CoSAI TSC Meeting

Second Meeting
October 8, 2024

Agenda

- Workstreams Members and Co-Chairs
- Next Steps for Workstreams
- Collaboration Tools:
  - Slack, Github and Google Drive
- AOB

W1: Software Supply Chain Security for AI systems

Description

- Expand provenance controls in the AI domain and lower the barriers to AI provenance adoption and risk management.
- Extend SSDF and SLSA principles to the security of AI development.

Targeted Persona	Classes of Use Cases	Possible Outcomes
• AI application developers • Data scientists • Model creators	• Model selection and usage • Technical controls for model governance • Model usage/prompt security • Secure deployment and containment practices • Standardization of model weight serialization/deserialization	• AI-specific SSDF and SLSA frameworks • Security controls for deployment, containment, use of AI • Guide standards for secure model weight serialization/deserialization. • Industry standards for secure model weight handling • **Not in scope:** Aspects of Provenance such as copyright information, licensing information and terms and conditions

Call for Action: Workstream Membership

Organization	First Name	Last Name	Title	Email Address	TSC member (yes/no)	Workstream	Do you want to be a WS co-chair	Notes/Comments
NVIDIA	Daniel	Rohrer	VP of Software Product Security	drohrer@nvidia.com	Yes		No	
NVIDIA	Rich	Harang	Principle Security Architect	rharang@nvidia.com	Yes		No	
OpenAI	Karthik	Rangarajan	Product & Platform Security	karthik@openai.com	Yes			
PayPal	Jen	Silk	Senior Director, Information Security	Jsilk@paypal.com	Yes			
Zscaler	TBD	TBD	TBD	TBD	Yes			
Zscaler	TBD	TBD	TBD	TBD	Yes			

W1 Membership and Co-Chair Volunteers

18
companies

30
members

Co-chair Volunteers:

- Matt Maloney, Cohere
- Peng Ning, Google
- Jay White*, Microsoft
- Andre Alizondo, Wiz

W1 Membership (1/4)

Organization	First Name	Last Name	Title	Email Address	TSCmember (yes/no)	Workstream	Do you want to be a WS co-chair	Notes / Comments
Anthropic	Matt	McNiece	Member of Technical Staff	matt@anthropic.com	No	W1: Software Supply Chain Security for AI systems	No	
Chainguard	Dustin	Kirkland	VP Engineering	kirkland@chainguard.dev	Yes	W1: Software Supply Chain Security for AI systems		
Chainguard	Dan	Fernandez	Staff Product Manager	Dan.fernandez@chainguard.dev	Yes	W1: Software Supply Chain Security for AI systems		
Cisco	Omar	Santos	Distinguished Engineer	osantos@cisco.com	Yes	W1: Software Supply Chain Security for AI systems, W2: Preparing Defenders for a Changing Cybersecurity Landscape	No	
Cisco	Bill	Hudson	Principal Engineer	bhudson@cisco.com	No	W1: Software Supply Chain Security for AI systems	No	
Cohere	Matt	Maloney	Staff Security Engineer	mattmaloney@cohere.com	Yes	W1: Software Supply Chain Security for AI systems	Yes	
Dell Technologies	Marina	Zeldin	Security / Zero Trust common architectures lead	Marina.zeldin@dell.com	No	W1: Software Supply Chain Security for AI systems, W2: Preparing Defenders for a Changing Cybersecurity Landscape, W3: AI Risk Governance	No	
Dell Technologies	Judy	Furlong	Sr. Distinguished Engineer	judith.furlong@dell.com	No	W1: Software Supply Chain Security for AI systems	No	
GenLab	Joerg	Eschweiller	Technical Staff	jes@genlab.studio	No	W1: Software Supply Chain Security for AI systems	No	

W1 Membership (2/4)

Organization	First Name	Last Name	Title	Email Address	TSCmember (yes/no)	Workstream	Do you want to be a WS co-chair	Notes / Comments
Google	Peng	Ning	Senior Engineering Director	pning@google.com	Yes	W1: Software Supply Chain Security for AI systems W2: Preparing Defenders for a Changing Cybersecurity Landscape	Yes	
Google	David	LaBianca	Senior Engineering Director	ddlb@google.com	Yes	W1: Software Supply Chain Security for AI systems W3: AI Risk Governance		
Google	Mihai	Maruseac	Software Engineer	mihaimaruseac@google.com	No	W1: Software Supply Chain Security for AI systems	No	
Google	Shamik	Chaudhuri	Product Manager	schaudhuri@google.com	No	W1: Software Supply Chain Security for AI systems	No	
Hidden Layer	Eoin	Wichens	Technical Research Director	eoin@hiddenlayer.com	Yes	W1: Software Supply Chain Security for AI systems		
IBM	Ian	Molloy	Department Head, Security Research	molloyim@us.ibm.com	No	W1: Software Supply Chain Security for AI systems		
IBM	Michael	Hind	Distinguished Research Staff Member	hindm@us.ibm.com	No	W1: Software Supply Chain Security for AI systems		
Intel	Asmae	Mhassni	Chief Security Technology Strategist	asmae.mhassni@intel.com	Yes	W1: Software Supply Chain Security for AI systems		
Intel	Harish	Thanneer	Principal Engineer	harish.thanneer@intel.com	Yes	W1: Software Supply Chain Security for AI systems	No	

W1 Membership (3/4)

Organization	First Name	Last Name	Title	Email Address	TSCmember (yes/no)	Workstream	Do you want to be a WS co-chair	Notes/Comments
Microsoft	Michael	Scovetta	Principal Security PM Manager	michael.scovetta@microsoft.com	Yes	W1: Software Supply Chain Security for AI systems, W2: Preparing Defenders for a Changing Cybersecurity Landscape	No	
Microsoft	Jay	White	Security Principal Program Manager	jaywhite@microsoft.com	Yes	W1: Software Supply Chain Security for AI systems, W3: AI Risk Governance	Yes	
Protect AI	Sean	Morgan	Chief Architect	sean@protectai.com	Yes	W1: Software Supply Chain Security for AI systems		
Protect AI	Mehrin	Kiani	Lead AI Threat Researcher	mehrin@protectai.com	Yes	W1: Software Supply Chain Security for AI systems W2: Preparing Defenders for a Changing Cybersecurity Landscape W3: AI Risk Governance		
Trend Micro	Josiah	Hagen	Sr Staff Engineer	Josiah_Hagen@trendmicro.com	Yes	W1: Software Supply Chain Security for AI systems W2: Preparing Defenders for a Changing Cybersecurity Landscape, W3: AI Risk Governance	Yes	I'd help chair Preparing Defenders.
Wiz	Andre	Elizondo	Principal Solutions Engineer	andre.elizondo@wiz.io	Yes	W1: Software Supply Chain Security for AI systems	Yes	
Wiz	Jeff	Thorne	Field Engineering	jeff.thorne@wiz.io	Yes	W1: Software Supply Chain Security for AI systems		
Thomson Reuters	Yassine	Ilmi	Director, Product Security	yassine.ilmi@thomsonreuters.com	No	W1: Software Supply Chain Security for AI systems		

W1 Membership (4/4)

Organization	First Name	Last Name	Title	Email Address	TSCmember (yes/no)	Workstream	Do you want to be a WS co-chair	Notes/Comments
Invariant Labs	Mislav	Balunovic	CTO	mislav@invariantlabs.ai	No	W1: Software Supply Chain Security for AI systems		
Protect AI	Faisal	Khan	Lead AI Threat Researcher	faisal@protectai.com	No	W1: Software Supply Chain Security for AI systems W2: Preparing Defenders for a Changing Cybersecurity Landscape W3: AI Risk Governance		
Fr0ntierX	Vladimir	Haltakov	VP Engineering	vladimir@fr0ntierx.com	Yes	W1: Software Supply Chain Security for AI systems W2: Preparing Defenders for a Changing Cybersecurity Landscape	No	
Protect AI	Sam	Washko	Sr Software Engineer	sam@protectai.com	No	W1: Software Supply Chain Security for AI systems W2: Preparing Defenders for a Changing Cybersecurity Landscape		

W2: Preparing Defenders for a Changing Cybersecurity Landscape

Description
• Address the security impacts of use of AI by business applications including attackers, defenders, mitigation techniques and best practices

Targeted Persona	Classes of Use Cases	Possible Outcomes

• CISO
• Security practitioners
• AI app developers
	• Threat and vulnerability management
	• AI Attack surface management
	• Human-AI collaboration interfaces
		• Helpful prompt libraries and templates to promote effective use of AI in security
		• Helpful prompt libraries and templates to prevent abuse of AI
		• Best practices for:
		  ○ Preventing data leaks in fine-tuned models
		  ○ Sharing model threat/vulnerability information
		• **Not in scope:** Security of Agentic Frameworks

W2 Membership and Co-Chair Volunteers

16
companies

27
members

Co-chair volunteers:

- Vinay Bansal, Cisco
- Josiah Hagen, Trend Micro

W2 Membership (1/5)

Organization	First Name	Last Name	Title	Email Address	TSCmember (yes/no)	Workstream	Do you want to be a WS co-chair	Notes/Comments
Amazon	Matt	Saner	Sr. Manager, Security Specialist SAs, AWS	msaner@amazon.com	Yes	W2: Preparing Defenders for a Changing Cybersecurity Landscape, W3: AI Risk Governance		
Amazon	Jason	Garman	Principal Security Solutions Architect, AWS	Garmaja@amazon.com	Yes	W2: Preparing Defenders for a Changing Cybersecurity Landscape, W3: AI Risk Governance		
Anthropic	Akila	Srinivasan	Staff Manager, Security Engineering	akila@anthropic.com	Yes	W2: Preparing Defenders for a Changing Cybersecurity Landscape	No	
Cisco	Omar	Santos	Distinguished Engineer	osantos@cisco.com	Yes	W1: Software Supply Chain Security for AI systems, W2: Preparing Defenders for a Changing Cybersecurity Landscape	No	
Cisco	Vinay	Bansal	Principal Engineer	vibansal@cisco.com	Yes	W2: Preparing Defenders for a Changing Cybersecurity Landscape	Yes	

W2 Membership (2/5)

Organization	First Name	Last Name	Title	Email Address	TSCmember (yes/no)	Workstream	Do you want to be a WS co-chair	Notes / Comments
Dell Technologies	Marina	Zeldin	Security / Zero Trust common architectures lead	Marina.zeldin@dell.com	No	W1: Software Supply Chain Security for AI systems, W2: Preparing Defenders for a Changing Cybersecurity Landscape, W3: AI Risk Governance	No	
Dell Technologies	Michael	Rash	Sr. Distinguished Engineer	Michael.Rash1@Dell.com	No	W2: Preparing Defenders for a Changing Cybersecurity Landscape	No	
Google	Peng	Ning	Senior Engineering Director	pning@google.com	Yes	W1: Software Supply Chain Security for AI systems, W2: Preparing Defenders for a Changing Cybersecurity Landscape	Yes	
Google	Anton	Chuvakin	Senior Staff Security Consultant	chuvakin@google.com	No	W2: Preparing Defenders for a Changing Cybersecurity Landscape, W3: AI Risk Governance	No	
Hidden Layer	Jason	Martin	Principal AI Security Researcher	jmartin@hiddenlayer.com	Yes	W2: Preparing Defenders for a Changing Cybersecurity Landscape	No	

W2 Membership (3/5)

Organization	First Name	Last Name	Title	Email Address	TSCmember (yes/no)	Workstream	Do you want to be a WS co-chair	Notes / Comments
IBM	Chris	Thompson	Global Head of X-Force Red	cthompson@ibm.com	No	W2: Preparing Defenders for a Changing Cybersecurity Landscape		
IBM	Sridhar	Muppidi	IBM Fellow and CTO Security Softwae	muppidi@us.ibm.com	Yes	W2: Preparing Defenders for a Changing Cybersecurity Landscape		
IBM	Jiyong	Jang	Principal Research Scientist & Manager, AI Supply Chain Security	jjang@us.ibm.com	No	W2: Preparing Defenders for a Changing Cybersecurity Landscape		
IBM	Jeff	Turnham	Sr. Tech Staff Member, AI Security	jturnham@ibm.com	No	W2: Preparing Defenders for a Changing Cybersecurity Landscape		
IBM	Krishna	Yelleped dy	Security CTO, Technology Expert Labs, WW Security Solutions Engineering	kyellepe@us.ibm.com	No	W2: Preparing Defenders for a Changing Cybersecurity Landscape		
Intel	Hsien-Hsin "Sean"	Lee	Intel Fellow	sean.lee@intel.com	Yes	W2: Preparing Defenders for a Changing Cybersecurity Landscape		
Microsoft	Michael	Scovetta	Principal Security PM Manager	michael.scovetta@microsoft.com	Yes	W1: Software Supply Chain Security for AI systems, W2: Preparing Defenders for a Changing Cybersecurity Landscape	No	

W2 Membership (4/5)

Organization	First Name	Last Name	Title	Email Address	TSCmember (yes/no)	Workstream	Do you want to be a WS co-chair	Notes / Comments
OpenAI	Ian	Brelinsky	Engineering Manager	brelinsky@openai.com	Yes	W2: Preparing Defenders for a Changing Cybersecurity Landscape		
PayPal	Joshua	Chou	Staff Engineer, Information Security Engineer	joschou@paypal.com	Yes	W2: Preparing Defenders for a Changing Cybersecurity Landscape		
Protect AI	Mehrin	Kiani	Lead AI Threat Researcher	mehrin@protectai.com	Yes	W1: Software Supply Chain Security for AI systems, W2: Preparing Defenders for a Changing Cybersecurity Landscape, W3: AI Risk Governance		
Trend Micro	Josiah	Hagen	Sr Staff Engineer	Josiah_Hagen@trendmicro.com	Yes	W1: Software Supply Chain Security for AI systems, W2: Preparing Defenders for a Changing Cybersecurity Landscape, W3: AI Risk Governance	Yes	I'd help chair Preparing Defenders.
Trend Micro	David	Girard	Sr Director Product Management	david_girard@trendmicro.com	Yes	W3: AI Risk Governance, W2: Preparing Defenders for a Changing Cybersecurity Landscape		

W2 Membership (5/5)

Organization	First Name	Last Name	Title	Email Address	TSCmember (yes/no)	Workstream	Do you want to be a WS co-chair	Notes / Comments
Thomson Reuters	Ryan	Cosgrove	Distinguished Engineer	ryan.cosgrove@thomsonreuters.com	No	W2: Preparing Defenders for a Changing Cybersecurity Landscape		
Styrk AI	Vilayannur	Sitaraman	CTO	sitaraman@styrk.ai	No	W2: Preparing Defenders for a Changing Cybersecurity Landscape	No	
Protect AI	Faisal	Khan	Lead AI Threat Researcher	faisal@protectai.com	No	W1: Software Supply Chain Security for AI systems, W2: Preparing Defenders for a Changing Cybersecurity Landscape, W3: AI Risk Governance		
Fr0ntierX	Vladimir	Haltakov	VP Engineering	vladimir@fr0ntierx.com	Yes	W1: Software Supply Chain Security for AI systems, W2: Preparing Defenders for a Changing Cybersecurity Landscape	No	
Protect AI	Sam	Washko	Sr Software Engineer	sam@protectai.com	No	W1: Software Supply Chain Security for AI systems, W2: Preparing Defenders for a Changing Cybersecurity Landscape		

W3: AI Risk Governance

Description
• Develop a risk and controls taxonomy, checklist, and scorecard to guide practitioners in readiness assessments, management, monitoring, and reporting of their AI products, services, and components

Targeted Persona	Classes of Use Cases	Possible Outcomes
• Chief Risk Officers • Compliance Officers • CISOs, CIOs, and CEOs • Policy and regulation framers	• Governance when **introducing** AI to your company • Governance when **using** AI • Demonstrating compliance to users and external authorities	• Transparent, consistent model cards to help enterprises assess AI adoption risks • Define technical controls to help enterprises achieve regulatory compliance • Discover and govern shadow AI usage and secure AI artifacts throughout the lifecycle. • Manage security risks of AI artifacts, including training data and tuning processes • **Not in scope:** Security of Agentic Frameworks

W3 Membership and Co-Chairs Volunteers

13
companies

20
members

Co-chair volunteers:

- Jay White*, Microsoft
- Lauren Clark, Thomsen Reuters
- Manhar Arora, EY

W3 Membership (1/4)

Organization	First Name	Last Name	Title	Email Address	TSCmember (yes/no)	Workstream	Do you want to be a WS co-chair	Notes / Comments
Amazon	Matt	Saner	Sr. Manager, Security Specialist SAs, AWS	msaner@amazon.com	Yes	W2: Preparing Defenders for a Changing Cybersecurity Landscape, W3: AI Risk Governance		
Amazon	Jason	Garman	Principal Security Solutions Architect, AWS	Garmaja@amazon.com	Yes	W2: Preparing Defenders for a Changing Cybersecurity Landscape, W3: AI Risk Governance		
Anthropic	Shawn	Owen	Director of Physical Security	shawn@anthropic.com	Yes	W3: AI Risk Governance	No	
Cohere	Joshua	Aguiar	GRC Specialist	joshua@cohere.com	Yes	W3: AI Risk Governance	No	
Dell Technologies	Marina	Zeldin	Security / Zero Trust common architectures lead	Marina.zeldin@dell.com	No	W1: Software Supply Chain Security for AI systems, W2: Preparing Defenders for a Changing Cybersecurity Landscape W3: AI Risk Governance	No	
Dell Technologies	Stephen Wright	tbd	Director, GRC lead	stephen_wright2@dell.com	No	W3: AI Risk Governance	No	
Dell Technologies	Igor	Pedan	Technical Staff, Software Engineering	Igor.Pedan@Dell.com	No	W3: AI Risk Governance	No	Will confrim his participation

W3 Membership (2/4)

Organization	First Name	Last Name	Title	Email Address	TSCmember (yes/no)	Workstream	Do you want to be a WS co-chair	Notes / Comments
GenLab	Sarah	Novotny	CTO, Partner	sarah@genlab.studio	Yes	W3: AI Risk Governance	No	
Google	David	LaBianca	Senior Engineering Director	ddlb@google.com	Yes	W1: Software Supply Chain Security for AI systems W3: AI Risk Governance		
Google	Eric	Tierling	Technical Program Manager	ericti@google.com	No	W3: AI Risk Governance	No	
Google	Anton	Chuvakin	Senior Staff Security Consultant	chuvakin@google.com	No	W2: Preparing Defenders for a Changing Cybersecurity Landscape W3: AI Risk Governance	No	
IBM	David	Kleimann	Cloud Risk & Controls Leader	David.Kliemann@ibm.com	No	W3: AI Risk Governance		
Microsoft	Jay	White	Security Principal Program Manager	jaywhite@microsoft.com	Yes	W1: Software Supply Chain Security for AI systems W3: AI Risk Governance	Yes	

W3 Membership (3/4)

Organization	First Name	Last Name	Title	Email Address	TSCmember (yes/no)	Workstream	Do you want to be a WS co-chair	Notes / Comments
Protect AI	Mehrin	Kiani	Lead AI Threat Researcher	mehrin@protectai.com	Yes	W1: Software Supply Chain Security for AI systems W2: Preparing Defenders for a Changing Cybersecurity Landscape W3: AI Risk Governance		
Trend Micro	Josiah	Hagen	Sr Staff Engineer	Josiah_Hagen@trendmicro.com	Yes	W1: Software Supply Chain Security for AI systems W2: Preparing Defenders for a Changing Cybersecurity Landscape W3: AI Risk Governance	Yes	I'd help chair Preparing Defenders.
Trend Micro	David	Girard	Sr Director Product Management	david_girard@trendmicro.com	Yes	W3: AI Risk Governance W2: Preparing Defenders for a Changing Cybersecurity Landscape		
Thomson Reuters	Lauren	Clark	Vice President, Security Strategy & Enablement	lauren.clark@thomsonreuters.com	No	W3: AI Risk Governance	Yes	

W3 Membership (4/4)

Organization	First Name	Last Name	Title	Email Address	TSC member (yes/no)	Workstream	Do you want to be a WS co-chair	Notes / Comments
Protect AI	Faisal	Khan	Lead AI Threat Researcher	faisal@protectai.com	No	W1: Software Supply Chain Security for AI systems W2: Preparing Defenders for a Changing Cybersecurity Landscape W3: AI Risk Governance		
Cranium	Joshua	Harguess	AI Security Chief	jharguess@cranium.ai	Yes	W3: AI Risk Governance		
EY	Manhar	Arora	Senior Manager, Responsible AI	manhar.arora@ey.com	Yes	W3: AI Risk Governance	Yes	

Original Launch Timelines

Date	Action
Friday, Sep 27, 2024	Launch Day of the CoSAI Technical Steering Committee (TSC)
Tuesday, Oct 1, 2024	Each TSC member to volunteer for a workstream: CoSAI Workstream sign up sheet Each organization has volunteered non-TSC members to participate in a workstream
Wednesday, Oct 2, 2024	(If necessary) TSC co-chair(s) will send a form to TSC members to vote for the WS leads (2 leads per workstream)
Friday, Oct 4, 2024	Second CoSAI TSC Meeting: Workstream leads will be announced
Week of Oct 7, 2024	TSC co-chair(s) and OASIS rep(s) to meet with workstream leads to plan workstream launch
By Oct 16, 2024	Workstream leads have set the first meeting with their workstream to kick off the effort
Friday, Oct 18, 2024	Schedule periodic comebacks by WS leads to report on their scope and deliverables

Revised Timelines

Date	Action
Friday, Sep 27, 2024	Launch Day of the CoSAI Technical Steering Committee (TSC)
Monday, Oct 7, 2024	Each TSC member to volunteer for a workstream: CoSAI Workstream sign up sheet Each organization has volunteered non-TSC members to participate in a workstream
Tuesday, Oct 8, 2024	TSC co-chair(s) to request nomination paragraph from co-chair volunteers by eob Thursday, Oct 10, 2024
Friday, Oct 11, 2024	TSC co-chair(s) will send a form to TSC members to vote for the WS leads (2 leads per workstream)
Tuesday, Oct 15, 2024	Third CoSAI TSC Meeting: Workstream leads will be announced
Week of Oct 15, 2024	TSC co-chair(s) and OASIS rep(s) to meet with workstream leads to plan workstream launch
By Oct 21, 2024	Workstream leads have set the first meeting with their workstream to kick off the effort
Friday, Oct 25, 2024	Schedule periodic comebacks by WS leads to report on their scope and deliverables

Collaboration Tools

- Slack:
  - https://join.slack.com/t/cosai-op/shared_invite/zt-2ryr8ekxz-cv1UJWnZuQewJ1ryJVU1wQ
  - Workspace: cosai-op.slack.com
  - We use free Slack = 90-day message history only
  - Don't use Slack to store important info or to keep history on any decisions
  - Channels are not moderated - be professional & mindful
  - Use :
    - GitHub for official docs and any decisions
    - Google Docs for drafts
- Github:
  - https://github.com/cosai-oasis/cosai-tsc
- Google Drive:
  - https://drive.google.com/drive/u/0/folders/1bKp-Byf6wiqjihoXrLw1_DEUq_35arxj

Any Other Business?

Main List

Organization	First Name	Last Name	Title	Email Address	TSCmember (yes/no)	Workstream	Do you want to be a WS co-chair	Notes / Comments
Amazon	Matt	Saner	Sr. Manager, Security Specialist SAs, AWS	msaner@amazon.com	Yes	W2: Preparing Defenders for a Changing Cybersecurity Landscape, W3: AI Risk Governance		
Amazon	Jason	Garman	Principal Security Solutions Architect, AWS	Garmaja@amazon.com	Yes	W2: Preparing Defenders for a Changing Cybersecurity Landscape, W3: AI Risk Governance		
Anthropic	Akila	Srinivasan	Staff Manager, Security Engineering	akila@anthropic.com	Yes	W2: Preparing Defenders for a Changing Cybersecurity Landscape	No	
Anthropic	Shawn	Owen	Director of Physical Security	shawn@anthropic.com	Yes	W3: AI Risk Governance	No	
Anthropic	Matt	McNiece	Member of Technical Staff	matt@anthropic.com	No	W1: Software Supply Chain Security for AI systems	No	
Chainguard	Dustin	Kirkland	VP Engineering	kirkland@chainguard.dev	Yes	W1: Software Supply Chain Security for AI systems		
Chainguard	Dan	Fernandez	Staff Product Manager	Dan.fernandez@chainguard.dev	Yes	W1: Software Supply Chain Security for AI systems		
Cisco	Omar	Santos	Distinguished Engineer	osantos@cisco.com	Yes	W1: Software Supply Chain Security for AI systems, W2: Preparing Defenders for a Changing Cybersecurity	No	