



COMMUNITY DAY

AOTEAROA

Dead Reckoning the Digital Landscape

A Deep Dive into AI's Emergence and its Role in Cybersecurity

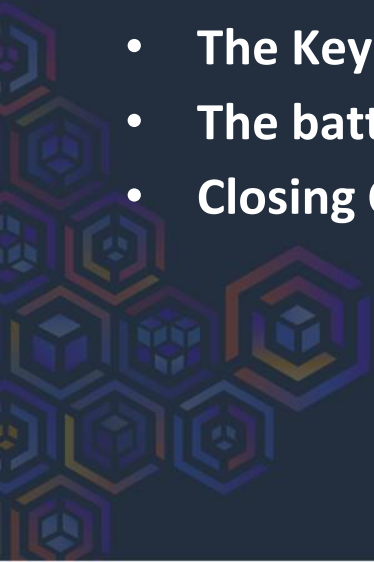


COMMUNITY DAY

AOTEAROA

CONTENTS

- **Unveiling the Mission**
- **The Threat of the Entity**
- **The Key to Control**
- **The battle for control**
- **Closing Credits**





Unveiling the Mission





COMMUNITY DAY

AOTEAROA



AI IS IMPOSSIBLE



AI IS JUST AUTOMATION



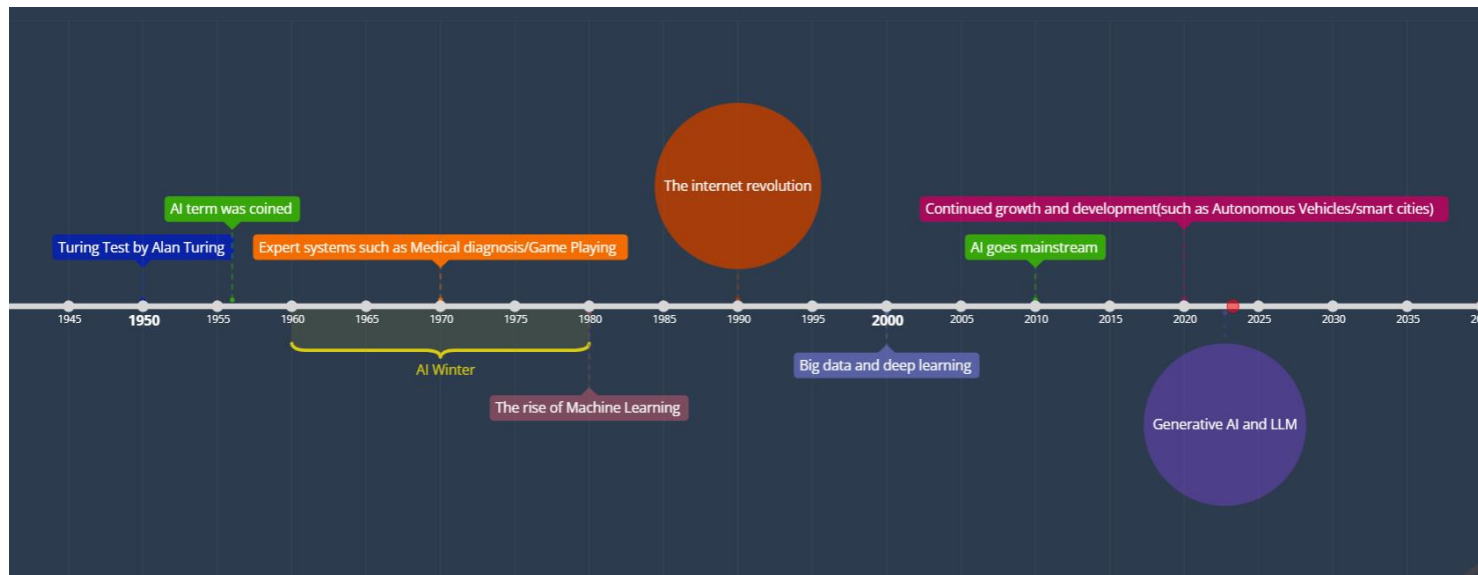
AI WILL SOLVE ALL
PROBLEMS



AI MAY KILL US



Introduction to AI and ML



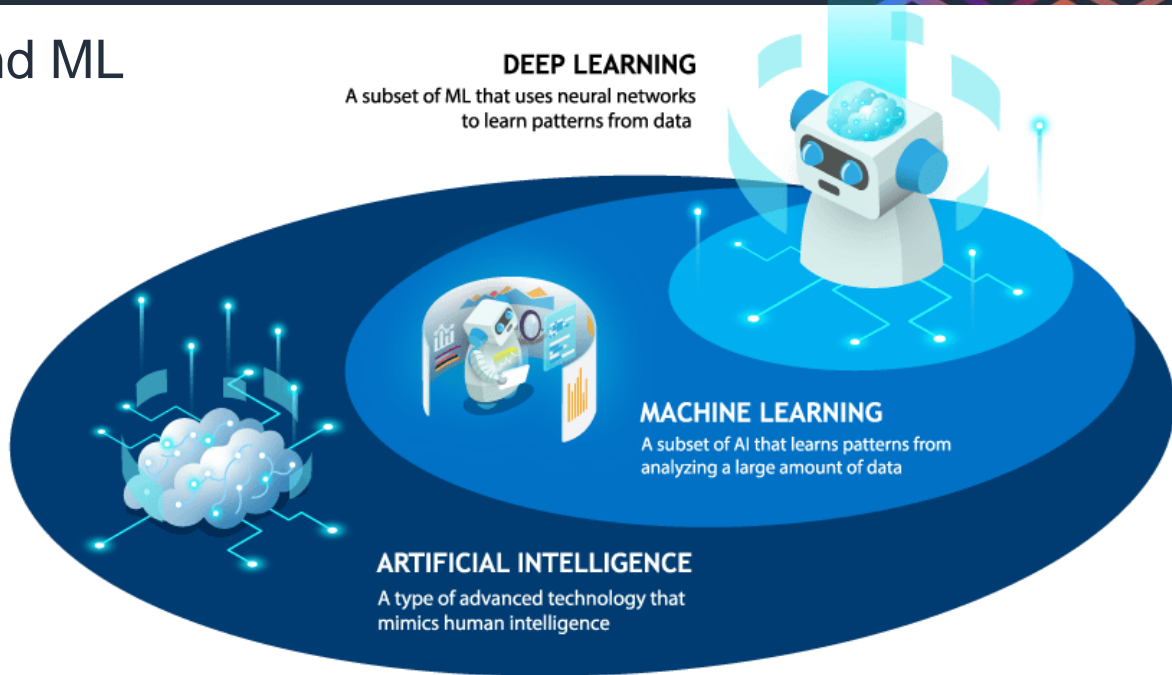


COMMUNITY DAY

AOTEAROA

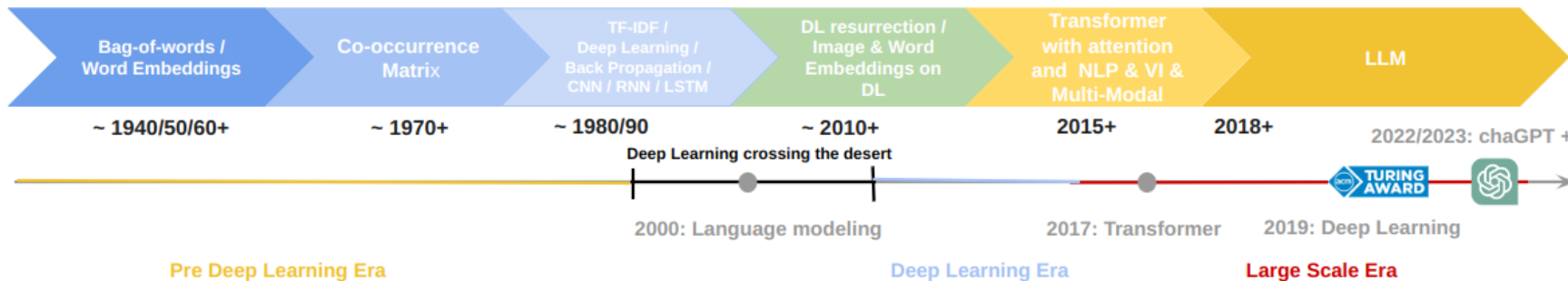
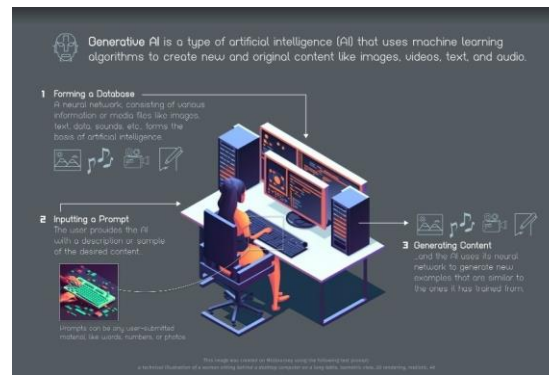


Introduction to AI and ML





Generative AI





COMMUNITY DAY

AOTEAROA

Generative AI



- Requirements writing and analysis
- User story generation

- Architecture writing assistance
- Sequence, flow diagram generation
- Data Model authoring
- UX design assistance

- Code generation
- Debugging
- Explain code
- Improve consistency
- Code translation

- Test cases writing
- Testing code generation

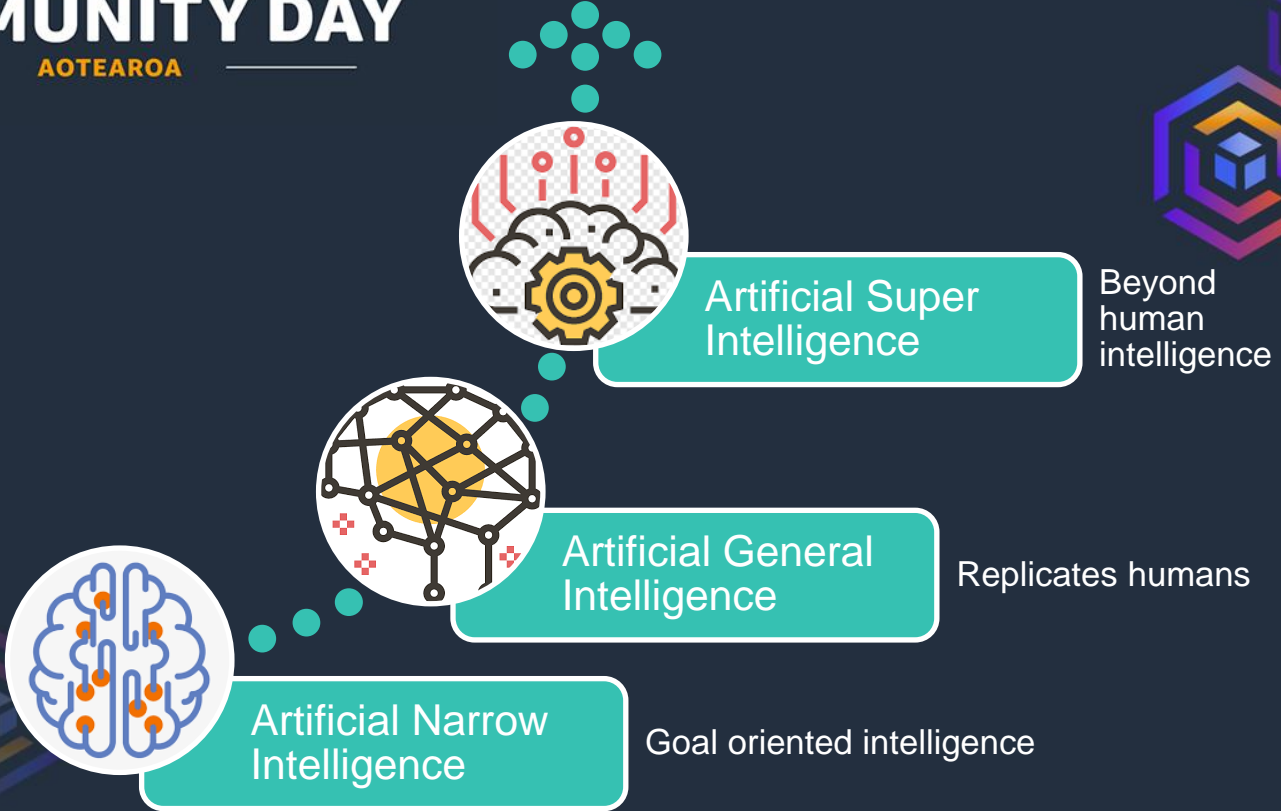
- Continuous integration/Continuous deployment generation
- Infrastructure as Code script writing support
- Automation script writing assistance

- Performance monitoring and remedy suggestion
- Document generation
- AI-assisted support



COMMUNITY DAY

AOTEAROA





COMMUNITY DAY

AOTEAROA

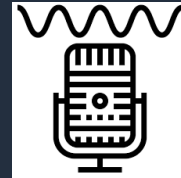
Human-Computer Interface



Graphical User Interface



Command line interface



Natural language interface

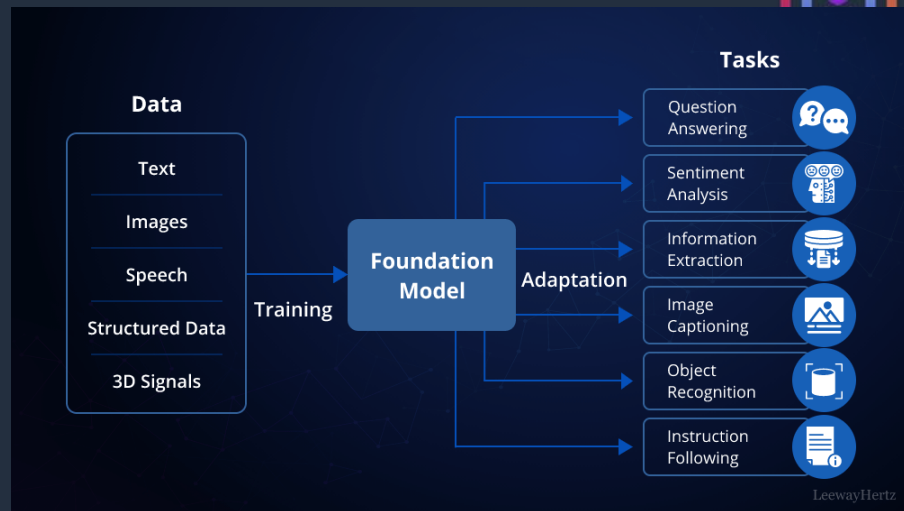
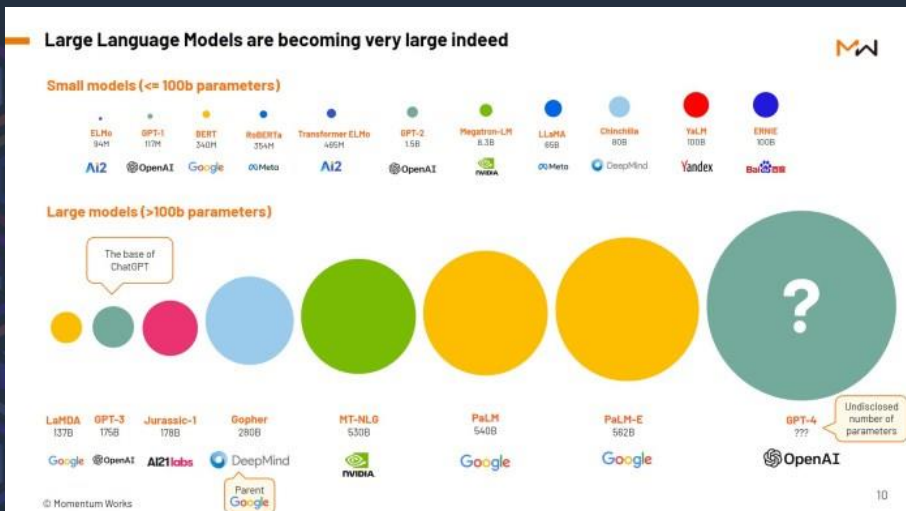




COMMUNITY DAY

AOTEAROA

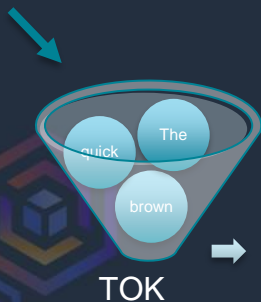
Large language Models (LLMs) are machine learning models capable of Natural Language Processing (NLP), as they are trained on huge amounts of text data (usually from the internet/books) via deep-learning algorithms.



How LLMs work

Prompt

The quick brown
fox



Context

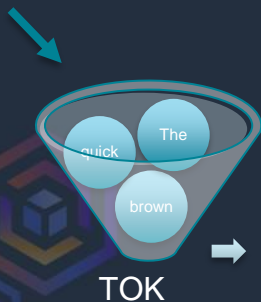
The(1) quick(10) brown(4)
fox(2)



How LLMs work

Prompt

The quick brown
fox

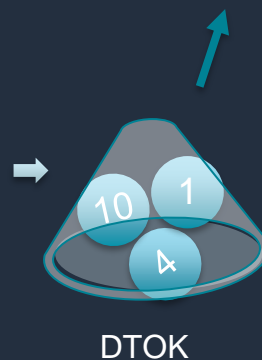


Context

The(1) quick(10) brown(4)
fox(2) jumps(6) over(8)
the(1) lazy(20) dog(7).(0)

Output

The quick brown fox
jumps over the lazy dog.



Prompt Engineering

Zero shot inference

Prompt

One shot inference

Prompt

Example

few shot inference

Prompt

Multiple
examples

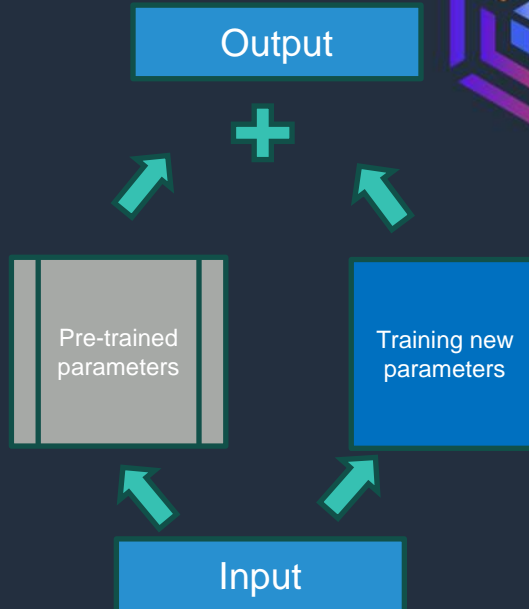
Fine tuning techniques:

Repurpose the model

Unsupervised vs supervised fine-tuning

Reinforcement learning from Human Feedback (RLHF)

Parameter Efficient Fine Tuning (PEFT)

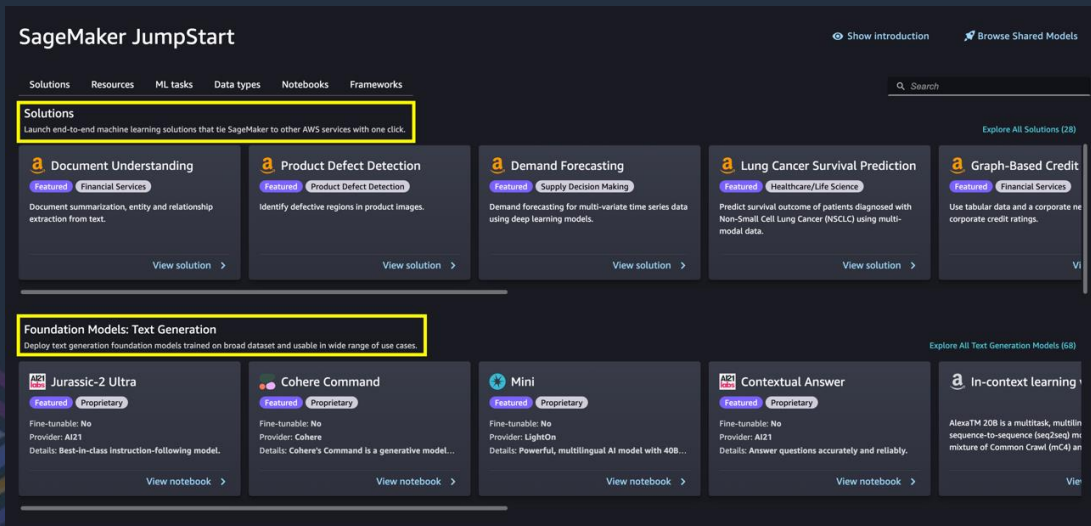




COMMUNITY DAY

AOTEAROA

AWS Sagemaker Jumpstart -



SageMaker JumpStart [Show introduction](#) [Browse Shared Models](#)

Solutions Resources ML tasks Data types Notebooks Frameworks

Solutions

Launch end-to-end machine learning solutions that tie SageMaker to other AWS services with one click. [Explore All Solutions \(28\)](#)

- Document Understanding** (Financial Services)
Document summarization, entity and relationship extraction from text. [View solution](#)
- Product Defect Detection** (Product Defect Detection)
Identify defective regions in product images. [View solution](#)
- Demand Forecasting** (Supply Decision Making)
Demand forecasting for multi-variate time series data using deep learning models. [View solution](#)
- Lung Cancer Survival Prediction** (Healthcare/Life Science)
Predict survival outcome of patients diagnosed with Non-Small Cell Lung Cancer (NSCLC) using multi-modal data. [View solution](#)
- Graph-Based Credit** (Financial Services)
Use tabular data and a corporate network graph to predict corporate credit ratings. [View solution](#)

Foundation Models: Text Generation

Deploy text generation foundation models trained on broad dataset and usable in wide range of use cases. [Explore All Text Generation Models \(68\)](#)

- Jurassic-2 Ultra** (Proprietary)
Fine-tunable: No
Provider: AI21
Details: Best-in-class instruction-following model. [View notebook](#)
- Cohere Command** (Proprietary)
Fine-tunable: No
Provider: Cohere
Details: Cohere's Command is a generative model... [View notebook](#)
- Mini** (Proprietary)
Fine-tunable: No
Provider: LightOn
Details: Powerful, multilingual AI model with 40B... [View notebook](#)
- Contextual Answer** (Proprietary)
Fine-tunable: No
Provider: AI21
Details: Answer questions accurately and reliably. [View notebook](#)
- In-context learning**
AlexaTM 20B is a multitask, multilin sequence-to-sequence (seq2seq) mixture of Common Crawl (mC4) an... [View notebook](#)

Examples of LLMs

- ChatGPT – Text Generation
- Copilot/Codex – Code Generation tool
- DALL-E/Midjourney – Image generation
- Whisper – Transcription from audio to text



Théâtre d'Opéra Spatial (Image credit: Jason Allen)

The threat of the entity





COMMUNITY DAY

AOTEAROA

- Cybersecurity is the practice of protecting systems, networks, and programs from digital attacks
- The first hacker was in 1970 called creeper
- Attacks can be in different shapes or forms

A black terminal window with green text that reads "I'M THE CREEPER. CATCH ME IF YOU CAN!".

Top Cybersecurity Threats





COMMUNITY DAY

AOTEAROA

Security is asymmetrical problem- Why?



Security is asymmetrical problem- Why?

"To build may have to be the slow and laborious task of years. To destroy can be the thoughtless act of a single day." Winston Churchill

So true, isn't it...

Defenders have to prevent all attacks and all potential vulnerabilities for the life of the system.

Attackers have to find and exploit ONE vulnerability to meet their objective





COMMUNITY DAY

AOTEAROA



Global Artificial Intelligence In Cyber Security Market

2023-2030





The key to control





AI-Based solutions



Detect and respond
in real-time



Continuously learn
and adapt



Analyse user
behavior



Analyse security
logs



Detection anomaly
in the network

Binary visual comparison of malicious files (a) and (b) against normal files (c) and (d)



(a) Backdoor.Win32.Shoda bot.b



(b) Trojan-Dropper.Win32.HeliosBinder.p



(c) Vmware player



(d) Google

When cyber attacks meet financial crime

- Identity theft
- Money laundering
- Credit card fraud
- Tax evasions

AI is used to analyze large amounts of data and identify patterns and anomalies that might indicate fraudulent behavior or suspicious activity.



BNZ Use Case - Prevent Financial crime



Pattern

- Huge Payment
- Frequent payments

Model

- Define target
- Predict High Risk customers

Validate

- Data Test-set validation
- Experts Validation



The battle for control





COMMUNITY DAY

AOTEAROA

Generative AI – Curse or a boon

Curse

Deepfakes

Text generation-phishing emails

Image generation

Audio generation

Synthetic data

Automated frauds

Boon

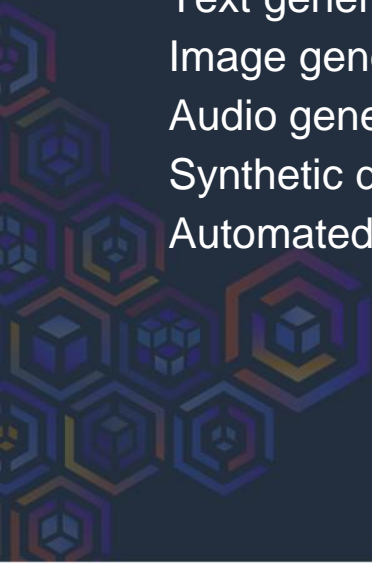
Efficient threat reporting

Enhanced Vulnerability Management

Automated incident response

Policy generation

Simulation



AI Ethics pillars

AI ethics pillars



Explainability



Fairness



Robustness



Transparency



Privacy

Guardrails

- Tools and processes
- Validate the contents
- Governance and policies
- Monitoring
- Education





COMMUNITY DAY

AOTEAROA

Everyone has a role to play...

CLOSING CREDITS

Executive Producer

Director

Lead Actor

Supporting Actor

Scriptwriter

Costume Design

Special Effects

Stunt Doubles

Audience

Organizations & Regulatory Bodies

AI Experts

AI Engineers

Cybersecurity Analysts

Legal and Ethical Advisor

UI/UX Designers

Devops Teams

Open Source Communities

End user community

Implementing AI in cybersecurity is a collaborative effort. Each one of us has a unique role to play in making our digital world more secure



COMMUNITY DAY

AOTEAROA