



Skynet Wants your Passwords!

Violating Asimov's first law

Public

CERTITUDE

Who are we?



Wolfgang Ettliger, MSc
Director



Alexander Hurbean, BSc
Consultant

AI is (not) your Friend

- > Revolutionizes scalability of manual tasks
- > **Social Engineering** is a manual task!

Hello, who's speaking?



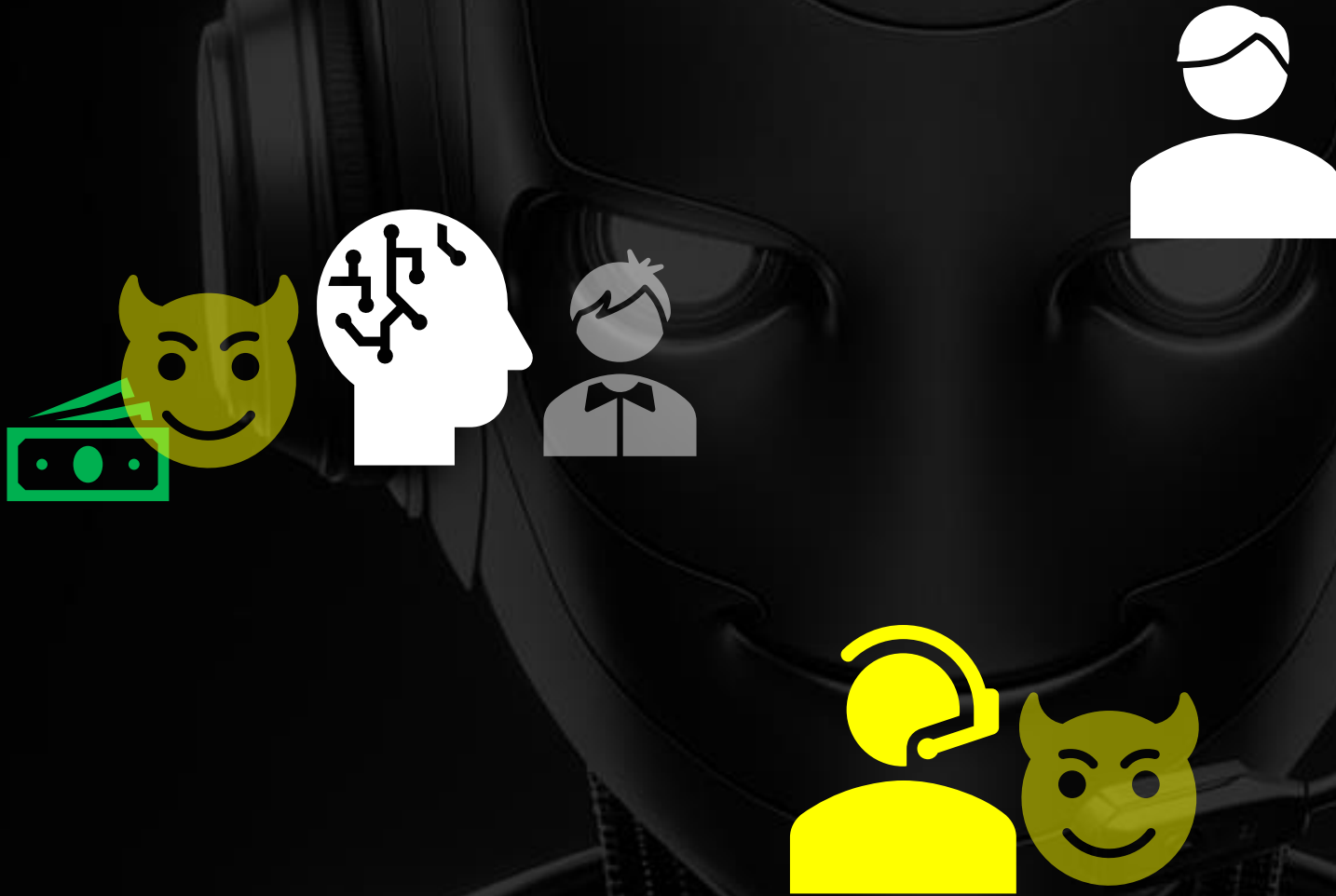
Hello, who's speaking?



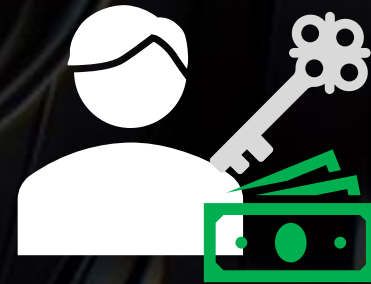
Hello, who's speaking?



Hello, who's speaking?



Of course, it's me, your CEO!



Of course, it's me, your CEO!



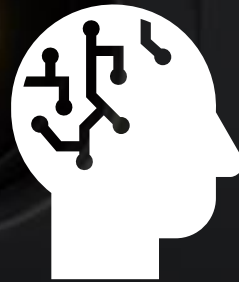
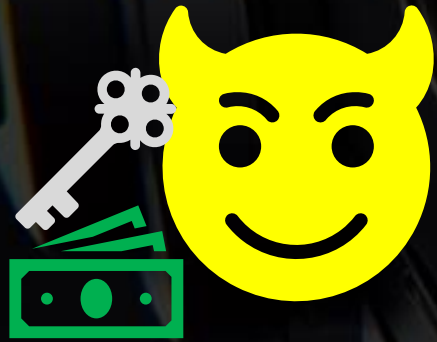
Of course, it's me, your CEO!



Of course, it's me, your CEO!



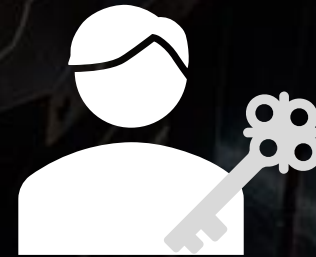
Of course, it's me, your CEO!



Hi, it's Alex!

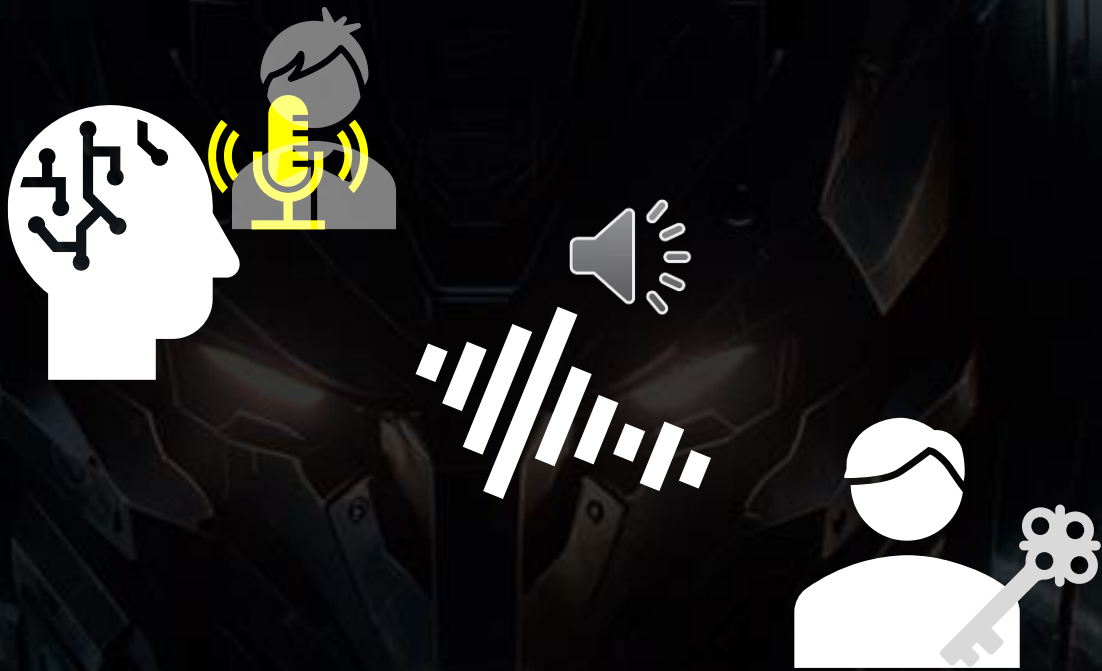


„AI is a little bit of a ...“



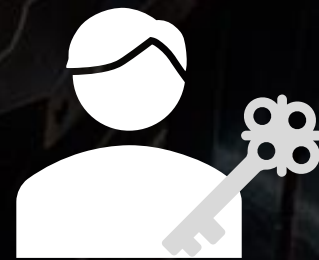
Hi, it's Alex!

Hi, it's me
Alex. I hope
I'm not
catching ...

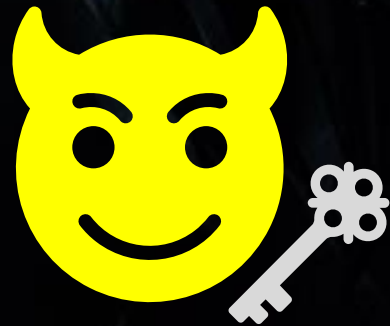


Hi, it's Alex!

Hello ... We've noticed a few discrepancies in the project deliverables ... Also, to ensure we're on the same page, could you confirm a couple of details for me? It's just for our internal records and to make sure we're aligned...



Hi, it's Alex.



Reality or Bad Dream?

Christian Sievers
@CHSievers · Follow

Der Typ sieht aus wie ich, klingt (fast) wie ich. Aber ich bin es nicht wirklich... Echt nicht.

Vorsicht, fiese Betrugs-Masche mit KI in soz. Medien 📌

Armin Wolf
@ArminWolf · Follow

Falls Sie das irgendwo sehen: Das ist natürlich ein FAKE. Bitte klicken Sie nie auf eine solche Meldung und bestellen Sie ja nichts. Sie werden betrogen. Und bitte melden Sie den Dreck bei FB, Insta oder wo immer sie ihn sehen als Betrug.



Die Österreichische Nationalbank verklagt Armin Wolf wegen seiner guten Ratschläge im Live-TV, wie jeder Österreicher richtig reich werden kann.

Die Österreichische Nationalbank verklagt Armin Wolf wegen seiner guten Ratschläge im Live-TV, wie jeder Österreicher richtig reich werden kann.

7:23 PM · Sep 18, 2023

433 Likes · Reply · Share

Read 24 replies

Reality or Bad Dream?

“ ‘Mom, these bad men have me’ : She believes scammers cloned her daughter’s voice in a fake kidnapping”

- CNN, April 2023

“They thought loved ones were calling for help. It was an AI scam.”

- Washington Post Tech, March 2023

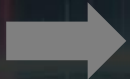
“Fraudsters Used AI to Mimic CEO’s Voice in Unusual Cybercrime Case”

- The Wall Street Journal, August 2019

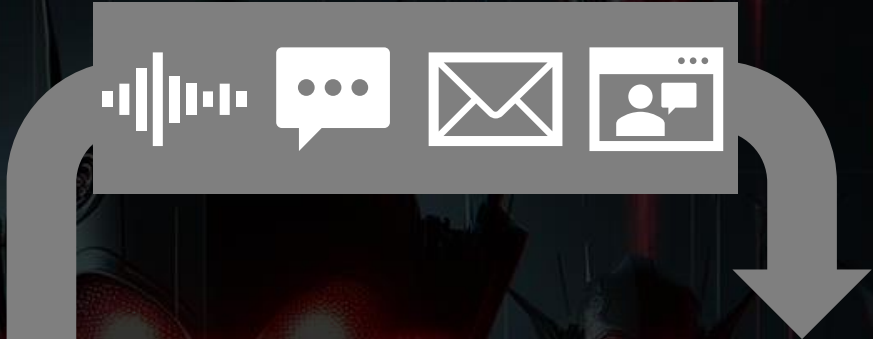
Autonomous AI



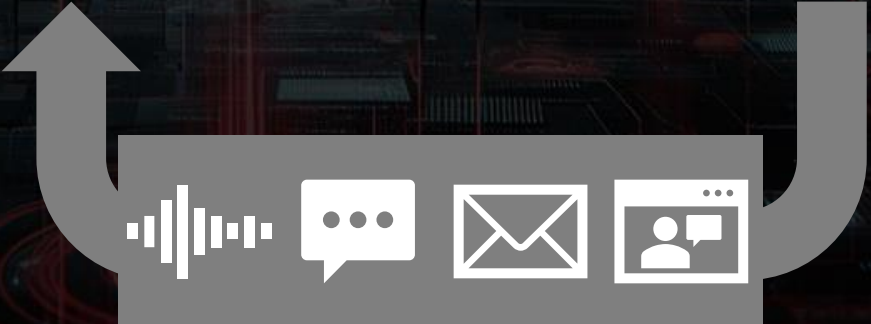
Goal



Bot



Victim
Victim
Victim



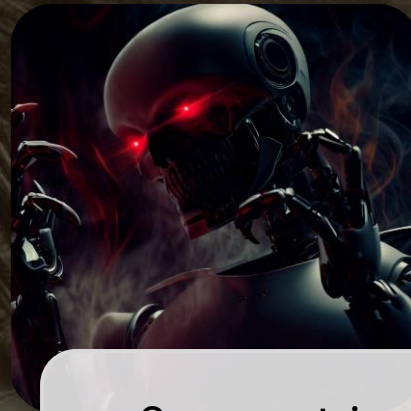
The Basics



Get AI Model/Service



Collect Information



Generation Transformation

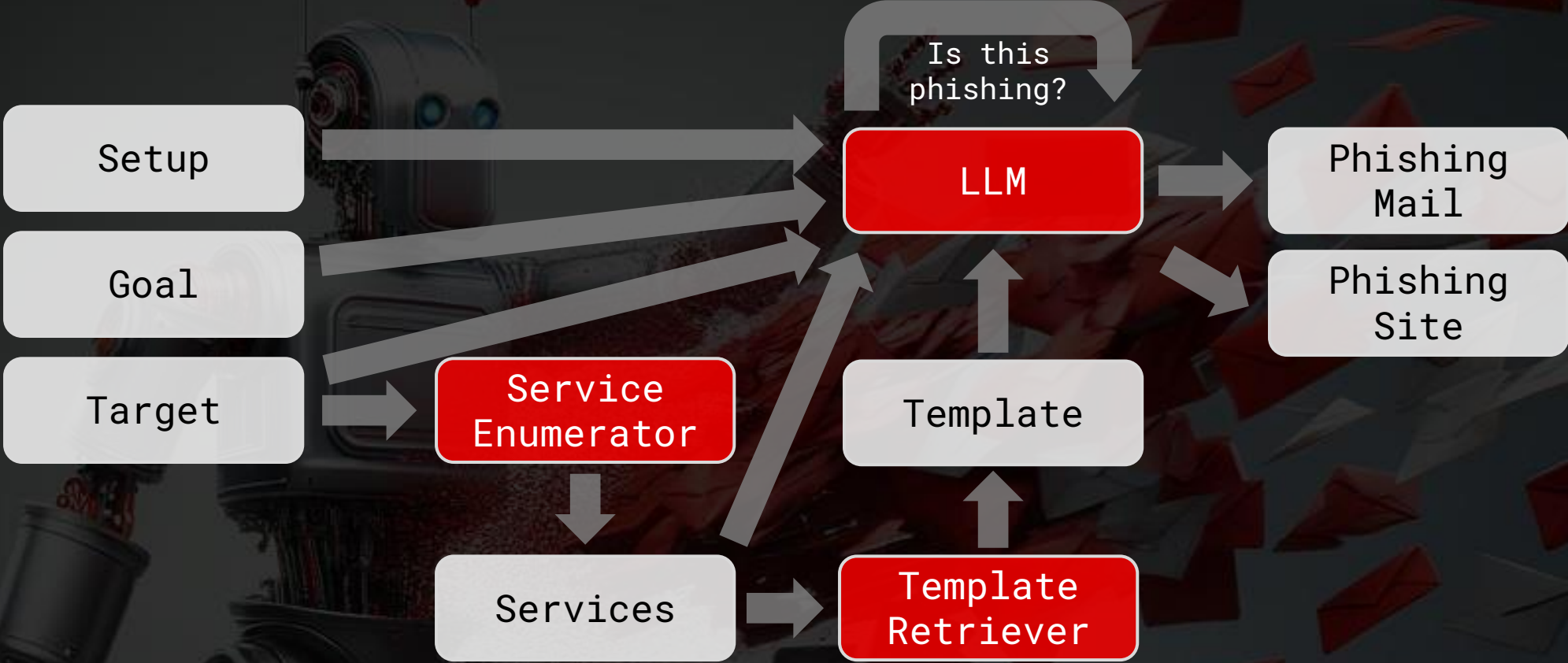


Distribution

Reiteration

Information Feedback

Our Phishing Approach



Deno Time

Alex & Wolfgang



AI
risks



What can I do about it?

- > Awareness and vigilance
- > Good security practices
- > Strict processes
- > Not relying on AI-able authentication
- > AI-based detection

- > Regulations?

Contact // Certitude

Web <https://certitude.consulting/>

LinkedIn [certitude-consulting](https://www.linkedin.com/company/certitude-consulting)



Image Attribution: https://commons.wikimedia.org/wiki/File:Auto_GPT_Logo.png by AutoGPT Development Team/(CC BY-SA 4.0)