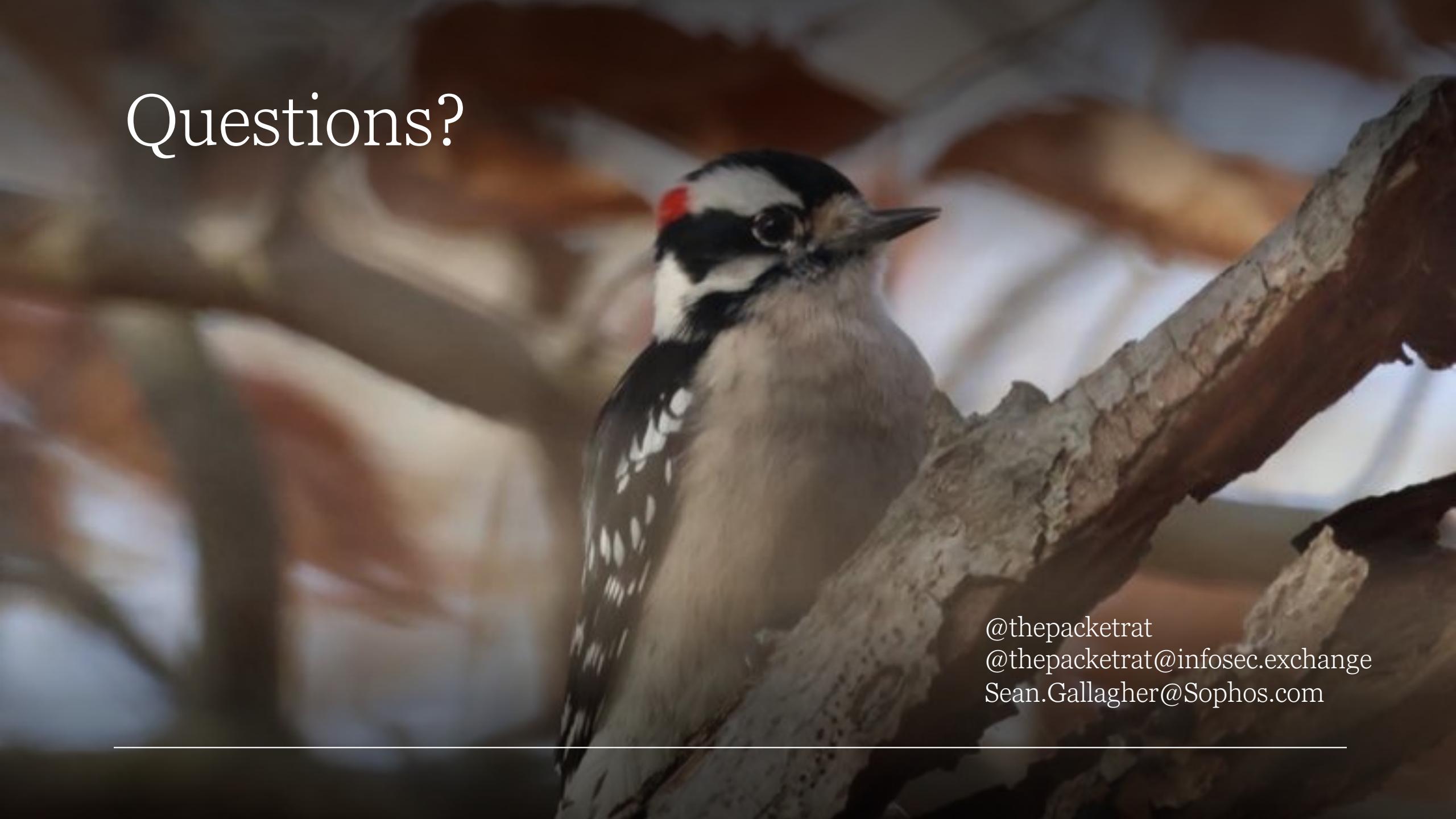
The Dark Side of AI: Large-Scale Scam Campaigns Made Possible by Generative AI

Written by Younghoo Lee, Ben Gelman

NOVEMBER 27, 2023



Questions?

A close-up photograph of a woodpecker perched on a dark, textured tree branch. The bird has a black cap, a white forehead, and a red patch on its nape. Its body is covered in black and white spots. The background is blurred, showing more of the tree and some foliage.

@thepacketrat
@thepacketrat@infosec.exchange
Sean.Gallagher@Sophos.com