

RSAC | 2025
Conference
San Francisco • April 28 – May 1 • Moscone Center

RSAC 2025 Call For Submissions Trends Report

EXPLORE THE TRENDS

Many Voices.
One Community.

AUTHORED BY
Kacy Zurkus
Senior Content Manager
RSA Conference

RSAC[™] | 2025 Conference

San Francisco • April 28 – May 1 • Moscone Center



It's official! Artificial Intelligence (AI) and all things related to AI have taken center stage in conversations across silos, sectors, and industries, and it happened fast. As recently as 2023, AI-related submissions only accounted for about 5% of the talks people wanted to deliver at RSAC Conference. When the **RSAC 2025 Conference** Call for Submissions opened, AI was everywhere. Of the more than 2,800 proposals, over 40% referenced AI and its companion topics of machine learning and agents.

The Program Committees for all 26 tracks anticipated they'd see a lot of submissions on AI. Specifically, the Intersection of AI & Security track chairs expected they'd be reviewing proposals related to AI governance, the need for agents around ML models, and the EU's AI Act. So, it's no surprise that the strongest trending topics from this year's submissions all involved elements of AI from securing to collaborating with them.

Let's take a look.

Click below to see what the future holds for our industry.

AGENTS OF AI

**LARGE LANGUAGE MODELS
(LLMS)**

NON-HUMAN IDENTITIES (NHI)

AI ASSISTANTS

ETHICS

API RISKS

QUANTUM

GUARDIANS OF ALL THINGS

COMMUNITY

**MANY VOICES.
ONE COMMUNITY.**



Who are the agents of AI?

With regard to agentic AI, many submitters considered the ways in which humans and agents will coexist. Some questioned the impact of agents acting on their own and the consequences of unpredictable things happening. Overwhelmingly, security practitioners in every sector shared ideas on everything from safeguarding identities in an AI-driven world to exposing how hackers target AI models and balancing regulation with innovation. Many recognized the criticality of guardrails. Where once the SBOM was trendy, the AIBOM (AI Bills of Materials) emerged this year with an intended promise to improve transparency and security in AI development.

<< RETURN TO INTRODUCTION

CONCLUSION >>

AGENTS OF AI	LARGE LANGUAGE MODELS (LLMS)	NON-HUMAN IDENTITIES (NHI)	AI ASSISTANTS	ETHICS
API RISKS	QUANTUM	GUARDIANS OF ALL THINGS	COMMUNITY	MANY VOICES. ONE COMMUNITY.



LLMs are all the (RAG)e, but are they creating new risk?

While some proposals touted large language models (LLMs) as a solution to patching or enabling scalable AI infrastructure, others warned of the dark side of their use in AI attacks, the ability to generate malicious code, and potential data pitfalls. This year's submissions reflected that there are big hopes and justifiable prudence around implementing LLM-powered tools with the more cautious practitioners noting that these tools can introduce vulnerabilities into security products. Malicious actors have the potential to weaponize or poison models, which also raises questions of accuracy. Logically, this led to many submissions exploring the role of Retrieval Augmented Generation (RAG)-based applications, securing RAG workflows to mitigate risks in data retrieval, and ensuring the correct information is being used to build systems.

[<< RETURN TO INTRODUCTION](#)

[CONCLUSION >>](#)

AGENTS OF AI

LARGE LANGUAGE MODELS (LLMs)

NON-HUMAN IDENTITIES (NHI)

AI ASSISTANTS

ETHICS

API RISKS

QUANTUM

GUARDIANS OF ALL THINGS

COMMUNITY

MANY VOICES.
ONE COMMUNITY.



Non-human identities are proliferating

Identity and all things related to authentication and access control were again some of the strongest trends. This year, however, AI has ushered in a new identity challenge for security practitioners who are feverishly trying to manage the proliferation of non-human identities (NHI). Managing the burgeoning number of machine identities that employees are adopting in pursuit of improved efficiency is only growing more complex, especially as organizations scale cloud environments. Submissions looked to both expose the issues of NHI and address the problems. Potential solutions ranged from guidance on how to defend against NHI attacks, how to build an NHI security framework, and how to secure NHIs within RAG architectures.

[<< RETURN TO INTRODUCTION](#)

[CONCLUSION >>](#)

[AGENTS OF AI](#)

[LARGE LANGUAGE MODELS
\(LLMS\)](#)

[NON-HUMAN IDENTITIES \(NHI\)](#)

[AI ASSISTANTS](#)

[ETHICS](#)

[API RISKS](#)

[QUANTUM](#)

[GUARDIANS OF ALL THINGS](#)

[COMMUNITY](#)

[MANY VOICES.
ONE COMMUNITY.](#)

Collaborating with AI assistants

A growing trend is the personification of technology. New tools are blurring the lines between human and machine. So, it's no surprise that proposed talks had AI assistants making confessions, dreaming, hallucinating, over-sharing, and contributing to workplace productivity, leaving some asking, "what is human anymore?". Increasingly, all the biases that have long been attributed to human behavior are being applied to technology. The risk of insider threat comes not only from a disgruntled employee but also from common misconfigurations. Session proposals warned that while developers regularly engage with LLMs, an over-reliance on AI-generated code can lead to quality, security, and maintainability issues as well as reduce learning opportunities. Some feared these tools may also limit creative problem-solving, foster a false sense of expertise among developers, and increase security risks.

<< RETURN TO INTRODUCTION

CONCLUSION >>

AGENTS OF AI	LARGE LANGUAGE MODELS (LLMS)	NON-HUMAN IDENTITIES (NHI)	AI ASSISTANTS	ETHICS
API RISKS	QUANTUM	GUARDIANS OF ALL THINGS	COMMUNITY	MANY VOICES. ONE COMMUNITY.



A question of ethics

The ideas put forth about ethics in this year’s submissions evidence that the RSAC Community is mindful of the implications of a failure to align strategy with ethics, particularly as it relates to AI governance. Many submissions highlighted the growing concern around the rapid implementation of AI and ensuring its use is not only safe and responsible but also ethical. Whether it was exploring communication at all levels, the criticality of making ethical decisions, or arguing for integration of AI ethics into regulations, including GDPR, many cybersecurity professionals want to establish ethical policies and practices to shape the future of cybersecurity from product development to risk management and frameworks.

[<< RETURN TO INTRODUCTION](#)

[CONCLUSION >>](#)

AGENTS OF AI	LARGE LANGUAGE MODELS (LLMS)	NON-HUMAN IDENTITIES (NHI)	AI ASSISTANTS	ETHICS
API RISKS	QUANTUM	GUARDIANS OF ALL THINGS	COMMUNITY	MANY VOICES. ONE COMMUNITY.



Mitigating API risks

Innovation is inevitably changing the threat landscape, which impacts an organization’s overall security strategy. With the explosion of LLMs and Generative AI has come increased concern for API security. Recognizing that APIs power the supply chains of today’s digital organizations, some submissions highlighted the hidden threats in shadow APIs, the dangers of API exposure, and the crucial role of APIs in securely accessing tools. Others offered solutions for protecting APIs, securing network APIs for 5G, and comprehensive API security solutions for GenAI/LLM applications.

<< RETURN TO INTRODUCTION

CONCLUSION >>

AGENTS OF AI	LARGE LANGUAGE MODELS (LLMS)	NON-HUMAN IDENTITIES (NHI)	AI ASSISTANTS	ETHICS
API RISKS	QUANTUM	GUARDIANS OF ALL THINGS	COMMUNITY	MANY VOICES. ONE COMMUNITY.

Questions and concerns around quantum

Even though we’re not yet living in a quantum world, the security industry is looking ahead to a post-quantum world with a mix of panic and strategic thinking. AI is informing the way cryptographers are planning for post-quantum cryptography (PQC). As a result, cybersecurity teams are preparing to take the quantum leap by looking at the current state of quantum computing and building a roadmap. Quantum-related submissions explored everything from basic quantum concepts to the intersection of AI, cybersecurity, and quantum computing with a focus on practical solutions to protect against future quantum threats.

<< RETURN TO INTRODUCTION

CONCLUSION >>

AGENTS OF AI	LARGE LANGUAGE MODELS (LLMS)	NON-HUMAN IDENTITIES (NHI)	AI ASSISTANTS	ETHICS
API RISKS	QUANTUM	GUARDIANS OF ALL THINGS	COMMUNITY	MANY VOICES. ONE COMMUNITY.



Guardians of all things

Many creative titles played with words in fun ways, which always adds extra appeal for reviewers. Given that the role of the security practitioner is to defend against threats, it makes sense that the use of “Guardians”, appeared in many submissions. Several aspiring speakers echoed the sentiment that cybersecurity practitioners are the caretakers and protectors of everything from identity and policy to AI-powered MSSPs. The industry’s quest to secure our world was evident in several proposals. To that end, these guardians advised a ‘back to basics’ approach, warning those with both limited and unlimited resources to be cautious about shiny new things. The goal is to make cybersecurity accessible to all. While there was a strong focus on service to others, there was also the recognition that security teams themselves needed safeguarding from burnout.

[<< RETURN TO INTRODUCTION](#)

[CONCLUSION >>](#)

[AGENTS OF AI](#)

[LARGE LANGUAGE MODELS
\(LLMS\)](#)

[NON-HUMAN IDENTITIES \(NHI\)](#)

[AI ASSISTANTS](#)

[ETHICS](#)

[API RISKS](#)

[QUANTUM](#)

[GUARDIANS OF ALL THINGS](#)

[COMMUNITY](#)

[MANY VOICES.
ONE COMMUNITY.](#)

Continued commitment to protect and serve others

The RSAC 2025 Conference submissions reflected a thoughtfulness about the whole of the community—not just the cybersecurity industry. While many submissions focused on topics related to building a more inclusive and resilient culture, several also looked more broadly at protecting everyone—from young digital citizens to seniors. We saw sessions that thoughtfully examined how to drive community engagement, the need for cybersecurity awareness as a community service, the need to raise the ‘cybersecurity poverty line,’ and the benefits of collaboration. Understanding the interconnectedness of today’s digital enterprise, security practitioners are thinking differently about the many—large and small, for profit and nonprofits—that comprise the whole to strengthen supply chain security, better mitigate third-party risk, and build a safer and more secure world.

<< RETURN TO INTRODUCTION

CONCLUSION >>

AGENTS OF AI	LARGE LANGUAGE MODELS (LLMS)	NON-HUMAN IDENTITIES (NHI)	AI ASSISTANTS	ETHICS
API RISKS	QUANTUM	GUARDIANS OF ALL THINGS	COMMUNITY	MANY VOICES. ONE COMMUNITY.

Many Voices. One Community.

In analyzing the trends from the RSAC 2025 Conference Call for Submissions, it is evident that there are so many incredible thinkers and innovators who want to share their voices with the RSAC Community. Security professionals are cautiously optimistic about the promise of GenAI and thinking ahead. In looking at our relationship with emerging tools, many also want to ensure that while technology enhances the business and affords greater efficiency, it doesn't replace the need for human collaboration. Overwhelmingly, we saw a continued desire to share stories, which is a human need that transcends time and generation.



<< RETURN TO INTRODUCTION

CONCLUSION >>

AGENTS OF AI

LARGE LANGUAGE MODELS
(LLMS)

NON-HUMAN IDENTITIES (NHI)

AI ASSISTANTS

ETHICS

API RISKS

QUANTUM

GUARDIANS OF ALL THINGS

COMMUNITY

MANY VOICES.
ONE COMMUNITY.

RSACTM | 2025 Conference

San Francisco • April 28 – May 1 • Moscone Center

Many Voices.
One Community.

In conclusion

Thank you to everyone who contributed to the **RSAC 2025 Conference** Call for Submissions. Your innovative ideas, thoughtful insights, and dedication to the cybersecurity community are what make this event so impactful. We appreciate your time and effort in sharing your expertise, and we look forward to seeing you at RSAC 2025 Conference in San Francisco!

[<< RETURN TO INTRODUCTION](#)

[LEARN MORE ABOUT RSAC 2025 CONFERENCE >>](#)

AGENTS OF AI

LARGE LANGUAGE MODELS
(LLMS)

NON-HUMAN IDENTITIES (NHI)

AI ASSISTANTS

ETHICS

API RISKS

QUANTUM

GUARDIANS OF ALL THINGS

COMMUNITY

MANY VOICES.
ONE COMMUNITY.