aws

COMMUNITY DAY

AOTEAROA

aws
COMMUNITY DAY
AOTEAROA

Dead Reckoning the Digital Landscape

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

aws
COMMUNITY DAY
AOTEAROA

CONTENTS

aws
COMMUNITY DAY
AOTEAROA

Unveiling the Mission

aws
COMMUNITY DAY
AOTEAROA

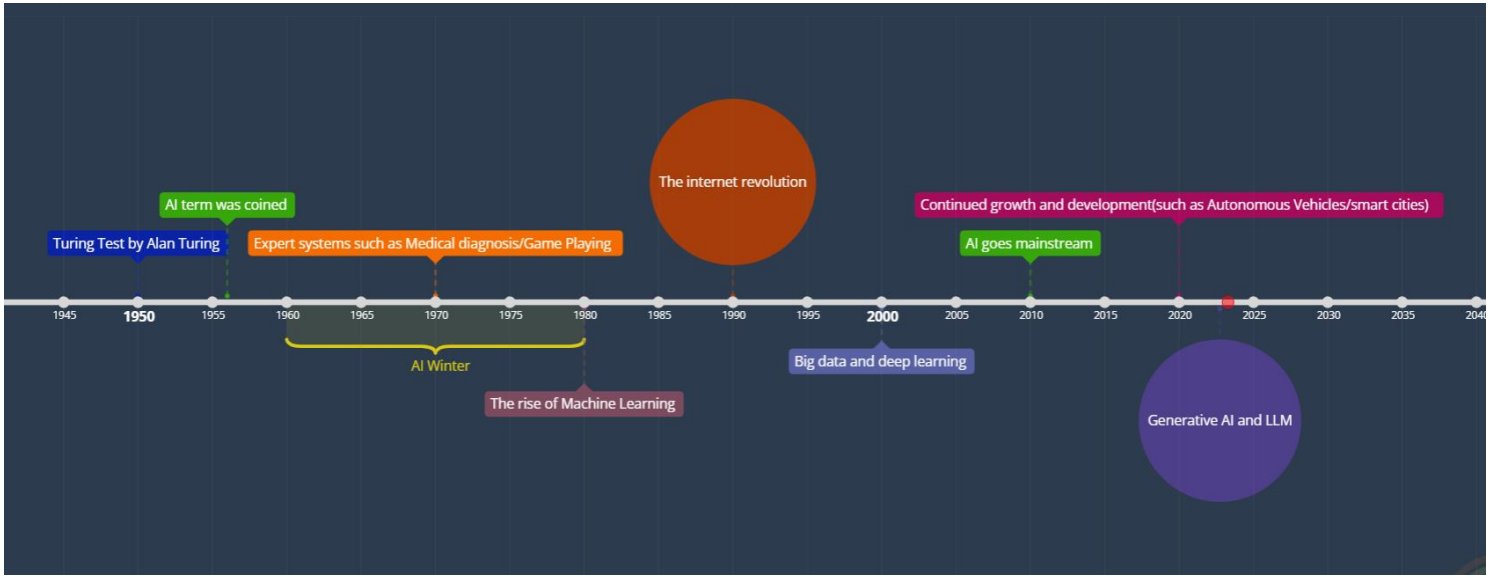
AI IS IMPOSSIBLE

AI IS JUST AUTOMATION

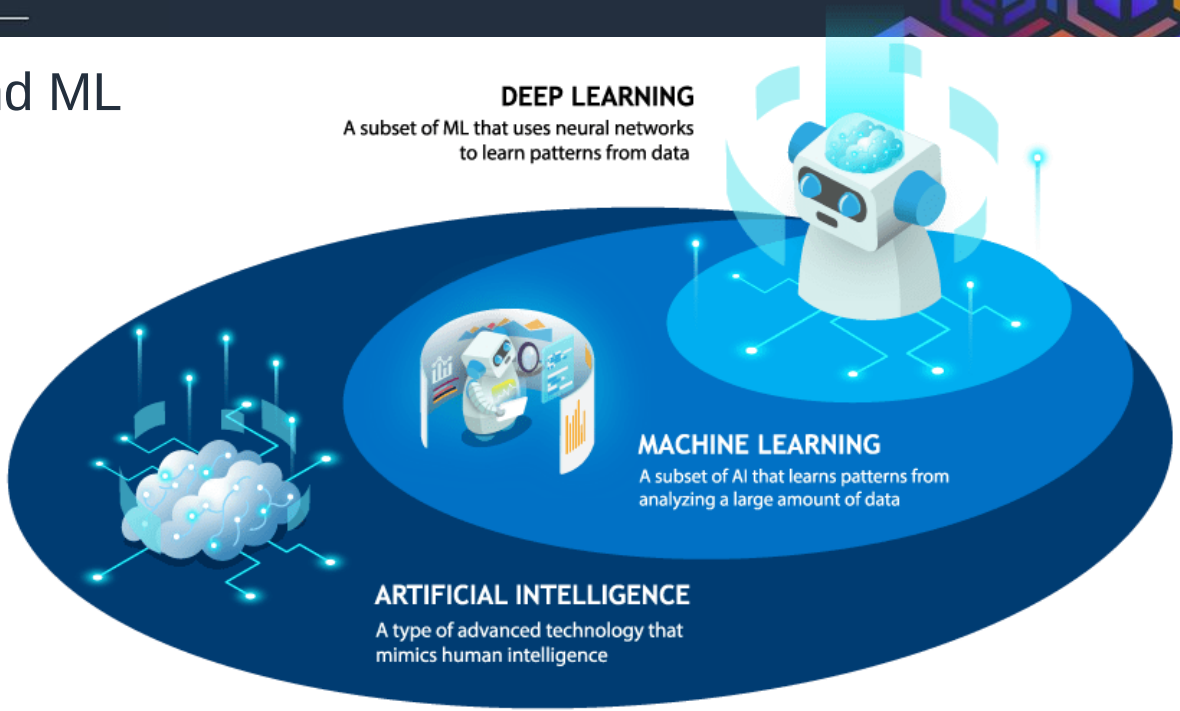
AI WILL SOLVE ALL PROBLEMS

AI MAY KILL US

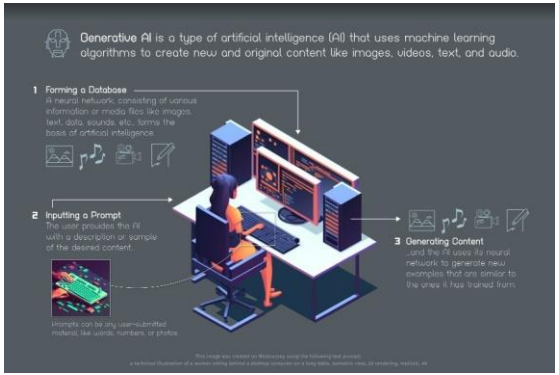
Introduction to AI and ML

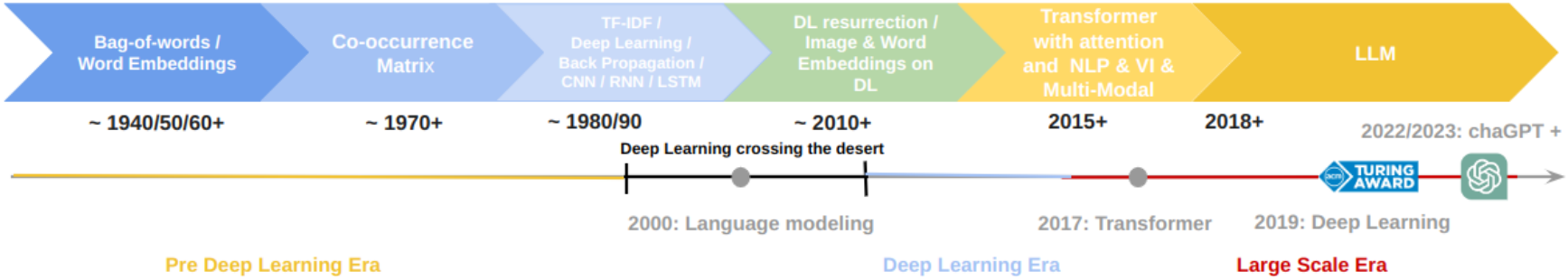


Introduction to AI and ML



Generative AI





aws COMMUNITY DAY AOTEAROA

Generative AI

Analysis	Design	Development	Testing	Deployment	Maintenance
• 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

aws

COMMUNITY DAY

AOTEAROA

Artificial Super Intelligence

Beyond human intelligence

Artificial General Intelligence

Replicates humans

Artificial Narrow Intelligence

Goal oriented intelligence

aws COMMUNITY DAY AOTEAROA

Human-Computer Interface

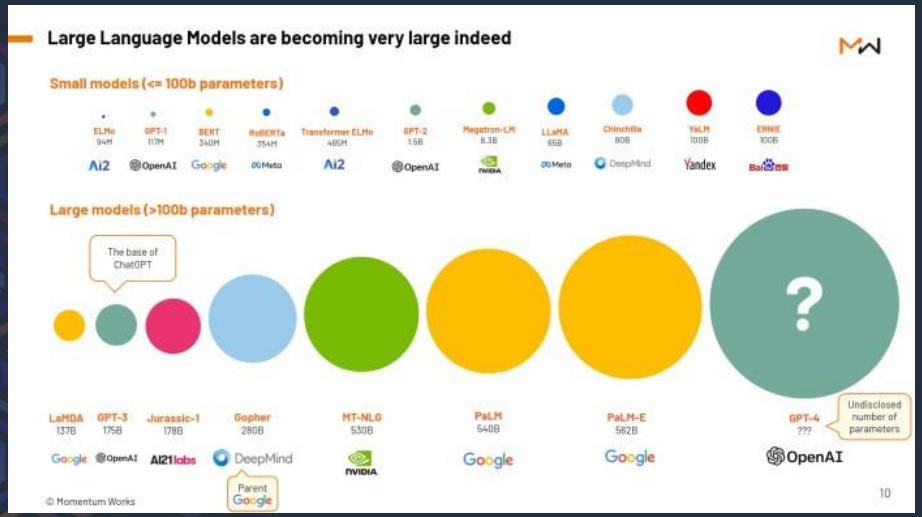
Graphical User Interface

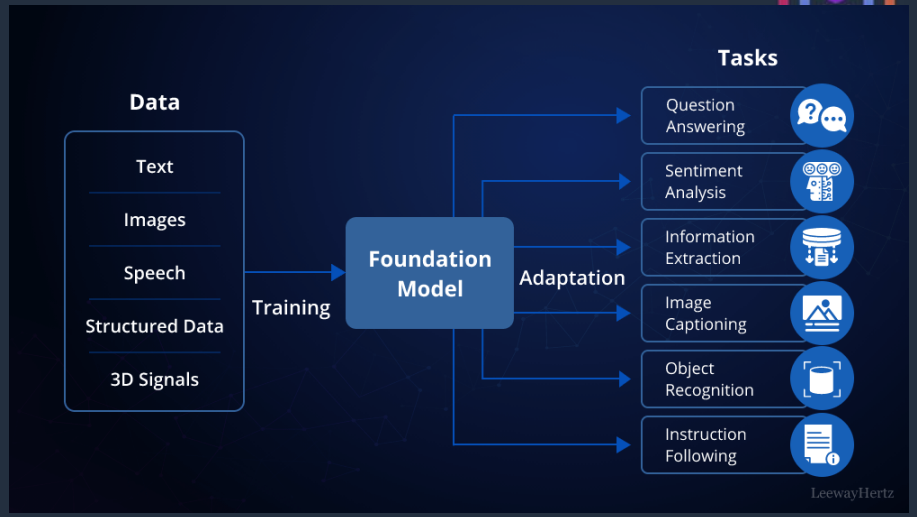
Command line interface

Natural language interface

aws
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.



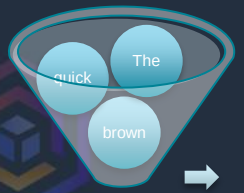


aws COMMUNITY DAY AOTEAROA

How LLMs work

Prompt

The quick brown fox



TOK

Context

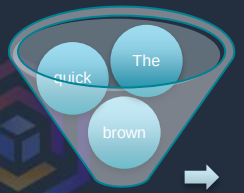
The(1) quick(10) brown(4) fox(2)

aws COMMUNITY DAY AOTEAROA

How LLMs work

Prompt

The quick brown fox



TOK

Context

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

DTOK

Output

The quick brown fox jumps over the lazy dog.

aws COMMUNITY DAY AOTEAROA

Prompt Engineering

Zero short inference

Prompt

One shot inference

Prompt

Example

few shot inference

Prompt

Multiple examples

aws COMMUNITY DAY AOTEAROA

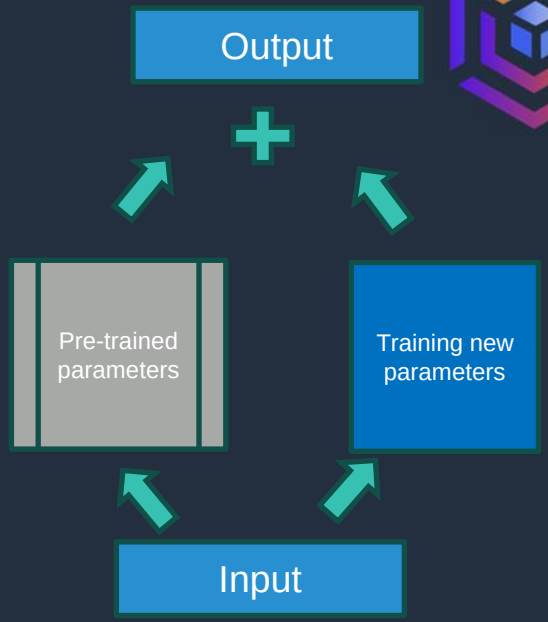
Fine tuning techniques:

Repurpose the model

Unsupervised vs supervised fine-tuning

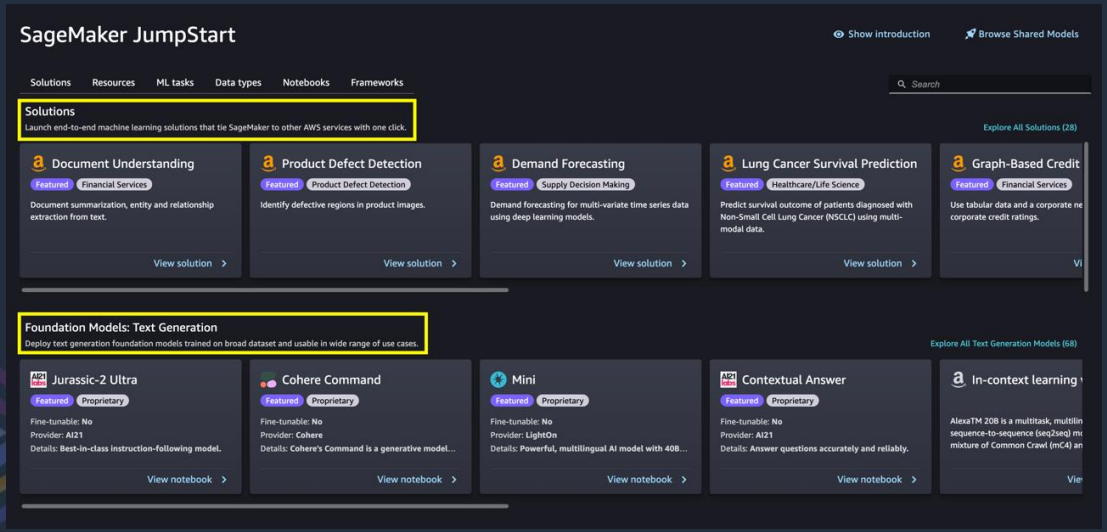
Reinforcement learning from Human Feedback(RLHF)

Parameter Efficient Fine Tuning(PEFT)



aws
COMMUNITY DAY
AOTEAROA

AWS Sagemaker Jumpstart -



aws COMMUNITY DAY AOTEAROA

Examples of LLMs

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

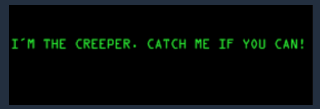
Théâtre d’Opéra Spatial (Image credit: Jason Allen)

aws COMMUNITY DAY AOTEAROA

The threat of the entity

aws 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



aws COMMUNITY DAY AOTEAROA

Security is asymmetrical problem- Why?

aws COMMUNITY DAY AOTEAROA

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 Churchil

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

aws

COMMUNITY DAY

AOTEAROA

aws
COMMUNITY DAY
AOTEAROA

The key to control

AI-Based solutions

Detect and respond in real-time

Continuously learn and adapt

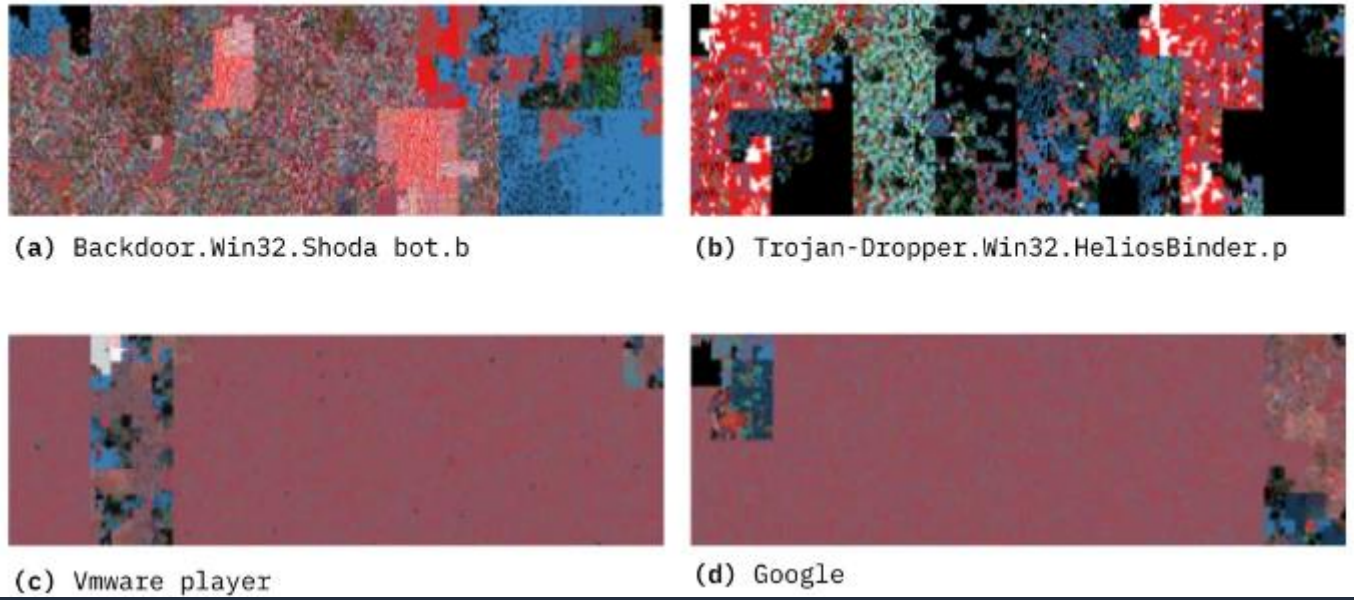
Analyse user behavior

Analyse security logs

Detection anomaly in the network

aws COMMUNITY DAY AOTEAROA

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



aws COMMUNITY DAY AOTEAROA

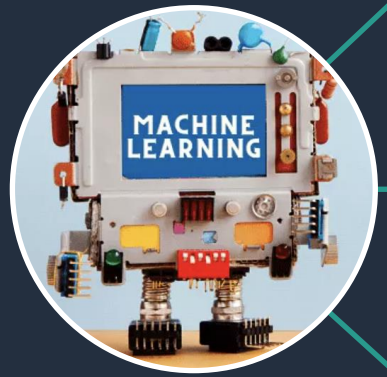
When cyber attacks meet financial crime

- 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.

aws COMMUNITY DAY AOTEAROA

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

aws
COMMUNITY DAY
AOTEAROA

The battle for control

aws COMMUNITY DAY AOTEAROA

Generative AI – Curse or a boon

Curse

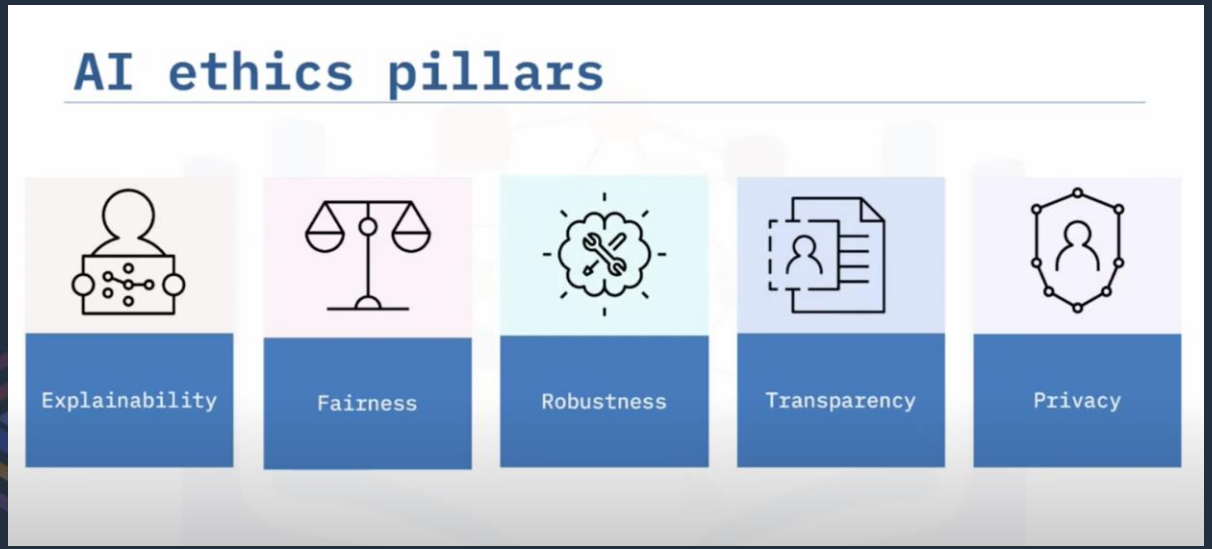
- Deepfakes
- Text generation-phishing emails
- Image generation
- Audio generation
- Synthetic data
- Automated frauds

Boon

- Efficient threat reporting
- Enhanced Vulnerability Management
- Automated incident response
- Policy generation
- Simulation

aws COMMUNITY DAY AOTEAROA

AI Ethics pillars



aws COMMUNITY DAY AOTEAROA

Guardrails

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

aws 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

aws

COMMUNITY DAY

AOTEAROA