# SA Summit at RSAC 2024

May 6, 2024 | Welcome!



## Al Safety Initiative

Practical, Responsible & Safe

PRESENTED BY



Illena Armstrong

President, Cloud Security Alliance





Y E A R ANNIVERSARY



Charting the future of a more secure, resilient, trusted cloud ecosystem

205k+

140+

**INDIVIDUAL MEMBERS** 

CHAPTERS

500+

30+

**CORPORATE MEMBERS** 

**ACTIVE WORKING GROUPS** 

2,700+

12,000+

STAR REGISTRY ENTRIES (provider certification)

CONTRIBUTING RESEARCH VOLUNTEERS



CSA research is FREE!



Strategic partnerships with governments, research institutions, professional associations and industry 2009

**CSA FOUNDED** 



**HEADQUARTERS** 

SEATTLE/BELLINGHAM// GLOBAL HEADQUARTERS



## **Al Safety Initiative**

"Al will be the most transformative technology of our lifetimes, bringing with it both tremendous promise and significant peril," said Jen Easterly, Director of the Cybersecurity and Infrastructure Security Agency (CISA). "Through collaborative partnerships like this, we can collectively reduce the risk of these technologies being misused by taking the steps necessary to educate and instill best practices when managing the full lifecycle of Al capabilities, ensuring – most importantly – that they are designed, developed, and deployed to be safe and secure."

"Anthropic's AI systems are designed to be helpful, honest and harmless. We look forward to lending our expertise to crafting guidelines for safe and responsible AI systems for the wider industry. By collaborating on initiatives like this one focused on generative models today – with an eye toward more advanced AI down the line – we can ensure this transformative technology benefits all of society," said Jason Clinton, Chief Security Officer, Anthropic.

"The CSA shares our belief that long-term generative AI advancements will be achieved when private organizations, government, and academia align around industry standards, outlined in our <u>Secure AI Framework (SAIF)</u>. Continued industry collaboration will help organizations ensure emerging AI technologies will have a major impact on the security ecosystem," said Phil Venables, CISO at Google.

"Security is the foundation of trustworthy, safe, and responsible AI, and is core to OpenAI's mission. We recognize the opportunity for new security frameworks and are glad to approach this in partnership. This coalition, and the guidelines emerging from it, will set standard that help ensure AI systems are built to be secure," said Matt Knight, Head of Security at Open AI.



## **Al Safety Initiative**



1,500 volunteer experts in research working groups

## What's up next?

#### **RSA** Announcements

Important Al-related research to be announced this week

### After our Summit at RSA

More research releases coming

June through August

#### **Peer Review & Final Release**

New Controls Framework for Al will be out for peer review & final publication in Q4

#### **SECtember.Al**

In-person September 10 - 12 in

Bellevue, WA at the

Meydenbauer Center

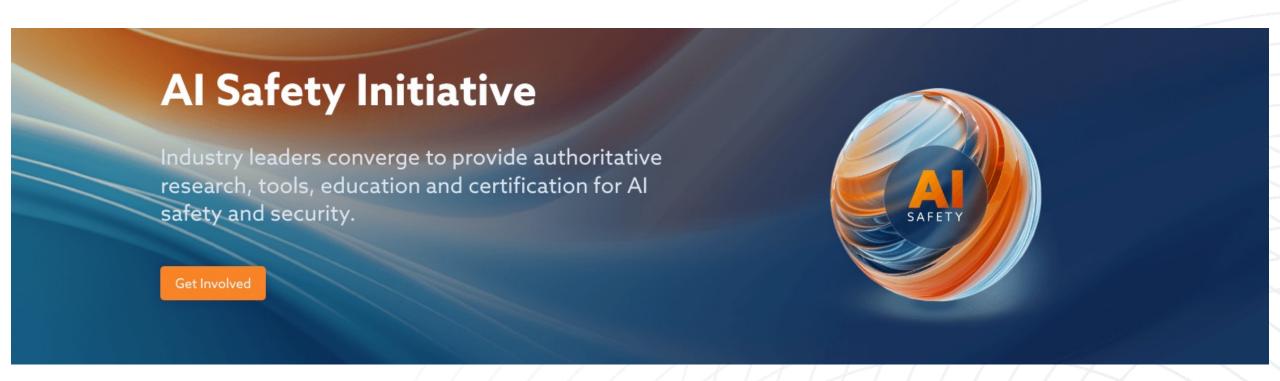
## For the Executive Leaders, Practioners & other Players

Professional AI Education & Certification in 2025

## For an Array of Service Providers

Organizational Al Attestation & Certification

## **Engage with Us!**



Go to CloudSecurityAlliance.Al to learn more.

## Thank You!



Illena Armstrong, Cloud Security Alliance President

iarmstrong@cloudsecurityalliance.org

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

