OPERATIONAL RESEARCH SOCIETY

ISMOR

INTERNATIONAL SYMPOSIUM on MILITARY OPERATIONAL RESEARCH

Presentation Session 2a *AI in Defence*

2a.1 GenAI for Defence Use Cases and Requirements

Wednesday 16 July, 2025
09:20 - 09:50
Hopkinson

Scott Mongeau
PhD MBA MA MA GD
ORSoc CSci, INFORMS CAP
CSci Chartered Scientist
Lead Engineer
NATO & UK/EU Defence Sector
Google Cloud
smongeau@google.com

Alphabet Google Cloud

NATO OTAN

Alphabet
Google Cloud

1. Google Cloud & AI
2. AI for Defence
3. GenAI Opportunities
4. GenAI as OR Compliment
5. Q&A

A. Appendix

01

Google Cloud AI in Context

Alphabet

Google Ventures
Venture & capital funding

Calico
Longevity Research

Google X
Innovation Lab & Research

Verily
Improving Quality of Life

DeepMind
Artificial Intelligence & Machine Learning

SideWalk Labs
Solving Big Urban Problems

Intrinsic
Robotics software

Google Fiber
High Speed Internet Services

Jigsaw
Online Global Security Solutions

Waymo
Self Driving Vehicles

Wing
Drone Freight delivery

Capital G
Technology venture capital

Google

Search
Search Engine

Google Cloud
Cloud Services, Workspace

Maps
Mapping, location services & logistics

Ads & Google Marketing
SEM & Ad Technology Stack

Google Play
Digital app distribution

Android
Mobile operating system

Hardware
Pixel, Chromecast, Home, Fitbit

YouTube
Internet video service

Chrome
OS & secure web browser

Google Research
Google Quantum AI

Google's unified AI stack

>10 years of R&D leadership

3,000 Researchers || 7,000 Publications

Integrated Gemini assistants

Gemini for Google Cloud | Gemini for Google Workspace

AI Applications and Agents

Google pre-built | Customer built

Google Agentspace

Enterprise Search | NotebookLM | Agent Garden

Vertex AI

Model Garden | Model Builder | Agent Builder

Data

Multimodal | Vector Search | AI Insights | Data Science

Models

Gemini | Imagen | Veo | Partner | Open

AI Hypercomputer

Performance-optimized hardware | Open software | Flexible consumption

02

AI for Defence

AI Geoanalytics for Disaster & Damage Assessment

WHO

Support defence strategy & tactics, emergency response, humanitarian aid, and reconstruction planning

WHAT

Accurate post-disaster assessment from satellite imagery by extracting infrastructure damage analysis from high-resolution satellite imagery

HOW

Two-step process: ML object detection for buildings, followed by AI classification of damage likelihood using pre- and post-disaster imagery

WHICH

Achieved 71-78% accuracy in damage assessment, significantly accelerating aid delivery and helping to track Ukraine conflict and damage

- Satellite data machine learning reveals fighting in Ukraine
- Machine Learning-based Damage Assessment for Disaster Relief
- Detecting ships in Ukraine with Google Earth Engine
- Airbus: Charting new territory with Google Cloud

Drone imaging and AI for agriculture

Google

TARANIS

WHO

Taranis provides agribusinesses and farmers with critical AI-driven insights into crop health in order to maximize productivity and yield

WHAT

Needed to process and analyze massive amounts of drone aerial imagery and sensor data from agricultural fields to automate crop health monitoring, pest and disease detection, and nutrient deficiency analysis

HOW

Utilized Google Cloud's AI/ML capabilities, including Vision AI, Vertex AI, and BigQuery, to create a comprehensive agricultural intelligence platform

WHICH

Enabled precise, real-time insights to farmers, leading to improved crop yields, reduced input costs, and more sustainable farming practices

Helping farmers to feed the planet with cutting-edge drone imaging and AI

Infrastructure & Logistics

Drone AI for predictive maintenance

Billions of dollars in savings predicted

Examines tens of thousands of images to prioritize repairs

Identifies and predicts future repairs needed

Coral coral.ai

AI-based corrosion-detection system for U.S. Navy to automate inspections of vessels

U.S. Navy and Google Cloud jumpstart expansion across DoD

03

GenAI Opportunities

What can Multimodal Generative AI do?

Text

- Conversation
- Copywriting
- Brainstorming
- Summarization
- Grammar correction
- Question answering
- Translation
- Note taking (Speech to text)

Conceptual understanding

Reasoning

Distinguish cause & effect

Image

- Image generation (Text to image)
- Design

Voice

- Voice synthesis (Text to audio)

Video

- Video generation (Text to video)

3D

- 3D models/scenes (2D to 3D)

Code

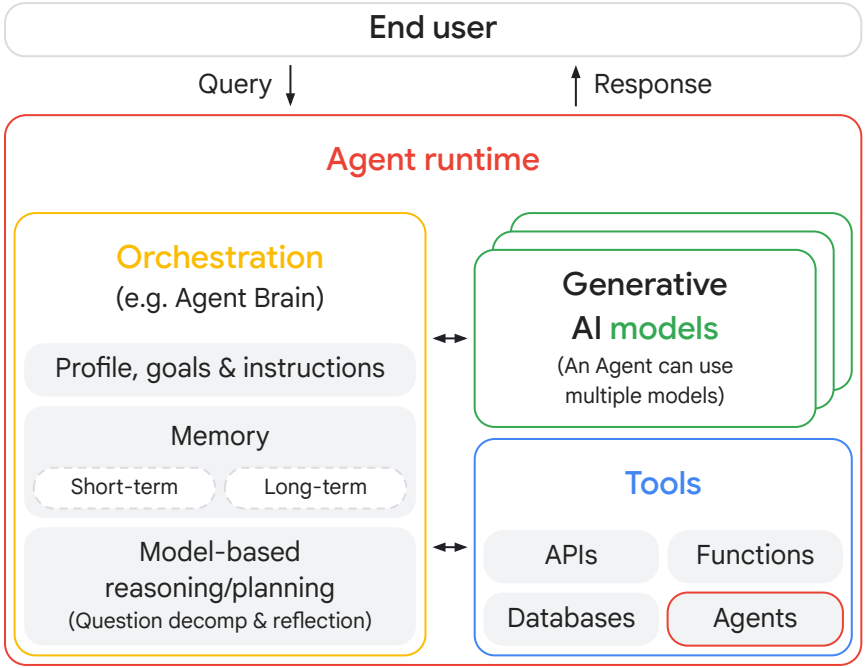
- Code generation
- Code documentation
- Text to SQL

Other

- Play games
- Music
- Audio
- Biology & chemistry
- Robotics

... and more

AI Agents plan, reason, and execute tasks for users



Four key components

Model(s)
Used to reason over goals, determine the plan and generate a response

Tools
Fetch data, perform actions or transactions by calling other APIs or services

Orchestration
Maintain memory and state (including the approach used to plan), tools, data provided/fetched, etc.

Runtime
Execute the system when invoked

GenAI Agentspace

cloud.google.com/products/agentspace

Single hub for a wide array of specialized agents

- Search across text, image, video
- Agents to summarise, reason, and interpret complex information
- Agents to take action on routine tasks
- Build your own custom agents
- Google expert agents (e.g. research, ideas, cyber, medical)

Examples

- NotebookLM
- Multimodal Search
- Deep Research Agent
- Idea Generation Agent
- Custom - Agent Designer (Agent Dev Kit)

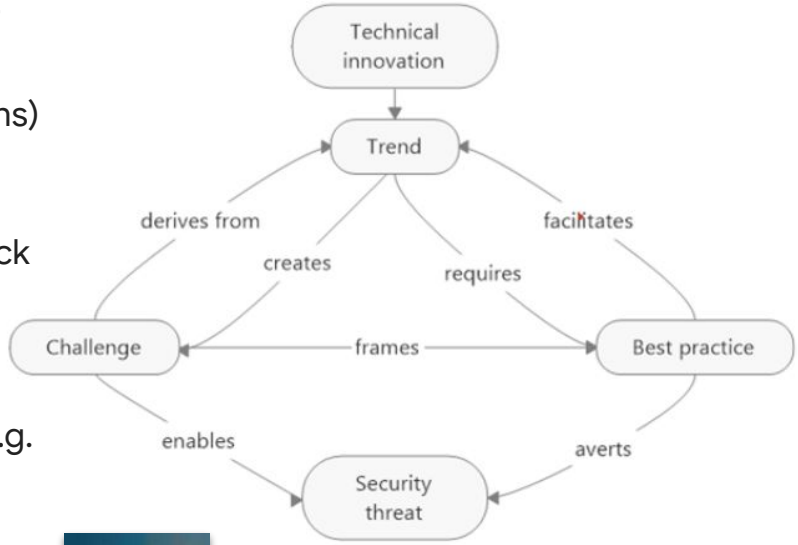
GenAI/LLM Cyber threats and defences

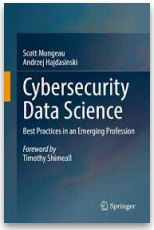
1. Semantic: generation of misinformation / fake news (e.g. propaganda campaigns)

2. Strategic: generation of high-level novel cyber attack strategies

3. Tactical: generation of novel procedural tactics (e.g. Mitre ATT&CK sequences)

4. Structured: generation of malware, virus, and other threat vector code





Mongeau & Hajdasinski. 2022. Cybersecurity Data Science. Springer. 338p. https://doi.org/10.1007/978-3-030-74896-8

1. Semantic: a) generate misinformation topics to orient monitoring; b) content for labeling / detection;

2. Strategic: a) identify emerging threats / exploits; b) defense strategies

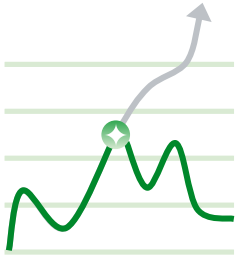
3. Tactical: a) identify threat categories for triage; b) generation of defense tactics

4. Structured: a) analysis of malware code; b) surface multivariate patterns indicative of particular threats; c) generating structured monitoring targets, rules, and code

GenAI for Cybersecurity

STOPPED
threats

Prevent Patient Ones

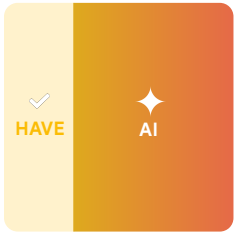


LESS
toil

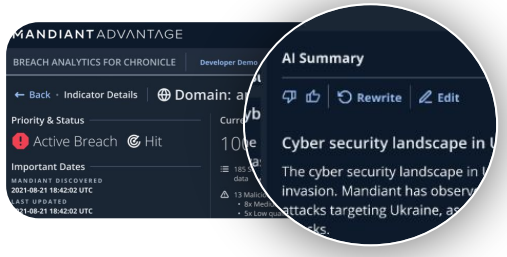
Systems secure themselves

SCALED
talent

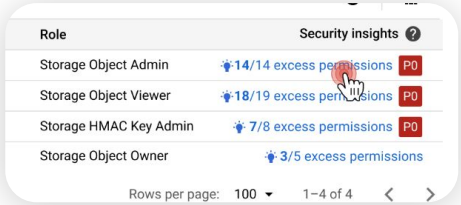
Democratize Security Expertise



AI-powered remediation with Frontline Threat Intel



Auto generate security controls, policies and configs



Novices => Experts

04

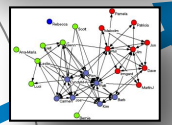
GenAI as OR Compliment

Continuum of Analytics Methods

AI = synergies across continuum

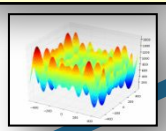
Optimizing Systems

SEMANTIC

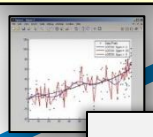


Synthesising Context & Meaning

PRESCRIPTIVE



PREDICTIVE



Forecasting & Probabilities

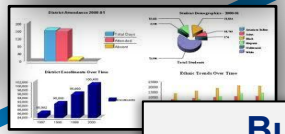
Understanding Patterns

Data visualization

Identifying Factors & Causes

DIAGNOSTICS

DESCRIPTIVE



Business Intelligence

DATA QUALITY

AI and OR synergies

Operations Research Supporting AI

- **Structured Frameworks:** OR provides a structured approach to problem-solving - valuable when developing AI systems for complex tasks.
- **Constraint Satisfaction:** OR techniques, like constraint programming, can help AI models handle complex constraints in real-world scenarios.
- **Optimization Algorithms:** OR algorithms, such as those used in linear programming, can be used to optimize the performance of AI models (i.e. training and hyperparameter tuning).
- **Decision Support Systems:** OR methods are increasingly integrated into AI-powered decision support systems, providing a framework for interpreting AI predictions and making informed decisions.

AI Enhancing Operations Research

- **Improved Prediction:** AI, particularly machine learning, can analyze vast datasets to predict future demand, resource availability, or other factors crucial for OR models. For example, AI can predict when and where demand will occur, allowing for better resource allocation.
- **Dynamic Decision Making:** By integrating AI's predictive capabilities with OR's optimization, organizations can create more adaptive and responsive decision-making systems.
- **Reinforcement Learning:** AI techniques like reinforcement learning, which involves learning through trial and error, can be used in OR to optimize sequential decision-making processes.

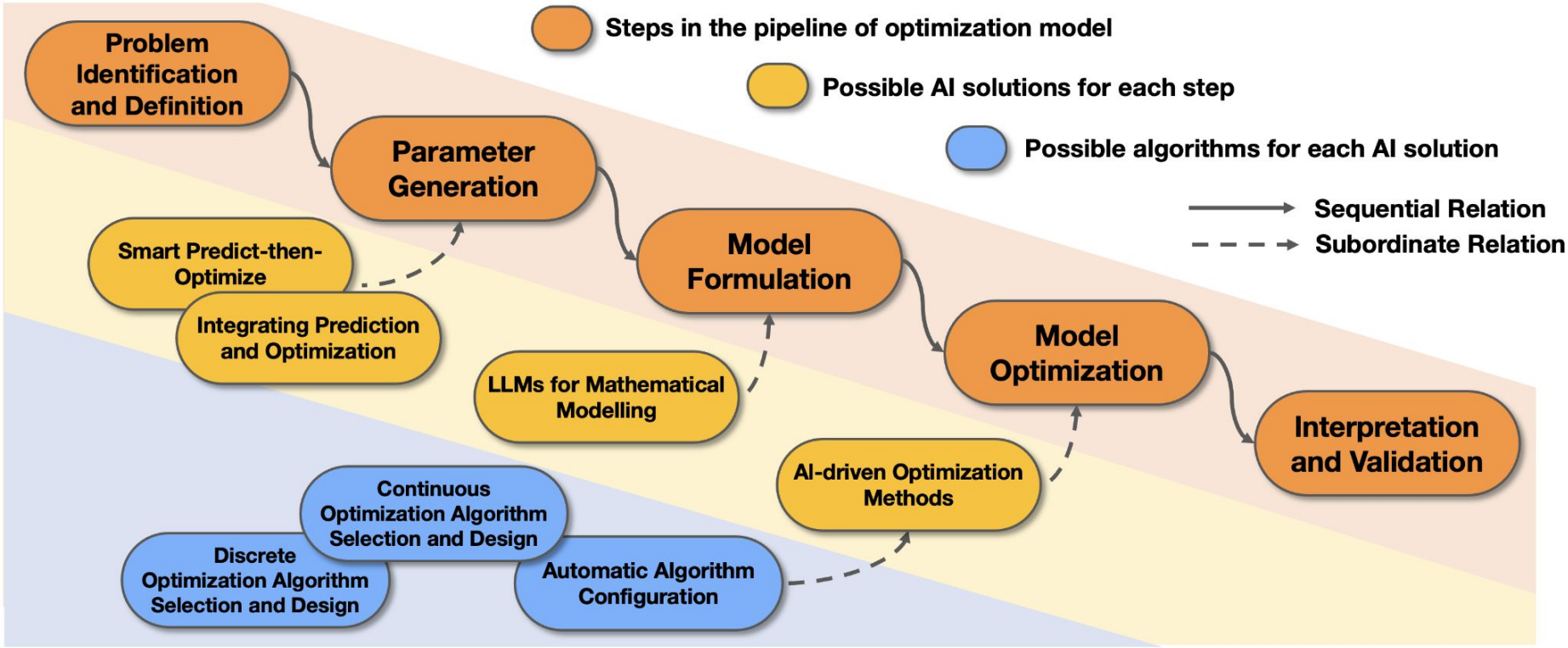
Examples of Integration

- **Supply Chain Management:** AI can be used to optimize logistics, inventory management, and other aspects of supply chain operations, while OR provides the framework for decision-making.
- **Resource Allocation:** AI can help predict resource needs, and OR techniques can be used to optimize the allocation of those resources in an efficient manner.
- **Planning and Scheduling:** OR and AI can be combined to optimize complex planning and scheduling problems, such as hospital scheduling or emergency services deployment.

Artificial Intelligence for Operations Research: Revolutionizing the Operations Research Process

arxiv.org/html/2401.03244v1/#S2 [math.OC] 06 Jan 2024

Zhenan Fan, Bissan Ghaddar, Xinglu Wang, Linzi Xing, Yong Zhang, Zirui Zhou



AI for procurement operations efficiency

Automate tasks

AI can be used to automate many of the tasks involved in procurement, such as data entry, contract management, and supplier evaluation.

Improve efficiency

AI can help to improve the efficiency of the procurement process by identifying opportunities for cost savings and streamlining workflows.

Reduce costs

AI can be used to analyze data and provide insights that can help procurement professionals make better decisions and reduce costs.

Build relationships

AI can be used to build relationships with suppliers by providing them with personalized support and communication.

Manage risk

AI can be used to manage risk in the procurement process by identifying potential risks and developing mitigation strategies.

When used together, digital transformation, process automation, and artificial intelligence can have a significant impact on procurement effectiveness as well as on the cost of procurement.

05

Conclusion / Q&A

Google

Lockheed Martin Collaboration

WHO

Collaboration between the aerospace and defense company Lockheed Martin and Google

WHAT

Integration of Google's advanced generative AI technologies into Lockheed Martin's existing AI Factory ecosystem

HOW

Adding Google Vertex AI platform into Lockheed Martin's system to enhance the training, deployment, and sustainability of AI models within a secure framework

WHICH

Accelerates AI-driven capabilities and enhanced performance in critical areas like national security, aerospace applications, scientific discovery, and operational efficiencies

Lockheed Martin and Google Cloud Collaboration to Advance Generative AI

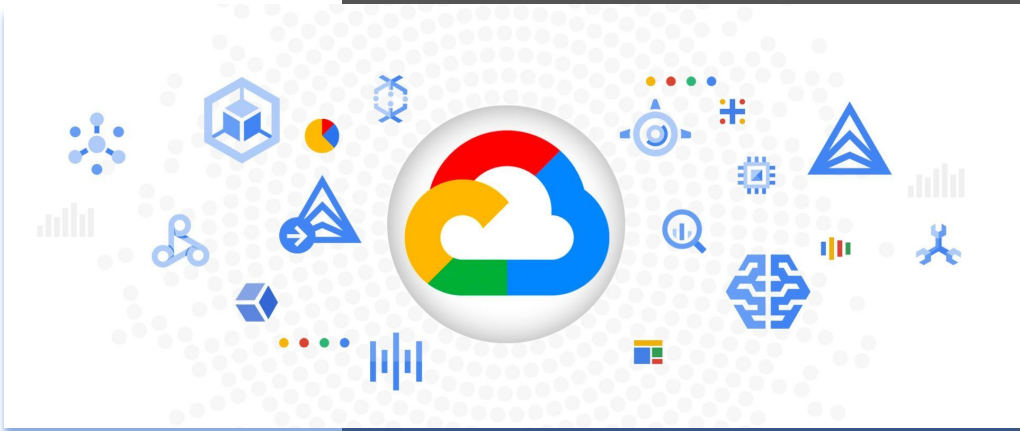
Transforming US DoD's data utilization with Generative AI

Challenge: The Department of Defense (DoD) possesses vast amounts of data, but struggles to effectively utilize it for decision-making due to data silos, complex formats, and the sheer volume of information.

Requirement: Transform data utilization by leveraging generative AI to improve data accessibility, analysis, and insights.

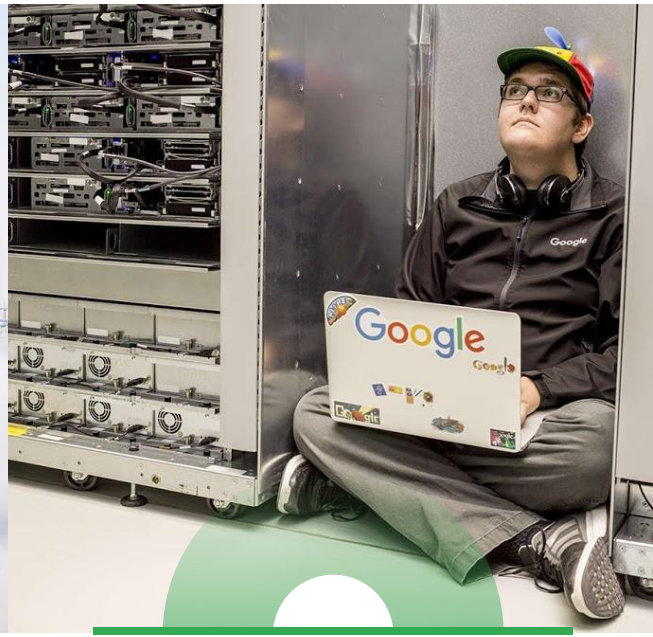
Solution: The article discusses how the DoD is exploring and implementing generative AI to synthesize information from multiple sources, automate data analysis tasks, and generate insights that can inform strategic and operational decisions.

Results: Generative AI has the potential to significantly enhance the DoD's ability to leverage its data assets, leading to improved situational awareness, faster decision-making, and more effective operations.



Transforming DoD's data utilization with Generative AI

Sharing Google's organisational code with our customers



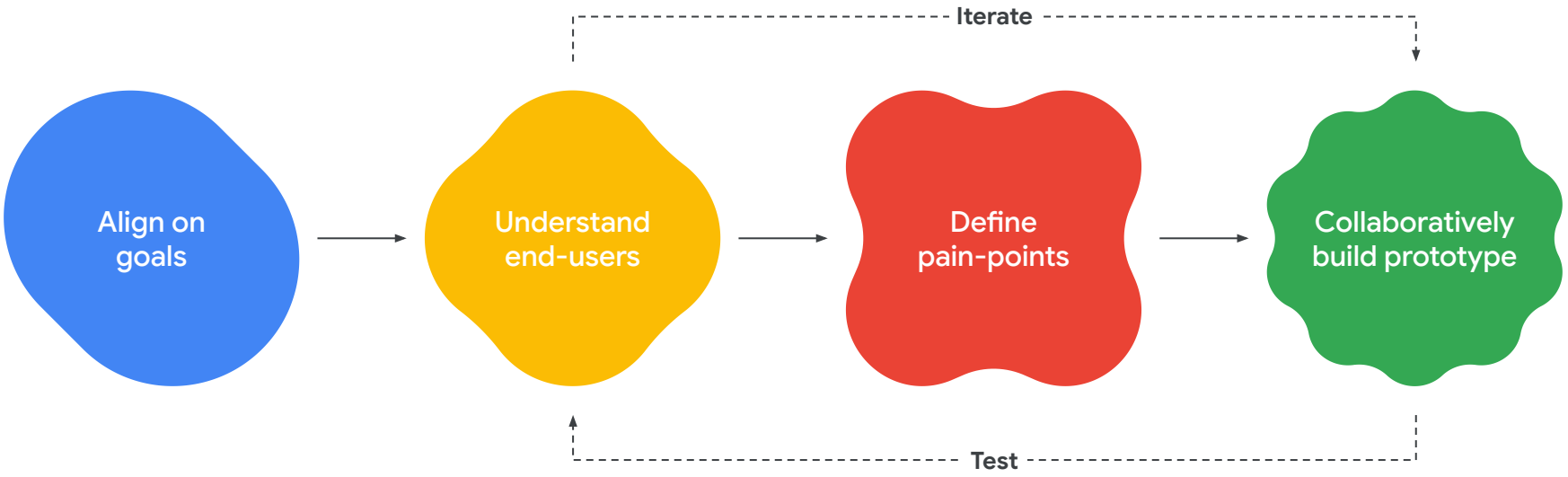
Culture & organisation Transformation

On demand, best in class processes & technology

Data driven decision making & intelligent automation

Google Cloud

Google Sprint GenAI Prototype Co-creation

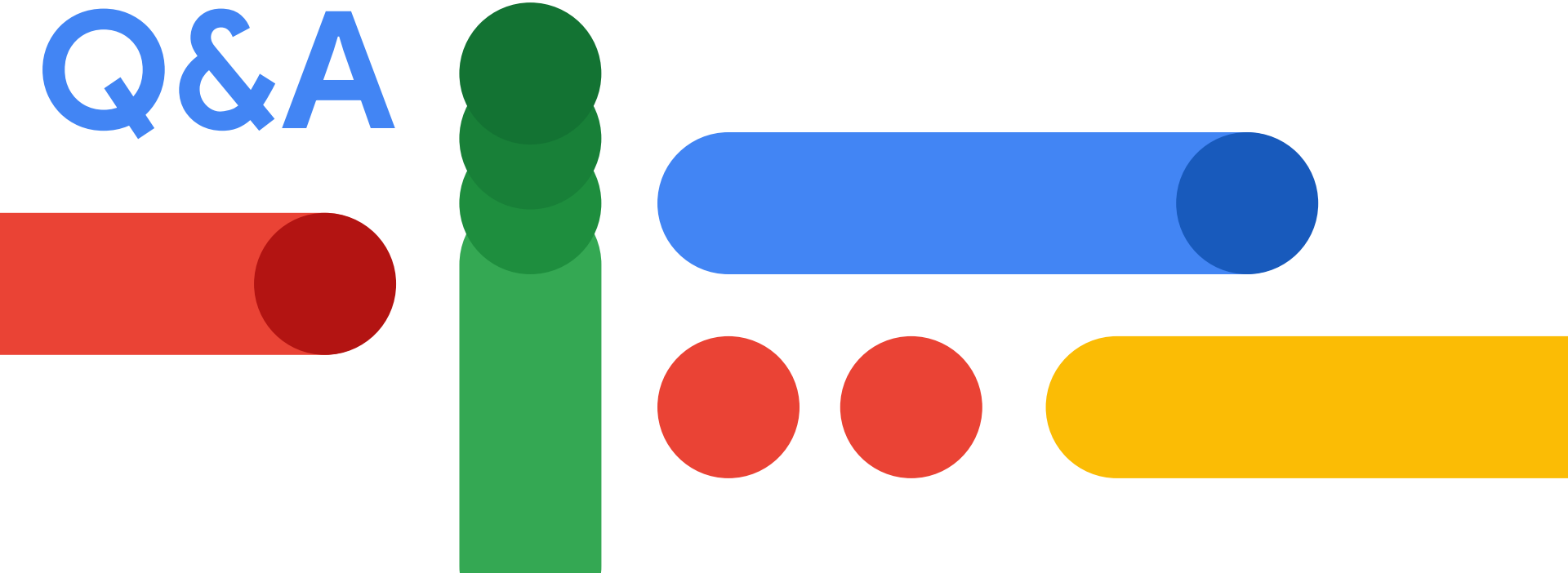


Google Cloud GenAI Resources

Learn about GenAI on Google Cloud	GenAI Live Labs Events	Join GenAI Trusted Tester Program	GenAI Consulting	GenAI Training

Thank you!

Q&A



APPENDIX

Google

Sovereignty

Sovereignty & Privacy

To meet policy, regulatory, and organizational objectives

Cloud on Europe´s terms

Compliance

Compliance & Control

Achieving compliance through controls, tracking, and reporting

cloud.google.com/security/compliance

Security

Security & Assurance

Infrastructure designed, built, and operated to assure against threats

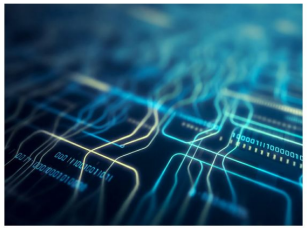
cloud.google.com/security/best-practices

BLOG **Engineering Trust** the cloud trust paradox: to trust cloud more, you need the ability to trust it less...

AI Thought Leadership

Google Cloud

Google Cloud's Approach to Trust in Artificial Intelligence



By: Marina Kaganovich, Rohan Kanungo, and Heidi Hanesen

The cover image was generated by Gemini.

From turnkey to custom: Tailor your AI risk governance to help build confidence

October 17, 2023

Google Cloud

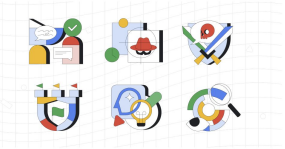
Securing AI: Similar or Different?

Anton Chuvakin, John Stone, Tanya Popova-Jones at Office of the CISO, Google Cloud

Google

Secure AI Framework Approach

A quick guide to implementing the Secure AI Framework (SAIF)



Google

Secure, Empower, Advance

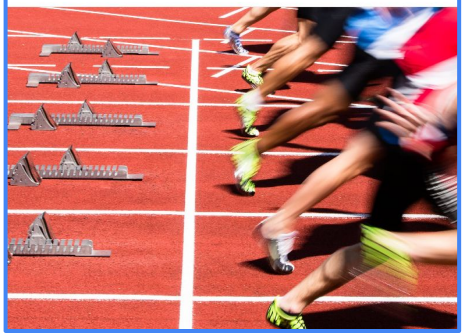
How AI Can Reverse the Defender's Dilemma

Spotlighting 'shadow AI': How to protect against risky AI practices

December 15, 2023

Gen AI governance: 10 tips to level up your AI program

January 31, 2024



The Prompt: What to think about when you're thinking about securing AI

August 23, 2023

Security & Identity

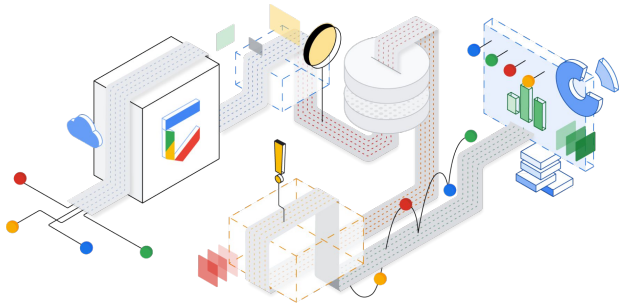
How to craft an Acceptable Use Policy for gen AI (and look smart doing it)

May 14, 2024

Links to Key Google AI Resources

Google Cloud Controls / Security Guidance

- Google Cloud's Approach to Trust in Artificial Intelligence
- Generative AI, Privacy, and Google Cloud
- Securing AI: Similar or Different?
- Why Red Teams Play a Central Role in Helping Organizations Secure AI Systems
- Security controls for Vertex AI
- Secure, Empower, Advance: How AI Can Reverse the Defender's Dilemma
- Best Practices for Securely Deploying AI on Google Cloud
- 7 key questions CISOs need to answer to drive secure, effective AI
- Coalfire evaluates Google Cloud AI: "Mature," ready for governance, compliance
- Navigating the EU AI Act: Google Cloud's Proactive Approach
- Google Cloud's commitment to responsible AI is now ISO/IEC certified



Vertex AI

- Overview of Generative AI & corresponding resources
- Certifications

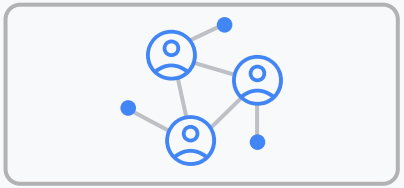
Legal

- GCP Terms
- GC Service Terms
- GC Services Summary
- Protecting customers with Generative AI Indemnification (blog)
- Cloud Data Processing Addendum

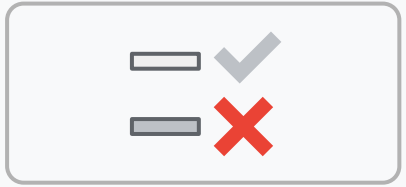
AI Frameworks

- Introducing Google's Secure AI Framework
- Secure AI Framework Approach
- SAIF Risk Assessment
- Applying Model Risk Management Guidance to Artificial Intelligence / Machine Learning-based risk models
- Generative AI Risk Management in Financial Institutions

Google is committed to developing AI responsibly



1 Be socially beneficial

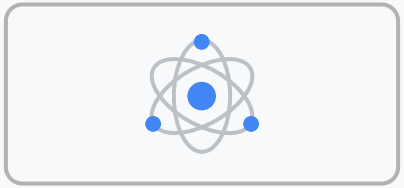


2 Avoid creating or reinforcing unfair bias

3 Be built and tested for safety

4 Be accountable to people

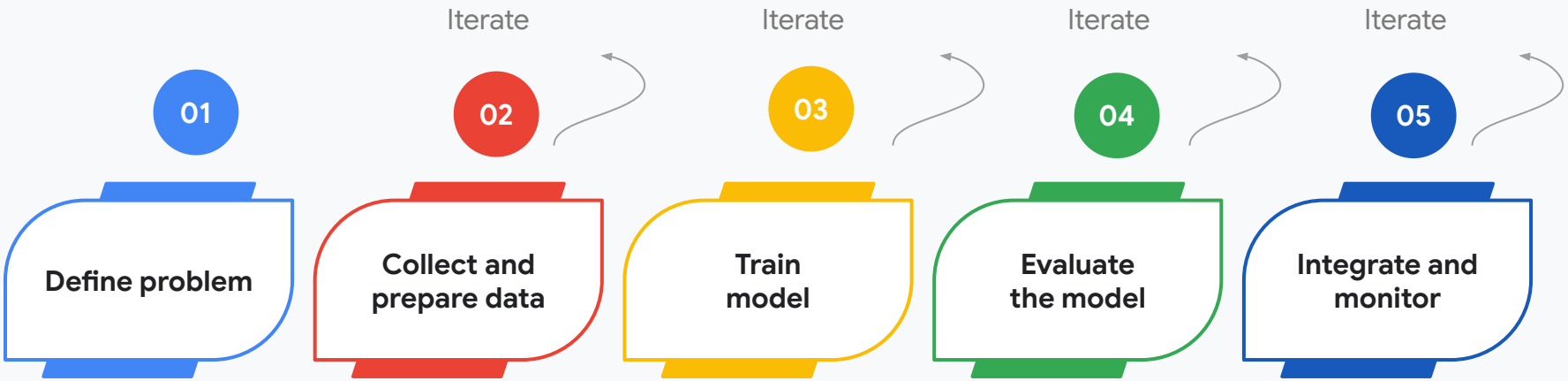
5 Incorporate privacy design principles



6 Uphold high standards of scientific excellence

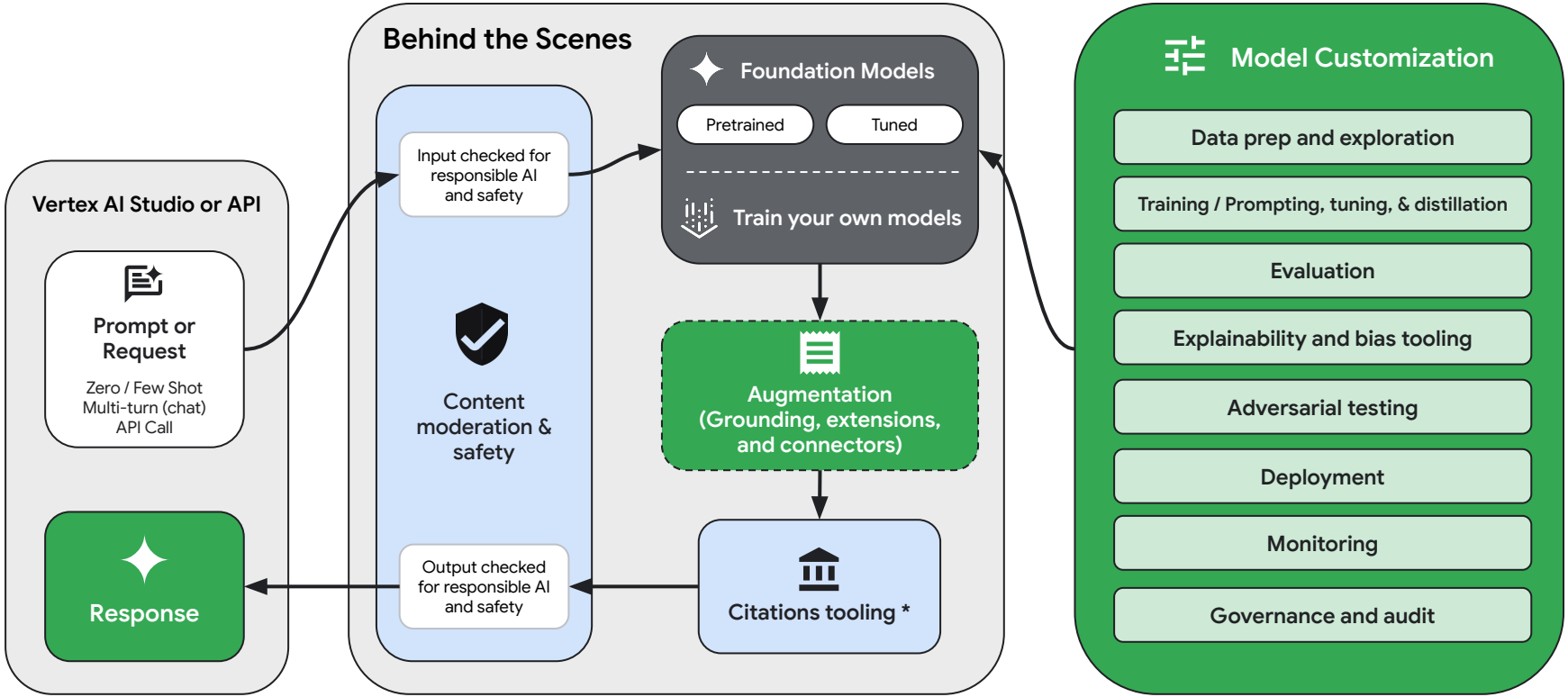
7 Be made available for uses that accord with these principles

Building AI responsibly requires a structured process



Reviews happen before our products are released for general availability.

Responsible AI Tooling, Enablement, and Support



* Applicable to first-party foundation models only

Built on a foundation of enterprise readiness

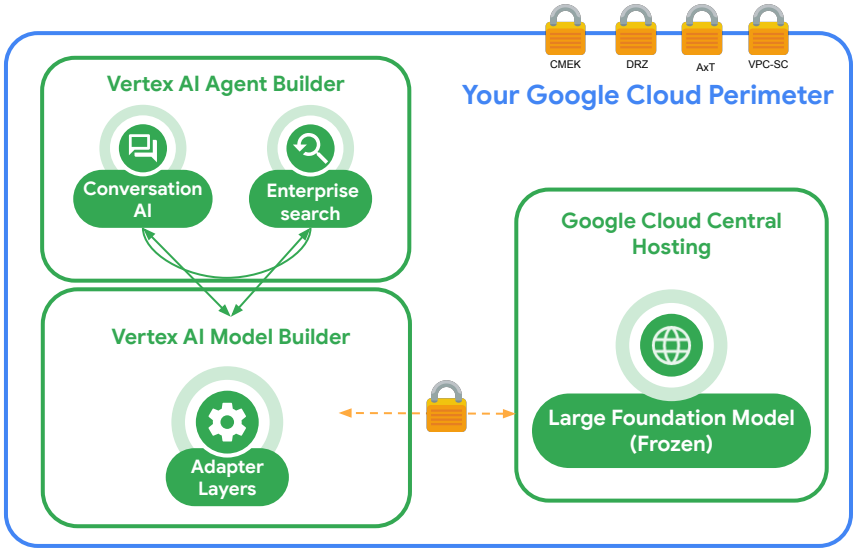
Whether 1st-party, 3rd-party, or open-source, Google Cloud gives you the tools, services, and infrastructure to make every deployment enterprise ready

Data governance, indemnity, and privacy

Security and compliance support

Reliability and sustainability

Responsible AI



- You own and control your data, not Google
- Security Controls with VPC-SC, CMEK, access transparency
- Intellectual property indemnity for training data and generated output
- Cost Controls with Dynamic Workload Scheduler and Provisioned Throughput
- Responsible AI tooling, enablement and support