cloud security alliance®

Mariner Guide to Protecting Regulated Data in Cloud and AI

Why it can’t be completed and how we will write it

Much of Generative AI remains unchartered, bringing unknown opportunities and unforeseen risk

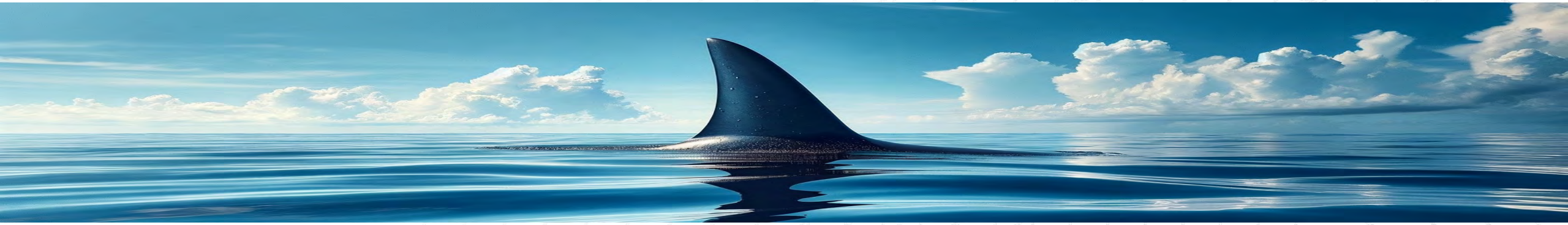
Evolving Cybersecurity Sophistication

Authentication will never be the same: Vishing attacks and deep fake bio attacks

Misconfigurations and targeted supply chain attacks

Expanded number of malicious actors with the ability to generate attacks

New attack surface with difficulty to find the "database" things pull from



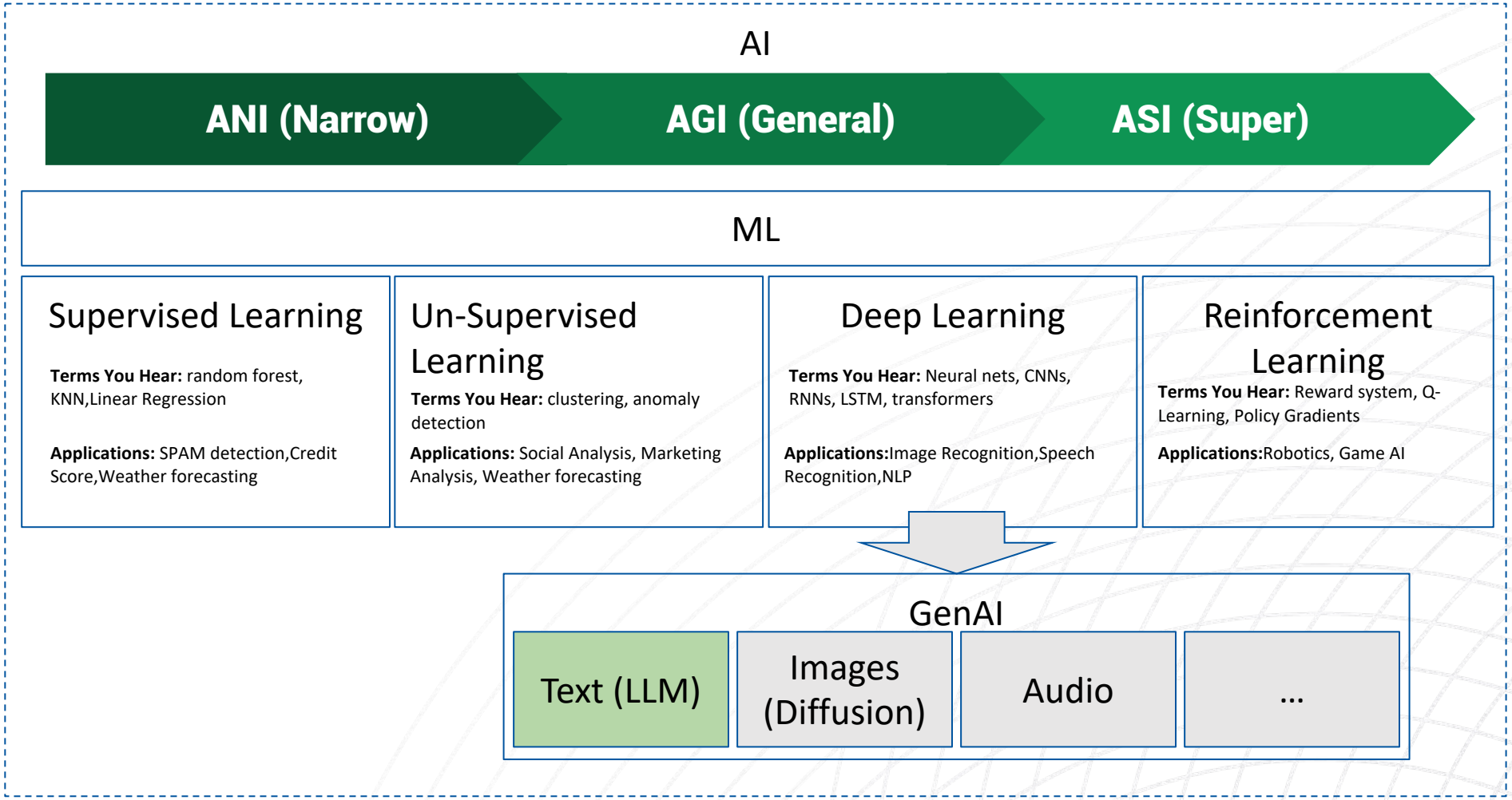
ABOUT THE CLOUD SECURITY ALLIANCE

"To promote the use of best practices for providing security assurance within Cloud Computing and provide education on the uses of Cloud Computing to help secure all other forms of computing."

- **Building security best practices for next generation IT**
- **Global, not-for-profit organization**
- **Research and Educational Programs**
- **Cloud Provider Certification**
- **User Certification**
- **The globally authoritative source for Trust in the Cloud**

How my background has me cautiously optimistic

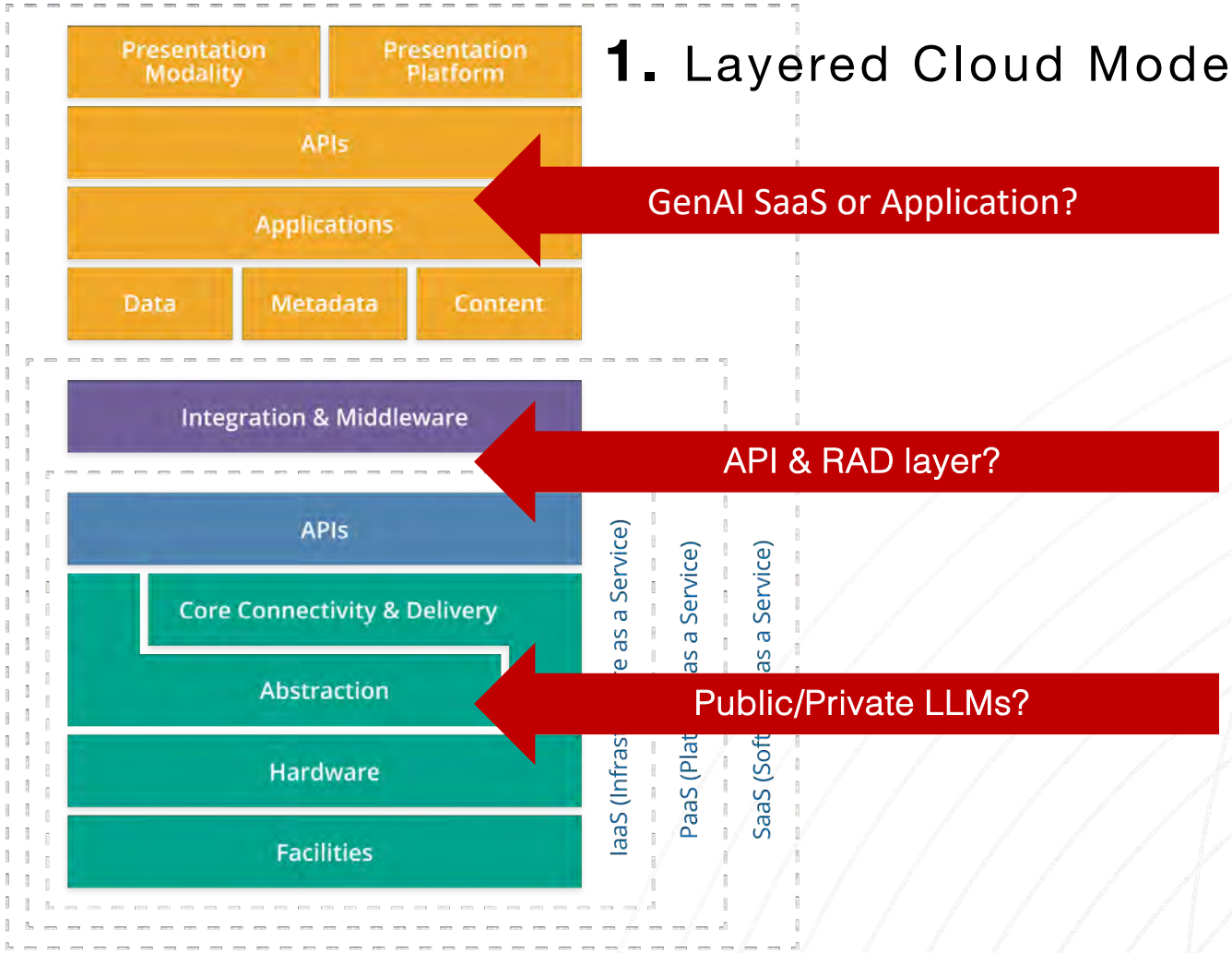
AI Family


AI
ANI (Narrow)
AGI (General)
ASI (Super)
ML
Supervised Learning
Terms You Hear: random forest, KNN,Linear Regression
Applications: SPAM detection,Credit Score,Weather forecasting
Un-Supervised Learning
Terms You Hear: clustering, anomaly detection
Applications: Social Analysis, Marketing Analysis, Weather forecasting
Deep Learning
Terms You Hear: Neural nets, CNNs, RNNs, LSTM, transformers
Applications:Image Recognition,Speech Recognition,NLP
Reinforcement Learning
Terms You Hear: Reward system, Q-Learning, Policy Gradients
Applications:Robotics, Game AI
GenAI
Text (LLM)
Images (Diffusion)
Audio
...

Thinking about GenAI/LLMs in Cloud Context

From the 2009 Cloud Security Alliance archives

1. Layered Cloud Model



2. Shared Responsibility

3. Controls Frameworks & Risk Management Strategies

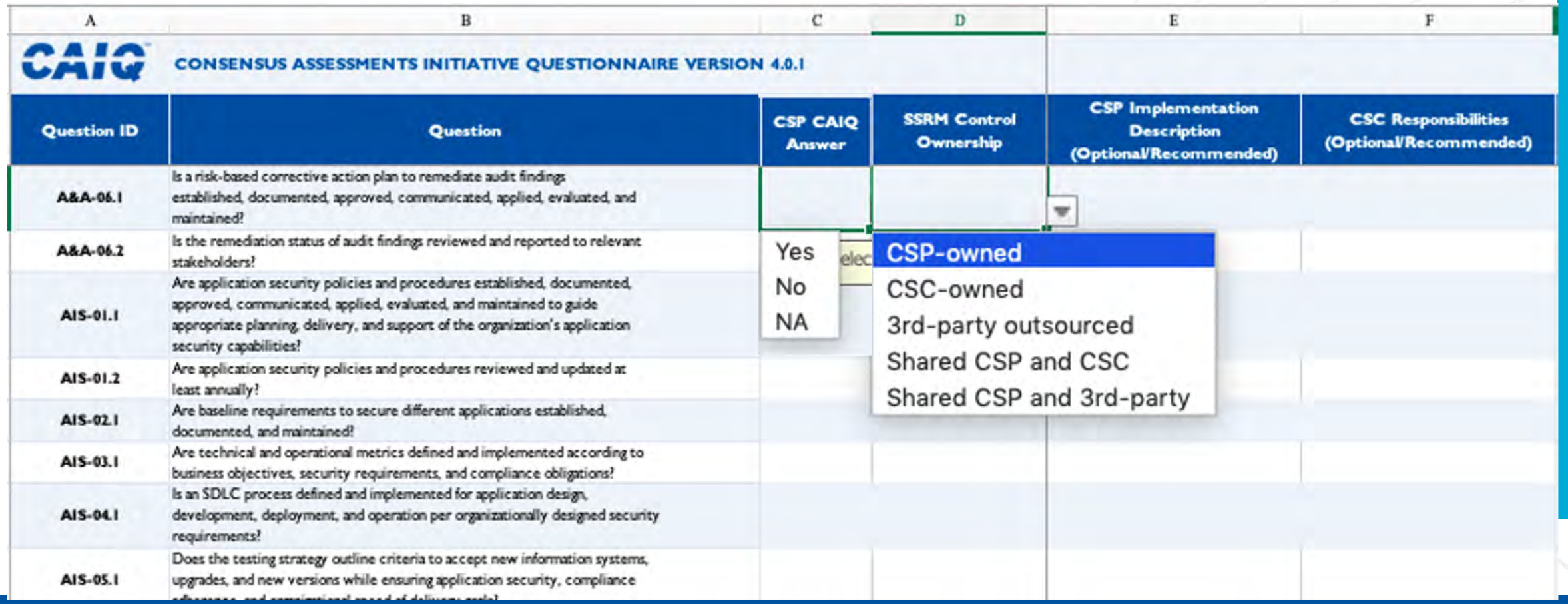
CCM Cloud Controls Matrix

PCI DSS COMPLIANT

AICPA SOC


THE SIX PILLARS OF
STAR™
Cloud Controls Matrix
CCM™
Cloud Controls Matrix
STAR Assessment Portfolio
STAR LEVEL ONE: SELF-ASSESSMENT
STAR
LEVEL ONE
SECURITY TRUST ASSURANCE & RISK
STAR LEVEL TWO: THIRD-PARTY AUDIT
STAR
LEVEL TWO
SECURITY TRUST ASSURANCE & RISK
STAR Registry
STAR™
REGISTRY
Assurance Education
CCAK™
STAR™
LEAD AUDITOR
TRAINING
STAR Enabled Solutions
CLOUD SECURITY ALLIANCE
STAR
Enabled
Solution
CSA
STAR Extended
STAR™
EXTENDED

CSP Self-Assessment Columns



A	B	C	D	E	F
CAIQ	CONSENSUS ASSESSMENTS INITIATIVE QUESTIONNAIRE VERSION 4.0.1				
Question ID	**Question**	**CSP CAIQ Answer**	**SSRM Control Ownership**	**CSP Implementation Description (Optional/Recommended)**	**CSC Responsibilities (Optional/Recommended)**
A&A-06.1	Is a risk-based corrective action plan to remediate audit findings established, documented, approved, communicated, applied, evaluated, and maintained?				
A&A-06.2	Is the remediation status of audit findings reviewed and reported to relevant stakeholders?				
AIS-01.1	Are application security policies and procedures established, documented, approved, communicated, applied, evaluated, and maintained to guide appropriate planning, delivery, and support of the organization's application security capabilities?				
AIS-01.2	Are application security policies and procedures reviewed and updated at least annually?				
AIS-02.1	Are baseline requirements to secure different applications established, documented, and maintained?				
AIS-03.1	Are technical and operational metrics defined and implemented according to business objectives, security requirements, and compliance obligations?				
AIS-04.1	Is an SDLC process defined and implemented for application design, development, deployment, and operation per organizationally designed security requirements?				
AIS-05.1	Does the testing strategy outline criteria to accept new information systems, upgrades, and new versions while ensuring application security, compliance				

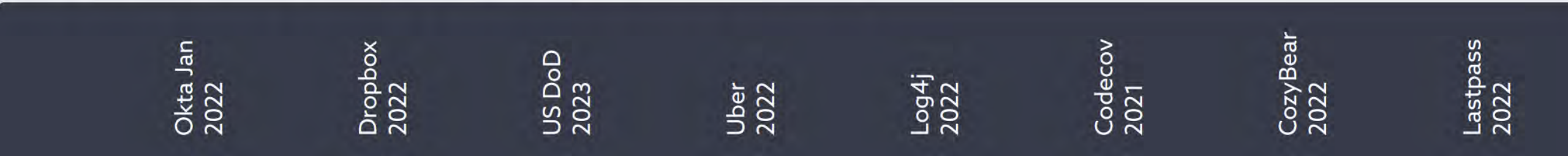
Evolving Cloud Security and Risk

Top Cloud Threats Coverage

In the 2022 "*Top Threats* to Cloud Computing - Pandemic Eleven" report, we surveyed over 700 industry experts on security issues in the cloud industry. Our respondents identified eleven important security issues to their cloud environment (ranked in order of concern indicated by the survey:

PE1. Insufficient Identity, Credentials, Access, and Key Management	PE7. System Vulnerabilities
PE2. Insecure Interfaces and APIs	PE8. Accidental Cloud Data Disclosure
PE3. Misconfiguration and Inadequate Change Control	PE9. Misconfiguration and Exploitation of Serverless and Container Workloads
PE4. Lack of Cloud Security Architecture and Strategy	PE10. Organized Crime/Hackers/APT
PE5. Insecure Software Development	PE11. Cloud Storage Data Exfiltration
PE6. Unsecured Third-Party Resources	

The top cloud concerns manifested in the breach cases covered this year are:



Rise of Cloud-Native and Multi-Cloud Strategies

75% of companies focusing primary development on cloud-native apps

45% have experienced security issues due to misconfiguration

57% of financial institutions using a multi-cloud strategy

Finding DORA and PCI DSS v4 Compliance in 2025 for CSPs

What the Future holds

Multi-factor Authentication will be ubiquitous

Zero Trust architecture will receive greater priority

Confidential Computing and SASE may simplify management

Machine-Learning Threat Detection will become a necessity

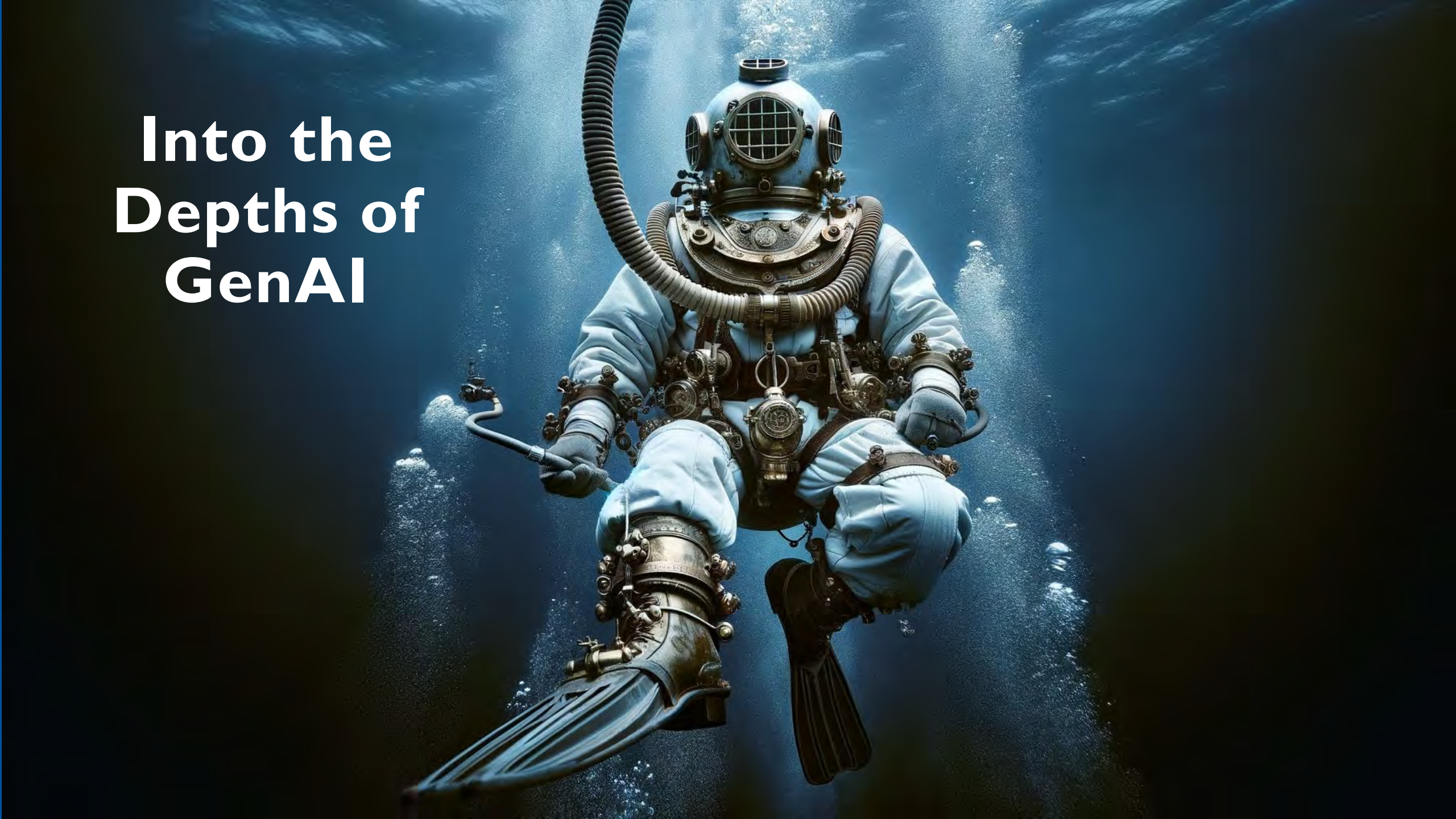
Cloud and AI

SaaS applications will use LLMs pervasively to address automation, personalization, user experience, analytics, scale, etc.

Cloud infrastructure providers will be dominant in providing LLMs to the market

Cloud providers will be able to expand compute power most efficiently

Into the Depths of GenAI



New Discoveries in AI

Scientific and technology breakthroughs with predictive analysis

Major improvements with automation and reporting

User and entity behavior analytics to improve experiences

Security Benefits

Better Coding

More real-time SBOM dependency and reporting

Compliance Automation Services

Self-healing apps


Blocks display code and outputs in different languages.
__init_
Define
elf.lang
elf.outp
elf.code
self.acti
self.live
Terminal
~ $ interpreter -y
> Make a virtual environment here
Sure, I can help with
A new way
to use computers
Open Interpreter lets LLMs run code on
your computer to complete tasks.

Speed of Understanding Threats Will Change

Threat hunters can correlate data much faster

Reverse engineering will be performed in real-time

AI-powered fuzzing constantly scans for s/w vulnerabilities at scale

Automated patch management will only increase in significance

Prompt Engineering for SOC Analysts will be mandatory training

Adversaries already in the wild

Phishing

Polymorphic code

FraudGPT

WormGPT

Reconnaissance

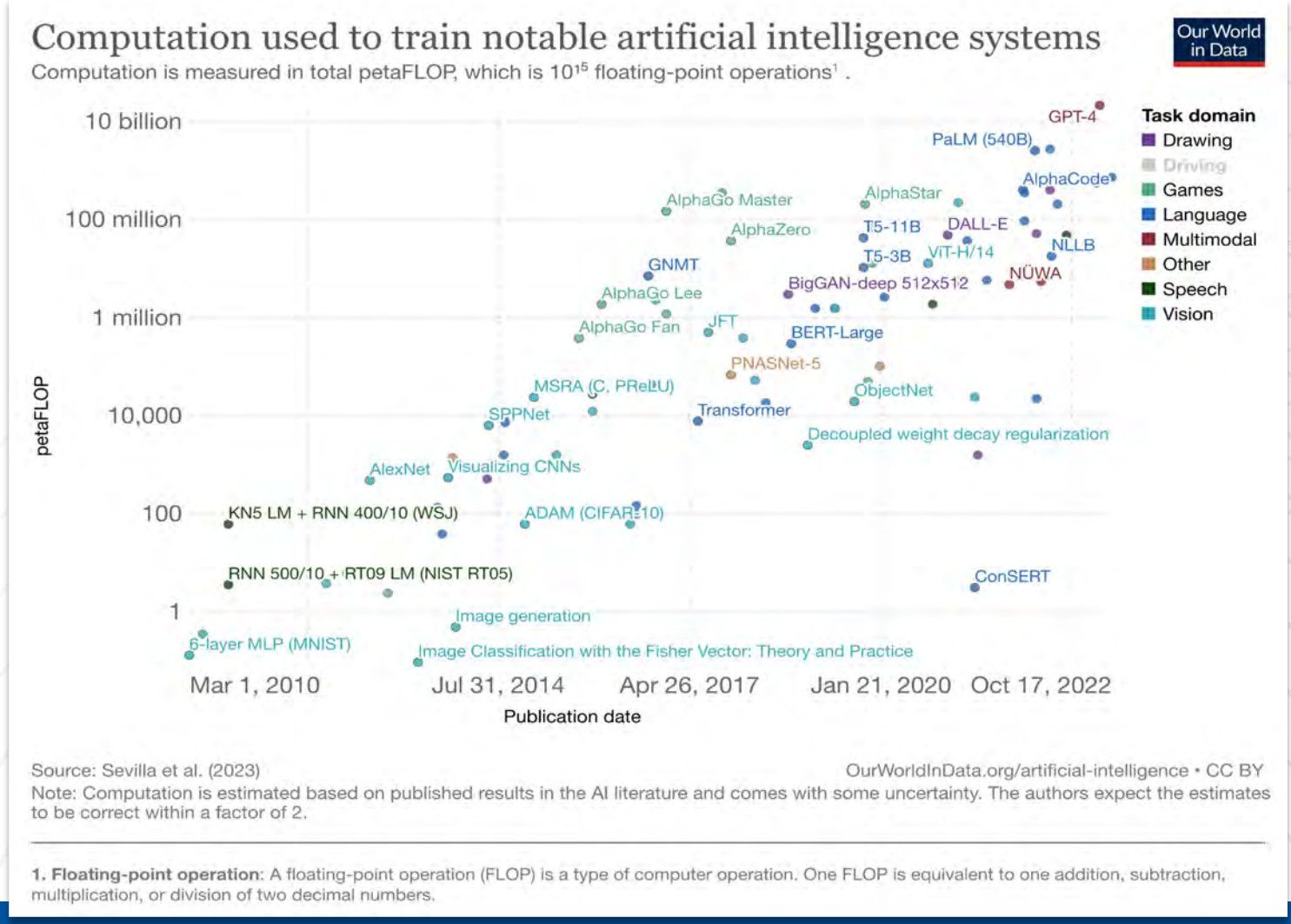
Prompt Injection

Data Poisoning

Sensitive Data Exposed

Thinking about the future…

- Exponential growth in compute
- Exponential growth in model training data
- Emergent capabilities result
- Need to apply new practices for AI Safety, possibly adapted from Bio Lab Safety Levels
- Next versions of Frontier LLMs coming sooner than expected



Critical AI Security Considerations

Pre-Training

How to train the model to minimize risk of jailbreaking, distillation attacks and data poisoning?

How to minimize DLP Inference as well as 3rd Party Retention of sensitive data?

What are the necessary investments in Fine Tuning and Deployment Abuse?

Prompt Engineering

How will the AI react to Role Playing, System Message and various User Instructions?

How to minimize output formats that guide AI response?

What should the temperature and max tokens be?

Untraining and Guardrails

How do you eliminate parts of a dataset?

How do you assure input classifiers are effective?

What are appropriate constraints for AI response?

Importance of Staying Between the Buoys

Many frameworks currently under development

Provides consistency and efficiency with sensitive data

Critical with unforeseen risk in the abyss

Will assist with regulation considerations

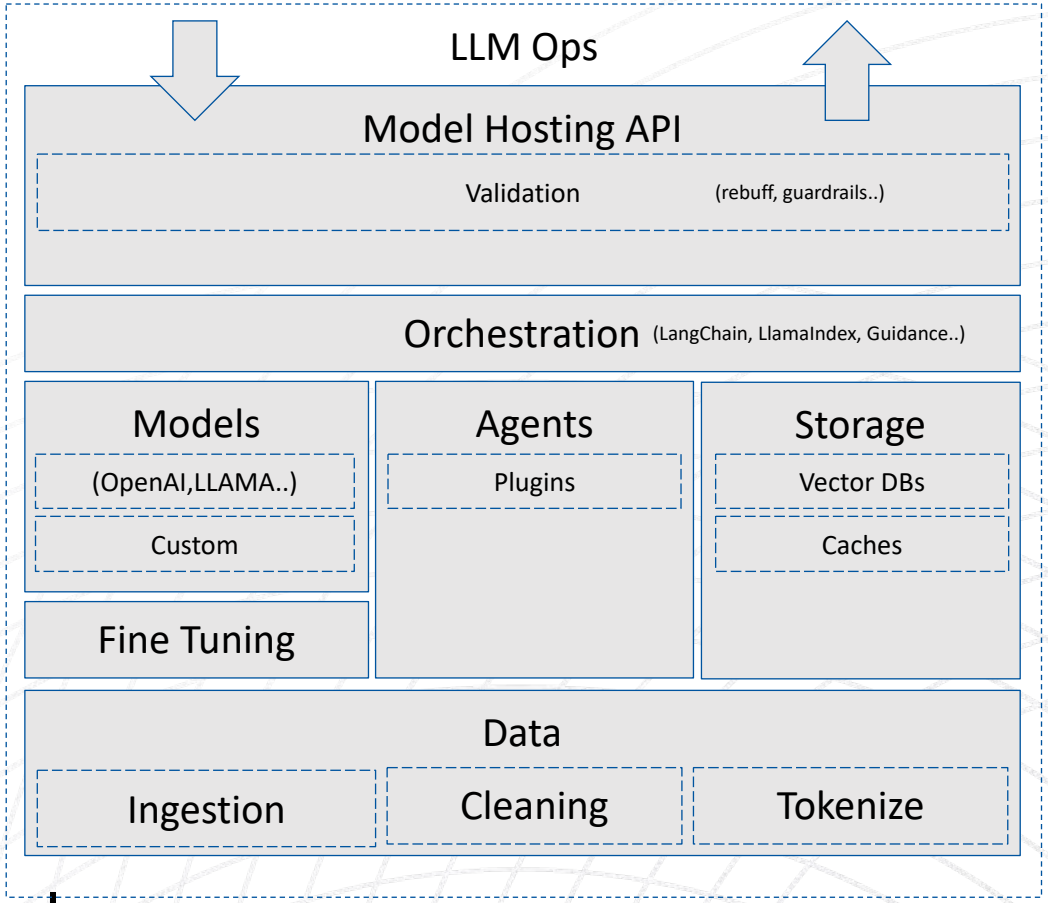
- AI Bill of Rights
- FTC
- CAAB331
- Colorado AI Transparency
- EU AI Act and GDPR

Overview of the CSA AI Safety Initiative

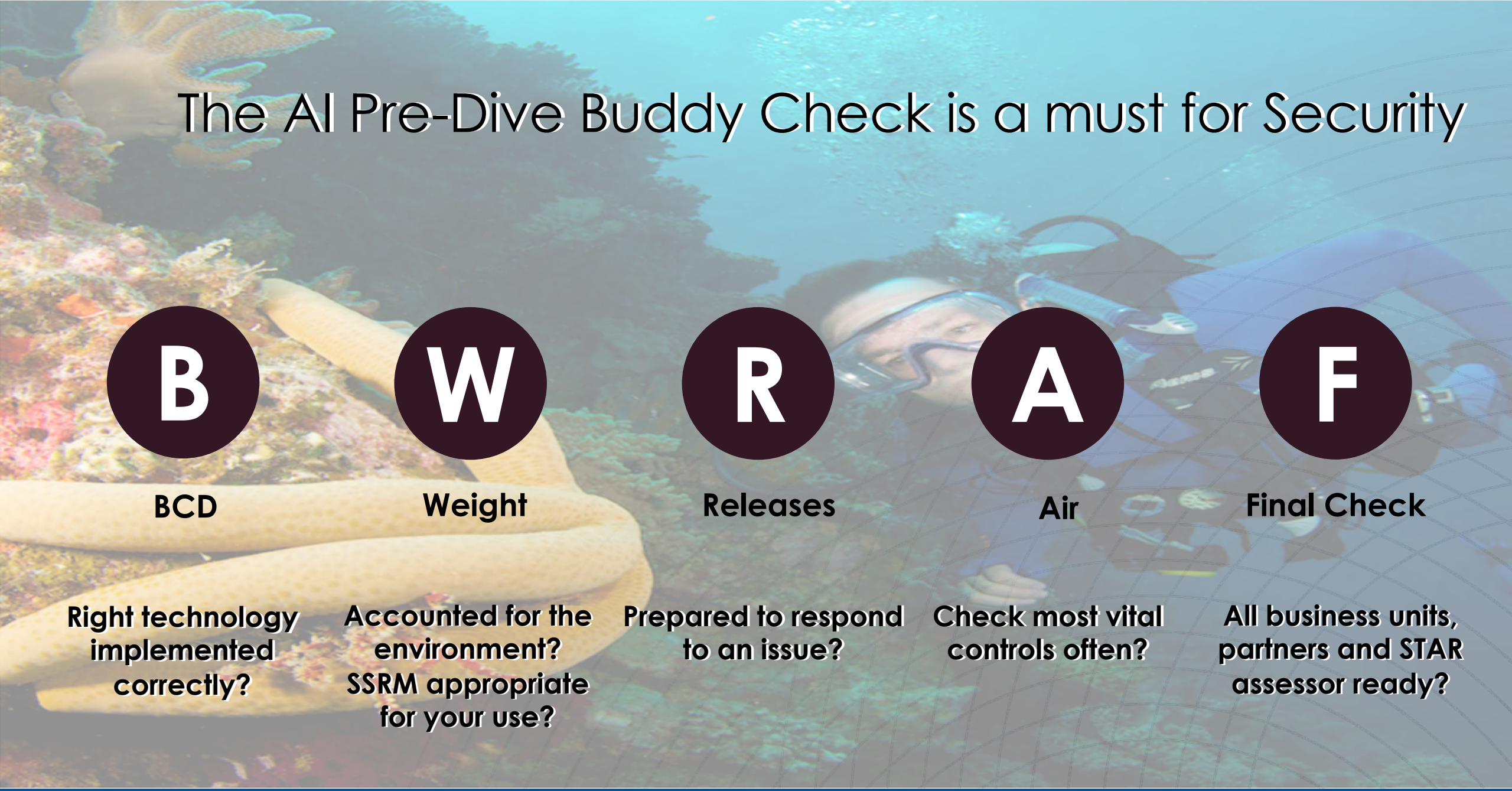
- Mission
  - Create **trusted security best practices** for AI and make them freely available, with an initial focus on Generative AI
  - Give customers of all sizes guidelines, templates and knowledge to deploy AI safely, responsibly and compliant
  - **Complement necessary government regulatory efforts** with aligned and agile industry guidelines and knowledge centers
  - Prepare for the future of **much more powerful AI**
- How
  - Develop a portfolio of research, education, certification and related tools for AI best practices
  - Disseminate best practices widely
  - Do both of the above using the Cloud Security Alliance (CSA) global footprint and over 14 years of earned credibility as a thought leading non-profit association

High priority Initiative Deliverables

- Consensus GenAI Definitions
- LLM Architectures
- AI Controls Framework & Auditing Guidelines
- Enterprise Readiness Frameworks & Playbooks
- Technology Innovations & Use Cases
- Threats & Risk Management Tools
- Policy Resource Center
- Benchmarks
- Prompt Engineering for Cybersecurity Professionals
- Educational Curriculum



The AI Pre-Dive Buddy Check is a must for Security



B	W	R	A	F
BCD	Weight	Releases	Air	Final Check
Right technology implemented correctly?	Accounted for the environment? SSRM appropriate for your use?	Prepared to respond to an issue?	Check most vital controls often?	All business units, partners and STAR assessor ready?

1. Let STAR be a guide

2. Need for education, collaboration and using smart tools properly

3. Understanding every stakeholder has a role in driving change and ensuring a secure future

Troy Leach, Cloud Security Alliance

tleach@cloudsecurityalliance.org

https://www.linkedin.com/in/troyleach/