DARKTRACE

AI and Machine learning in cybersecurity

Ronen, Leticia, Arun, Yodit

What is Darktrace

- Darktrace is an AI and machine learning based cybersecirty firm. They IPO'd In April 2021, they are very new.

- The topic of our investigation is the time it takes to detect a threat. We will explore this by comparing how legacy detection systems work vs how dark trace works. From their website; 'Where legacy security approaches rely on rules and signature based detection, Darktrace invented self-learning Cyber AI and autonomous response technology.'

- As we learned in class, the time it takes to detect an infiltration is critical. Once a system is breached, the time it takes to detect and remove the intrusion must be shorter than the time it takes the hackers to fully comprise the system.

Why?

A little more overview

- Members of our team are passionate and love machine learning, this is an interesting combination of both fields.

- Traditionally, threat detection is done by searching for ‘bad behavior’. This is a problem because its hard to detect new threats. With machine learning, we can train a model to recognize ‘normal behavior’ and then simply flag the rest.