

SANS

AI Cybersecurity Summit 2025

AGENDA

March 31–April 1

Denver, CO

#AISummit



AI Cybersecurity Summit 2025

View the complete agenda [here](#).

Monday, March 31

#AISummit

7:30–9:00 AM MT
12:30–2:00 PM UTC

Summit Registration (Location: Four Square Pre- Function Area [3rd Floor])

Pick up your badge and join us for a light breakfast before SANS AI Summit 2025 kicks off!

7:30–9:00 AM MT
12:30–2:00 PM UTC

Sponsorship Expo (Location: Marco Polo [3rd Floor])

9:00–9:10 AM MT
3:00–3:10 PM UTC

In-Person & Streaming Virtually – Location: Four Square Ballroom (3rd Floor)

Opening Remarks

[Kate Marshall](#), Director, Summits, SANS Institute

[Rob Lee](#), Chief of Research and Fellow, SANS Institute

9:10–9:40 AM MT
3:10–3:40 PM UTC

Keynote | *What to Expect When You're Expecting Your GenAI Baby*

[Sounil Yu](#), Co-founder and Chief AI Safety Officer, Knostic

9:45–10:10 AM MT
3:45–4:10 PM UTC

Fireside Chat

[Sounil Yu](#), Co-founder and Chief AI Safety Officer, Knostic

[Rob Lee](#), Chief of Research and Fellow, SANS Institute

10:15–10:35 AM MT
4:15–4:35 PM UTC

AI Security Controls Guidelines Release

[Rob Lee](#), Chief of Research and Fellow,
SANS Institute

Workshops (In-Person Only – Location: Peek-a-Boo Ballroom [2nd Floor])

10:15 AM–2:00 PM MT
4:15–8:00 PM UTC

Workshop | *LLM Mayhem: Hands-on Red Teaming LLM Powered Chatbots*

[Jim Simpson](#), Certified Instructor Candidate,
SANS Institute

10:35–11:00 AM MT
4:35–5:00 PM UTC

Break & Sponsorship Expo (Location: Marco Polo [3rd Floor])

11:00–11:35 AM MT
5:00–5:35 PM UTC

Using LLMs, Embeddings, and Similarity to Assist DFIR Analysis

[Matthew Seyer](#), Director, KPMG, LLP

[Devanshi Agnihotri](#), Associate, KPMG, LLP

11:40 AM–12:15 PM MT
5:40–6:15 PM UTC

Securing the Grid: AI's Promise for Cyber Resilience in Power Systems

Richard Macwan

Summit CPEs & Certificate of Completion

You will receive 12 CPEs for attending SANS AI Summit 2025 live, 6 for each day you attend. Currently, we are not able to issue CPEs to those that view the Summit recordings. A Certificate of Completion will be available in your account on Tuesday, April 8 (after the conclusion of the Summit & course training) and can be found under the *My Orders* section of your SANS Dashboard Account. SANS will automatically submit your Summit CPEs to GIAC within 14 business days after the event's end date, no action is required on your part.



Slack

AI Cybersecurity Summit 2025

View the complete agenda [here](#).

Monday, March 31 (continued)

#AISummit

12:15–1:15 PM MT 6:15–7:15 PM UTC	Lunch & Sponsorship Expo (Location: Marco Polo [3rd Floor])	
1:15–1:50 PM MT 7:15–7:50 PM UTC	In-Person & Streaming Virtually – Location: Four Square Ballroom (3rd Floor) Unlocking Cyber Insights with AI: Using ML and LLMs for Next-Gen Analysis Xenia Mountrouidou , Principal Cyber Data Scientist, Expel	
1:55–2:30 PM MT 7:55–8:30 PM UTC	Data to Defense: Generative AI and RAG Powering Real-Time Threat Response James Spiteri , Director of PM, Generative AI and ML – Security Analytics, Elastic	
2:35–3:10 PM MT 8:35–9:10 PM UTC	Influence Operations with AI and Cyber-Enabled Ops Gerardo Santos , Head of Threat Hunting, S2 Grupo	Workshops (In-Person Only – Location: Peek-a-Boo Ballroom [2nd Floor]) 2:35–4:35 PM MT 8:35–10:35 PM UTC Workshop Harnessing and Securing Large Language Models: A Hands-On Workshop for Cyber Defenders Sounil Yu , Co-founder and Chief AI Safety Officer, Knostic
3:10–3:30 PM MT 9:10–9:30 PM UTC	Break & Sponsorship Expo (Location: Marco Polo [3rd Floor])	
3:30–3:50 PM MT 9:30–9:50 PM UTC	Building an AI Pen-Testing Assistant Stephen Kalnoske , Innovation and GenAI, SANS Institute	
3:55–4:15 PM MT 9:55–10:15 PM UTC	The AI Security Gap: Addressing the Unique Vulnerabilities of GenAI-Based Applications Davide Annovazzi , EMEA Security Practice Lead, Google Gabriele Zanoni , Mandiant Consulting Country Manager Italy and Principal Strategic Consultant, Google	
4:20–4:40 PM MT 10:20–10:40 PM UTC	The Human Element in AI: Why People Still Matter in a Machine-Led Era Landi Spearman , CEO, Organized SHIFT	
4:40–5:00 PM MT 10:40–11:00 PM UTC	Day 1 Wrap-Up Kate Marshall , Director, Summits, SANS Institute Rob Lee , Chief of Research and Fellow, SANS Institute	
5:00–7:30 PM MT 11:00 PM–1:30 AM UTC	SANS 360 Reception (Location: Marco Polo [3rd Floor]) The 360 talks will run from 6:00–7:00 PM (Location: Four Square Ballroom [3rd Floor]) 10 speakers x 360 seconds/each = 60 minutes of amazing AI content. Don't miss this opportunity to connect, learn, and engage with AI and cybersecurity professionals in a high-energy setting.	

AI Cybersecurity Summit 2025

Monday, March 31

#AISummit

SOLUTIONS TRACK

View the complete agenda [here](#).

10:00–10:10 AM ET
4:00–4:10 PM UTC

Event Kickoff & Introduction

[Mick Douglas](#), SANS Principal Instructor

10:10–10:45 AM MT
4:10–4:45 PM UTC

Beyond the Hype: Making Autonomous Security Operations a Reality

[Stephen Morrow](#), Chief Solution Officer, AirMDR



10:45–11:20 AM MT
4:45–5:20 PM UTC

Unlock the Key to Cybersecurity Excellence: AI-Powered Security Operations Solutions from Fortinet

[Dan Migliore](#), Regional Manager, Enhanced Technology, Security Operations Solutions, Fortinet



11:20–11:55 AM MT
4:20–4:55 PM UTC

Beyond Security: The CISO's Role in Responsible AI

[Kristy Hornland](#), Cybersecurity Director, KPMG US



11:55 AM–12:10 PM MT
4:55–5:10 PM UTC

Break

12:10–12:45 PM MT
5:10–5:45 PM UTC

Scaling GRC with Trust, AI, and Automation

[Crystal Jackson](#), GRC Subject Matter Expert, Vanta

[Sammi Reinstein](#), Senior Product Marketing Manager, Vanta



12:45–1:20 PM MT
5:45–6:20 PM UTC

Static Analysis + LLMs: How to Cut Your Backlog by 20% Overnight

[Erik Buchanan](#), Head of AI Engineering, Semgrep



1:20–1:30 PM MT
6:20–6:30 PM UTC

Event Recap & Closing Remarks

[Mick Douglas](#), SANS Principal Instructor

Summit CPEs & Certificate of Completion

You are eligible to receive up to 8 CPEs for attending SANS AI Cybersecurity Solutions Track 2025 live—4 for each day you attend live.

AI Cybersecurity Summit 2025

View the complete agenda [here](#).

Tuesday, April 1

#AISummit

7:30–9:00 AM MT 12:30–2:00 PM UTC	Sponsorship Expo (Location: Marco Polo [3rd Floor])	
9:00–9:10 AM MT 3:00–3:10 PM UTC	In-Person & Streaming Virtually – Location: Four Square Ballroom (3rd Floor) Opening Remarks Kate Marshall , Director, Summits, SANS Institute Rob Lee , Chief of Research and Fellow, SANS Institute	
9:10–9:40 AM MT 3:10–3:40 PM UTC	Keynote Threat Modeling Agentic AI Systems: Proactive Strategies for Security and Resilience Helen Oakley , Director of Software Supply Chains Security & Secure Development, SAP	
9:45–10:10 AM MT 3:45–4:10 PM UTC	Fireside Chat Kate Marshall , Director, Summits, SANS Institute Helen Oakley , Director of Software Supply Chains Security & Secure Development, SAP	
10:15–10:35 AM MT 4:15–4:35 PM UTC	Watching the Watchers: Safeguards and Security for Artificial Intelligence Systems Eoin Wickens , Director of Threat Intelligence, HiddenLayer	Workshops (In-Person Only – Location: Peek-a-Boo Ballroom [2nd Floor]) 10:15 AM–1:45 PM MT 4:15–7:45 PM UTC Workshop Hooked on AI: Phishing Capture the Flag Foster Nethercott , Founder of Fortisec and author of SANS SEC535: Offensive AI™
10:35–11:00 AM MT 4:35–5:00 PM UTC	Break & Sponsorship Expo (Location: Marco Polo [3rd Floor])	
11:00–11:35 AM MT 5:00–5:35 PM UTC	AI Security Made Easy Rob van der Veer , Chief AI Officer, Software Improvement Group (SIG)	
11:40 AM–12:15 PM MT 5:40–6:15 PM UTC	The Dark Side of AI: Developing Unsecure Applications in Minutes! Chris Lindsey , Application Security Evangelist, OX Security	
12:15–1:15 PM MT 6:15–7:15 PM UTC	Lunch & Sponsorship Expo (Location: Marco Polo [3rd Floor])	

Summit CPEs & Certificate of Completion

You will receive 12 CPEs for attending SANS AI Summit 2025 live, 6 for each day you attend. Currently, we are not able to issue CPEs to those that view the Summit recordings. A Certificate of Completion will be available in your account on Tuesday, April 8 (after the conclusion of the Summit & course training) and can be found under the *My Orders* section of your SANS Dashboard Account. SANS will automatically submit your Summit CPEs to GIAC within 14 business days after the event's end date, no action is required on your part.



Slack

AI Cybersecurity Summit 2025

View the complete agenda [here](#).

Tuesday, April 1 (continued)

#AISummit

1:15–1:50 PM MT 7:15–7:50 PM UTC	In-Person & Streaming Virtually – Location: Four Square Ballroom (3rd Floor) Hacker's Perspective: Realistic AI Attack Scenarios Dan McNerney , Lead AI Security Researcher, Protect AI	
1:55–2:30 PM MT 7:55–8:30 PM UTC	AI in the Crosshairs: Exploring Novel Attacks on AWS AI as a Service Yash Verma , Senior Threat Researcher, Trend Micro	
2:35–3:10 PM MT 8:35–9:10 PM UTC	The Five Must-Haves of an AI Governance Framework Varun Prasad , Managing Director, BDO USA	Workshops (In-Person Only – Location: Peek-a-Boo Ballroom [2nd Floor]) 2:00–3:45 PM MT 8:00–9:45 PM UTC Workshop Artificial Infection: Using AI to Write Malware Foster Nethercott , Founder of Fortisec and author of SANS SEC535: Offensive AI™
3:10–3:30 PM MT 9:10–9:30 PM UTC	Break & Sponsorship Expo (Location: Marco Polo [3rd Floor])	
3:30–3:50 PM MT 9:30–9:50 PM UTC	Defending AI Models: Strategies for Securing AI Implementations Against Emerging Threats Aruneesh Salhotra , CEO/CISO, SNM Consulting Inc.	
3:50–4:15 PM MT 9:50–10:15 PM UTC	Closing Remarks Kate Marshall , Director, Summits, SANS Institute Rob Lee , Chief of Research and Fellow, SANS Institute	

Summit CPEs & Certificate of Completion

You will receive 12 CPEs for attending SANS AI Summit 2025 live, 6 for each day you attend. Currently, we are not able to issue CPEs to those that view the Summit recordings. A Certificate of Completion will be available in your account on Tuesday, April 8 (after the conclusion of the Summit & course training) and can be found under the *My Orders* section of your SANS Dashboard Account. SANS will automatically submit your Summit CPEs to GIAC within 14 business days after the event's end date, no action is required on your part.



Slack






AI Cybersecurity Summit 2025

Tuesday, April 1

#AISummit

SOLUTIONS TRACK

View the complete agenda [here](#).

10:00–10:10 AM MT 4:00–4:10 PM UTC	Event Kickoff & Introduction Mick Douglas , SANS Principal Instructor	
10:10–10:45 AM MT 4:10–4:45 PM UTC	Data to Defense: Generative AI and RAG Powering Real-Time Threat Response James Spiteri , Director of PM, Generative AI and ML – Security Analytics, Elastic	
10:45–11:20 AM MT 4:45–5:20 PM UTC	AI is the Supply Chain: Lessons from NullifAI Dan Petrillo , VP Product Marketing, ReversingLabs Saša Zdjelar , Chief Trust Officer, ReversingLabs	
11:20–11:55 AM MT 4:20–4:55 PM UTC	Guardrails for AI: How to Safeguard Enterprise Data in a Multi-Agent World Yasir Ali , CEO & Founder, Polymer	
11:55 AM–12:10 PM MT 4:55–5:10 PM UTC	Break	
12:10–12:45 PM MT 5:10–5:45 PM UTC	Navigating the AI Hype in Cybersecurity Andrew Mundell , Principal Sales Engineer, Sophos	
12:45–1:20 PM MT 5:45–6:20 PM UTC	Secure AI by Design Spencer Thellmann , Principal Product Manager, Palo Alto Networks	
1:20–1:30 PM MT 6:20–6:30 PM UTC	Event Recap & Closing Remarks Mick Douglas , SANS Principal Instructor	

THANK YOU TO OUR SUMMIT SPONSORS



Summit CPEs & Certificate of Completion

You are eligible to receive up to 8 CPEs for attending SANS AI Cybersecurity Solutions Track 2025 live—4 for each day you attend live.

Upcoming SANS Summits

2025

Cybersecurity Leadership

Virtual (CT)

SUMMIT: April 24

ICS

Orlando, FL & Virtual

SUMMIT: June 15–17

TRAINING: June 18–23

CloudSecNext

Denver, CO & Virtual

SUMMIT: October 2–3

TRAINING: October 4–9

Emerging Threats

Virtual (ET)

SUMMIT: May 14

DFIR

Salt Lake City, UT & Virtual

SUMMIT: July 24–25

TRAINING: July 26–31

Hack & Defend

Austin, TX & Virtual

SUMMIT: October 28–29

TRAINING: October 30–November 4

Ransomware

Virtual (ET)

SUMMIT: May 30

Security Awareness

Chicago, IL & Virtual

TRAINING: August 11–13

SUMMIT: August 14–15

Neurodiversity in Cybersecurity

Virtual (ET)

SUMMIT: November 20

All North American Virtual Summits in 2025 are free.
For more info on upcoming Summit events, visit: sans.org/summits

SANS