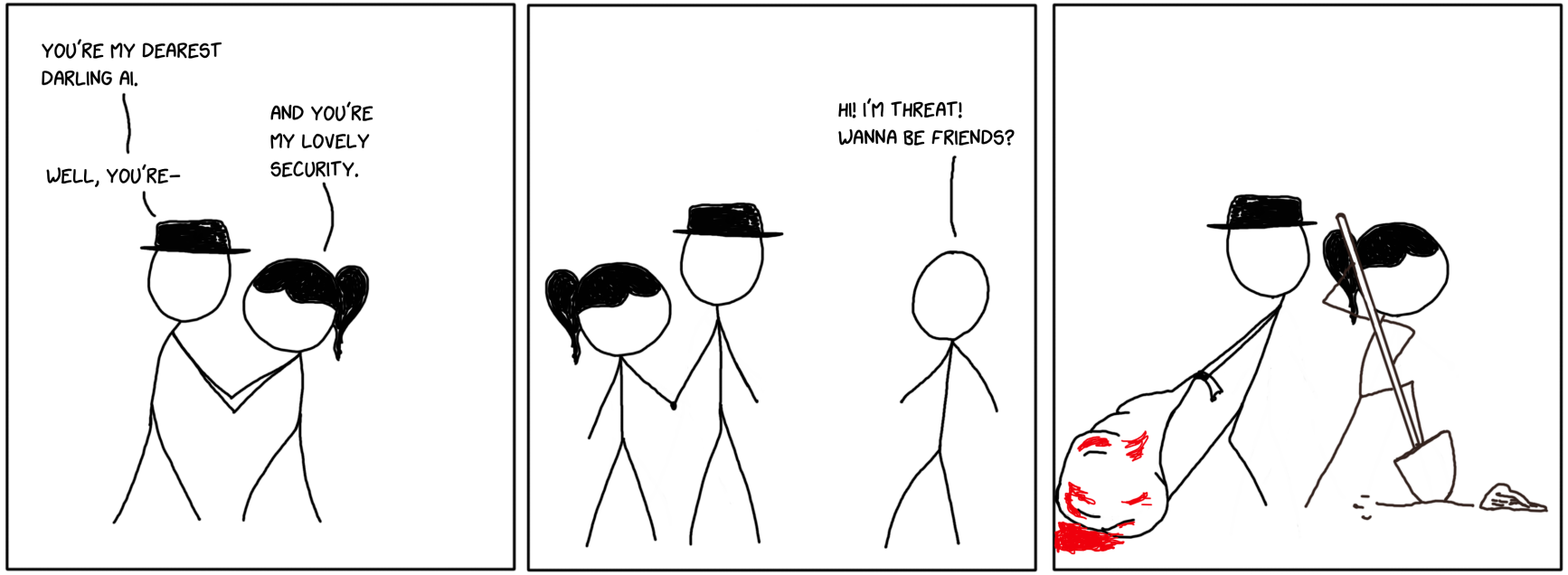
AI + Security = AiSec

Victoria Almazova

Cecilie Widsteen



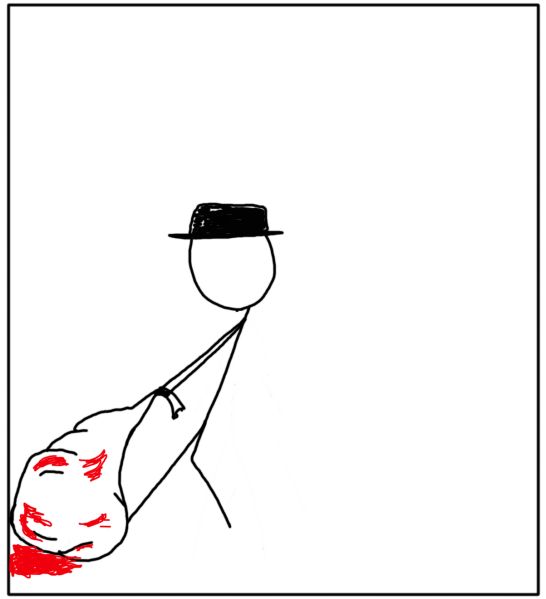
Speakers

Cecilie Widsteen

- AI expert
- Mostly into architecture for big data and AI but also generalist
- Does reading books while swinging in a hammock count as a hobby?

Victoria Almazova

- Security expert
- Loves Identity, DevSecOps, clouds
- When not killing security threats – kills legs by running, hiking and cycling



Agenda

- Introduction
- Overview
- Demo
- Wrap up and conclusions
- Q&A
- Useful resources

Introduction

Security objectives

- Security domains
- Challenges in the security world
  - Attacks are increasing in a scale and sophistication
  - Attackers entering new landscapes
  - Attackers follows footsteps of new technology development
  - Cat and mouse game on a defense side

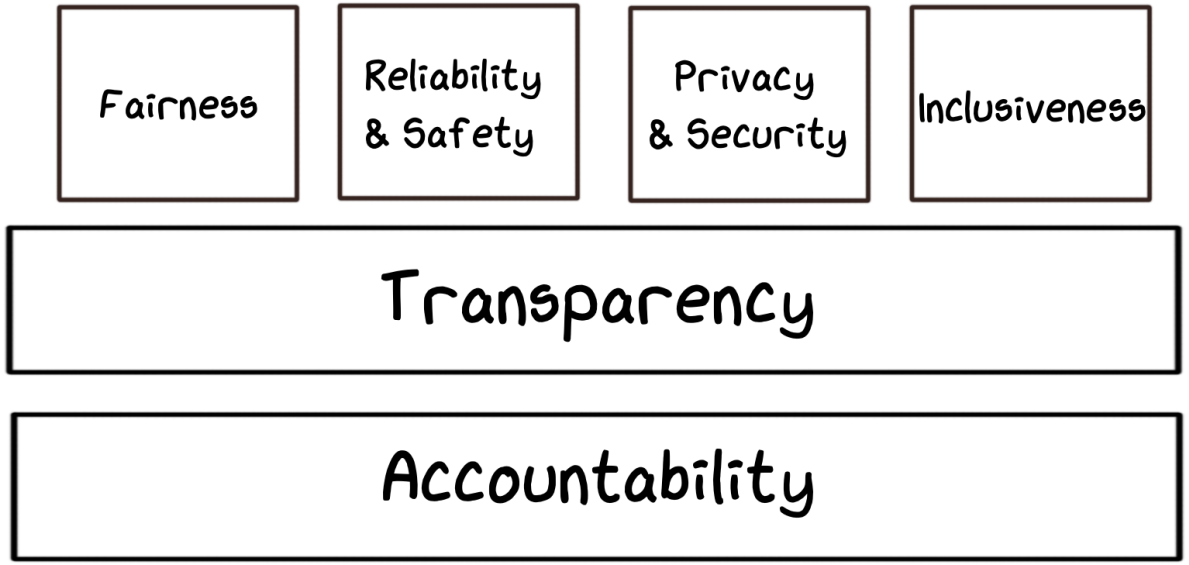
Security objectives

What is AI Security

- Using AI to improve security
- Defending against AI driven cyber attacks

AI objectives

- Machine Learning and Data Science
- Important concepts
- Responsible AI



AI objectives

What is security in AI

- Perturbation attacks
- Poisoning attacks
- Attacking the ML Supply Chain

Why is it important now?

AI and Security

- AI introduce new attack surface
- AI-specific threats
- Tools and mindset must adapt

Overview

What are use cases of AI in Security?

Cases:

- E-mail monitoring
- Network threat analysis and malware detection
- AI against AI-based threats
- AI to automate repetitive security tasks

The top security companies, who uses AI:

- Darktrace
- Sophos
- Fortinet
- Checkpoint
- Cynet

What are the challenges of securing AI?

- What is the state of the art in adversarial AI and how to protect your use of AI
- Mitigations:
  - Perturbation attacks
  - Poisoning attacks
  - Attacking the ML Supply Chain

Case: securing developers with AI

Challenges:

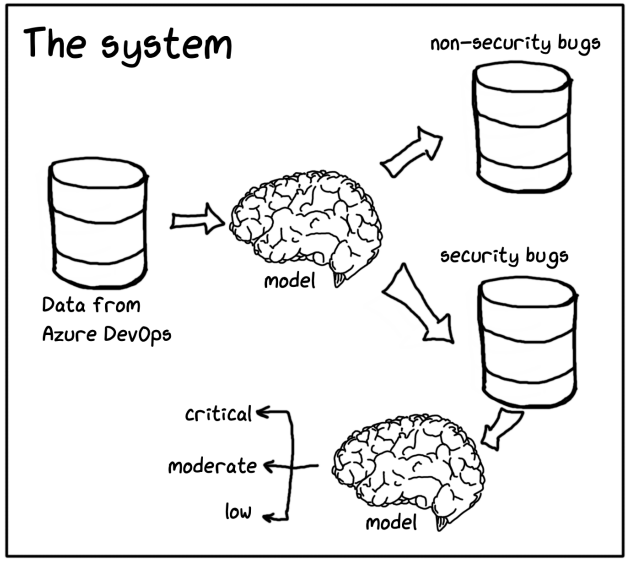
- Security knowledge or resources gap -> don't scale
- Security tools produces decent amount of "garbage" -> gets ignored

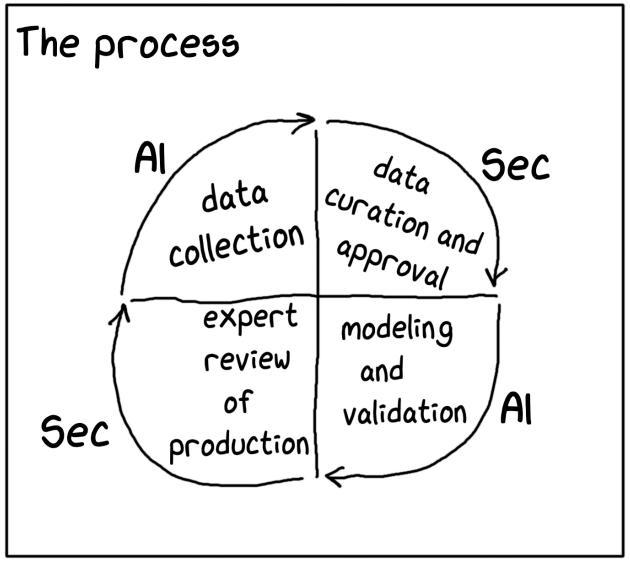
Microsoft "experiment":

- "Identifying security bug reports based solely on report titles and noisy data"
  - Classify a bug as security or non security
  - Based solely on the title of the bug report
- Outcome:
  - Classified work items correctly as security bugs 99% of the time
  - 97% accuracy at labeling critical and non-critical security bugs

Automate repetitive security tasks

- Bug report data
- "The machine learning test"
- Data scientist (AI) + Security SME (Sec) = ♥





Demo time!


THIS IS YOUR MACHINE LEARNING SYSTEM?
YUP! YOU POUR THE DATA INTO THIS BIG PILE OF LINEAR ALGEBRA, THEN COLLECT THE ANSWERS ON THE OTHER SIDE.
WHAT IF THE ANSWERS ARE WRONG?
JUST STIR THE PILE UNTIL THEY START LOOKING RIGHT.
DATA
ANSWERS

Wrap up and conclusions

Wrap up

- AI and Security challenges
- Importance of being present in both worlds
- Collaboration between AI and Sec

Call for the action:

- Security folks! Help AI to be cool and secure!
- Don't wait – find what data you have, interrogate it and then question what you still don't know...

QUESTIONS

FOUND IN GOOGLE AUTOCOMPLETE

WHY DO WHALES JUMP
WHY ARE WITCHES GREEN
WHY ARE THERE MIRRORS ABOVE BEDS
WHY DO I SAY UH
WHY IS SEA SALT BETTER
WHY ARE THERE TREES IN THE MIDDLE OF FIELDS
WHY IS THERE NOT A POKEMON MIMO
WHY IS THERE LAUGHING IN TV SHOWS
WHY ARE THERE DOORS ON THE FREEWAY
WHY ARE THERE SO MANY SHOSHOSIDXE RUNNING
WHY AREN'T THERE ANY COUNTRIES IN ANTARCTICA
WHY ARE THERE SCARY SOUNDS IN MINECRAFT
WHY IS THERE KICKING IN MY STOMACH
WHY ARE THERE TWO SUNSHES AFTER HTTP
WHY ARE THERE CELEBRITIES
WHY DO SNAKES EXIST
WHY DO OYSTERS HAVE PEARLS
WHY ARE DUCKS CALLED DUCKS
WHY DO THEY CALL IT THE CLAP
WHY ARE KYLE AND CARTMAN FRIENDS
WHY IS THERE AN ARROW ON AANG'S HEAD
WHY ARE TEXT MESSAGES BLUE
WHY ARE THERE MUSTACHES ON CLOTHES
WHY ARE THERE MUSTACHES ON CARS
WHY ARE THERE MUSTACHES EVERYWHERE
WHY ARE THERE SO MANY BIRDS IN OHIO
WHY IS THERE SO MUCH RAIN IN OHIO
WHY IS OHIO WEATHER SO WEIRD
WHY ARE THERE MALE AND FEMALE BIKES
WHY ARE THERE BRIDGETROLLS
WHY DO DYING PEOPLE REACH UP
WHY AREN'T THERE VARICOSE WOMEN
WHY ARE OLD KLINGONS DIFFERENT

WHY IS PROGRAMMING SO HARD
WHY IS THERE A 0 OHM RESISTOR
WHY DO AMERICANS HATE SOCCER
WHY DO RHYMES SOUND GOOD
WHY DO TREES DIE
WHY IS THERE NO SOUND ON ONN
WHY AREN'T POKEMON REAL
WHY AREN'T BULLETS SHARP
WHY DO DREAMS SEEM SO REAL

WHY AREN'T THERE DINOSAUR GHOSTS

WHY DO TESTICLES MOVE
WHY ARE THERE PSYCHICS
WHY ARE HATS SO EXPENSIVE
WHY IS THERE CAFFEINE IN MY SHAMPOO
WHY DO YOUR BOOBS HURT
WHY DO IGUANAS DIE

WHY ARE THERE SLAVES IN THE BIBLE
WHY DO TWINS HAVE DIFFERENT FINGERPRINTS
WHY ARE AMERICANS AFRAID OF DRAGONS

WHY IS HTTPS CROSSED OUT IN RED
WHY IS THERE A LINE THROUGH HTTPS
WHY IS THERE A RED LINE THROUGH HTTPS ON FACEBOOK
WHY IS YKK ON ALL ZIPPERS
WHY IS HTTPS IMPORTANT

WHY ARE THERE LEGS
WHY DO I FEEL DIZZY

WHY ARE THERE SWARMS OF GNATS
WHY IS THERE SMUDGE
WHY ARE THERE SO MANY CROWS IN ROCHESTER, MN

WHY AREN'T ECONOMISTS RICH
WHY DO AMERICANS CALL IT SOCCER
WHY ARE MY EARS RINGING
WHY ARE THERE SO MANY AVENGERS
WHY ARE THE AVENGERS FIGHTING THE X MEN
WHY IS WOLVERINE NOT IN THE AVENGERS

WHY IS THERE LAVA

WHY IS PSYCHIC WEAK TO BUG
WHY DO CHILDREN GET CANCER
WHY IS POSEIDON ANGRY WITH ODYSSEUS
WHY IS THERE ICE IN SPACE

WHY ARE THERE ANTS IN MY LAPTOP

WHY IS EARTH TILTED
WHY IS SPACE BLACK
WHY IS OUTER SPACE SO COLD
WHY ARE THERE PYRAMIDS ON THE MOON
WHY IS NASA SHUTTING DOWN

WHY IS THERE AN OWL IN MY BACKYARD
WHY IS THERE AN OWL OUTSIDE MY WINDOW
WHY IS THERE AN OWL ON THE DOLLAR BILL
WHY DO OWLS ATTACK PEOPLE
WHY ARE AK 47s SO EXPENSIVE
WHY ARE THERE HELICOPTERS CIRCLING MY HOUSE
WHY ARE THERE GODS
WHY ARE THERE TWO SPOOKS

WHY ARE THERE FEMALE MR MIMES

WHY ARE THERE TINY SPIDERS IN MY HOUSE
WHY DO SPIDERS COME INSIDE
WHY ARE THERE HUGE SPIDERS IN MY HOUSE
WHY ARE THERE LOTS OF SPIDERS IN MY HOUSE
WHY ARE THERE SPIDERS IN MY ROOM
WHY ARE THERE SO MANY SPIDERS IN MY ROOM
WHY DO SPIDER BITES ITCH
WHY IS DYING SO SCARY

WHY IS THERE HELL IF GOD FORGIVES

WHY IS THERE NO GPS IN LAPTOPS
WHY DO KNEES CLICK
WHY AREN'T THERE E GRADES
WHY IS ISOLATION BAD
WHY DO BOYS LIKE ME
WHY DON'T BOYS LIKE ME
WHY IS THERE ALWAYS A JAVA UPDATE
WHY ARE THERE RED DOTS ON MY THIGHS
WHY IS LYING GOOD

WHY IS GPS FREE

WHY IS MT VESUVIUS THERE
WHY DO THEY SAY T MINUS
WHY ARE THERE OBELISKS
WHY ARE WRESTLERS ALWAYS WET
WHY ARE OCEANS BECOMING MORE ACIDIC
WHY IS ARWEN DYING
WHY AREN'T MY QUAIL LAYING EGGS
WHY AREN'T MY QUAIL EGGS HATCHING
WHY AREN'T THERE ANY FOREIGN MILITARY BASES IN AMERICA

WHY IS LIFE SO BORING

WHY ARE MY BOOBS ITCHY
WHY ARE CIGARETTES LEGAL
WHY ARE THERE DUCKS IN MY POOL
WHY IS JESUS WHITE
WHY IS THERE LIQUID IN MY EAR
WHY DO Q TIPS FEEL GOOD
WHY DO GOOD PEOPLE DIE

WHY ARE ULTRASOUNDS IMPORTANT
WHY ARE ULTRASOUND MACHINES DIFFERENT
WHY IS STEALING WRONG

WHY ARE DOGS AFRAID OF FIREWORKS
WHY IS THERE NO KING IN ENGLAND

Useful resources

- Github repository: https://github.com/cecilidw/aisec
- https://www.microsoft.com/security/blog/2020/04/16/secure-software-development-lifecycle-machine-learning/
- https://www.rsaconference.com/usa/agenda/securing-the-software-development-life-cycle-with-machine-learning
- https://docs.microsoft.com/en-us/security/engineering/threat-modeling-aiml
- https://www.microsoft.com/en-us/ai/responsible-ai