ISC2 SECURITY CONGRESS 2025
October 28 - 30 | Nashville + Virtual

Call for Presentations

Call for Presentations Guidelines

Presentation proposals (maximum 3 per Speaker) must be submitted online by *February 28, 2025, at 11:59 pm EST* using the Call for Presentations Portal.

ISC2 is accepting presentation ideas to share insights, best practices, emerging trends, groundbreaking research, and critical updates in the cybersecurity industry at Security Congress 2025, taking place at the Gaylord Opryland Resort & Convention Center in Nashville, Tennessee + *Live Online* on October 28-30, 2025.

ABOUT THE EVENT

ISC2 Security Congress is our flagship conference that brings together over 4,000 infosec professionals to learn from best-in-industry content focusing on the latest developments in cybersecurity. Here, attendees can network, exchange ideas, explore key topics of interest, and broaden their horizons – all so that they can collect the skills and knowledge needed to bolster their value as a cyber professional.

EVENT FORMAT

Security Congress 2025 will be offered as a hybrid event. Many sessions will be live streamed and available on demand after the event. **All speakers will be required to present in person in Nashville, TN.**

ABOUT ISC2

ISC2 is the world's leading member organization for cybersecurity professionals, driven by our vision of a safe and secure cyber world. Our roughly 675,000 members, candidates and associates around the globe are a force for good, safeguarding the way we live. Our award-winning certifications – including cybersecurity's premier certification, the CISSP® – enable professionals to demonstrate their knowledge, skills and abilities at every stage of their careers. ISC2 strengthens the influence, diversity and vitality of the cybersecurity profession through advocacy, expertise and workforce empowerment that accelerates cyber safety and security in

an interconnected world. Our charitable foundation, The Center for Cyber Safety and Education, helps create more access to cyber careers and educate those most vulnerable. Learn more and get involved at ISC2.org. Connect with us on X, Facebook and LinkedIn.

TARGET AUDIENCE

Security Congress is open to cybersecurity professionals in all stages of their careers.

CONTENT AREAS

Priority will be given to session submissions that align with one or more of the following content areas. Top submissions relay timely, real-world experiences that are actionable and relevant to our global audience.

1. Cloud Security. Topics include:

- Technologies, policies and practices used to protect data, applications and infrastructure associated with cloud computing and/or distributed environments.
- Means of securing data in transit and at rest.
- The ability to ensure the privacy and compliance of data stored in the cloud.
- The shared responsibility model between cloud service providers and users, plus other cloud governance policies and practices.
- Zero Trust/IAM in a hybrid or multi-cloud IT environment.
- Cloud-native application and container security. (Your session is Cloud Security if it's about securing the cloud-based app development environment; your session is Software Security if it's about securing the apps themselves. Use your best judgment.)

2. Cyber Leadership & Ethics. Topics include:

- The ethics, principles, skills and practices that are necessary to manage and lead an organization's understanding of risk, data security and privacy.
- Identifying, maintaining, informing and executing effective security strategies, policies and practices.

- Protecting your organization's reputation, assets, interests and intellectual property.
- Optimally and responsibly managing your cyber/IT workforce.
- Interacting and communicating with upper-level executives and the board of directors in order to secure support and funding.
- Creating and developing security awareness programs, securing workforce and customer buy-in around key security initiatives, and establishing security champions to help advance your cause.
- Balancing business and operational needs with security priorities. Balancing new innovations and emerging technologies (e.g. AI) with security needs.

Cyber leaders are not always synonymous with a management title.

3. Frameworks, Standards & Guidelines. Topics include:

- Aligning and implementing global best practices and standards in cybersecurity and software development.
- Systems and data lifecycle management processes.
- Adhering to frameworks and standards from bodies such as CIS, ISO/IEC and NIST, as well as industry sector standards (e.g. HIPAA, PCI, etc.)
- Following rules and guidance from organizations/agencies such as CISA, the SEC, NCSC and ENISA.
- Alignment with newer frameworks for emerging tech such as AI.

4. Governance, Risk and Compliance (GRC). Topics include:

- The principles, processes and practices organizations use to ensure that they have and operate good governance principles.
- Compliance with international, federal and state laws and regulations.
- Risk quantification and mitigation, and making risk-based decisions.
- Striking a balance between risk/compliance obligations and business goals.
- Third- and fourth-party risk policies and practices.

5. SecOps & Threat Response. Topics include:

- Optimization and integration of the processes, practices and technologies used by organizations to identify and manage cybersecurity threats.

- Establishing a collaboration between your security team and operations team.
- Network security, including continuous network monitoring of security events. Detection and response.
- Securing IT, OT environments along with their connected (IoT) devices.
- Security Operations Center (SOC) responsibilities,
- Threat intelligence and threat hunting.
- Digital forensics and/or incident response (DFIR) best practices.
- Analysis of current threats (malware/ransomware, social engineering campaigns, APTs, etc.), and how to mitigate and recover from these threats.
- User and entity behavior analytics and eliminating internal threats.

6. Software Security. Topics include:

- Methods for effective application security testing and threat modeling to ensure that your apps operate safely and as intended.
- DevSecOps, shifting left, secure development lifecycles and other secure app development practices/policies.
- Securing APIs.
- Using AI, open-source code and other conveniences and emerging technologies responsibility when developing applications.
- Vulnerabilities, patching and bug bounties/mitigation. (If your session is only from the end-user perspective, this might get recategorized to a Network Security session instead.)
- Software supply chain security.
- Web app security (e.g. defenses against e-skimming, bots, DDoS, malvertising, etc.).

7. Careers.

Sessions in this category can adopt the perspective of a cybersecurity/IT employee, a hiring organization, or both. The focus can include how to improve your employability and build a career path for yourself in cyber, and/or how to hire, develop and upskill cyber workers in your organization.

Topics include:

- Improving employability and career advancement.

- Recruitment, job descriptions and job interviews.
- Educational opportunities, certifications, internships and apprenticeships.
- Hiring philosophies and practices.
- Upskilling and training.
- Cyber workforce trends and data.

SESSION TYPES

This event has the following session types open for submission. Most proposals will fall under the category of Breakouts.

BREAKOUTS (60 minutes)
50-minute panel or speaker presentation followed by 10-minute moderated Q&A. Breakout sessions run concurrently.

BRIGHT IDEAS ROUNDTABLES (60 minutes)
Small-group roundtable discussions or exercises (with a maximum of roughly 50 people) on a specific topic. In this presentation format, speakers will be facilitating the discussion. The presentation slide materials are generally minimal. Maximum of 2 facilitators, please.

PRESENTATION STYLES

Adults learn best in settings where they can participate actively, relate the new information or techniques to their other experiences, and practice new skills. Prospective presenters are encouraged to use session styles that incorporate these components and preference will be given to those proposals that include plans for active participant engagement and practical application of the concepts covered. Content may be delivered by one presenter, co-presenters, or a panel. Please ensure that there are no more than four speakers total (including panel moderators) in your session.

SPEAKER BENEFITS

The following benefits will be enjoyed by all speakers:

- Complimentary All Access pass to Security Congress 2025

- Speaker Challenge Coin
- Promotion in conference marketing materials, on event website, and on social media
- Unique attendance discount(s) to share with speaker's peer network.
- The opportunity to share ideas, knowledge, and experience with cybersecurity professionals.
- Contribution to furthering education in the cybersecurity industry
- CPE Credits

ISC2 does not cover travel or accommodation costs for speakers, unless otherwise agreed upon in writing with ISC2.

ISC2 NON-COMMERCIAL POLICY

Attendees at ISC2's events are seeking quality CPE-eligible education sessions free from commercial influence or bias and are critical of content that seeks to advertise, promote, or market products or companies. ISC2 requires that presenters do not use a conference session for commercial sales pitches or self-promotion. Speakers are not permitted to distribute promotional literature, brochures, or sales materials in any form to attendees during their session unless approved in writing by ISC2. Presentations must be free from inappropriate use of brands, trademarks, or logos. ISC2 reserves the right to maintain control over the content of the sessions and to make modifications as appropriate.

SUBMISSION, REVIEW, SELECTION AND NOTIFICATION PROCESS

CALL FOR PAPERS OPENS: January 13, 2025
CALL FOR PAPERS CLOSES: February 28, 2025
FINAL SELECTION: March 21, 2025 (date subject to change)
SPEAKER ACCEPTANCE DUE: April 7, 2025 (date subject to change).

ISC2 SECURITY CONGRESS 2025
October 28 - 30 | Nashville + Virtual

Call for Presentations

SUBMISSION

- Proposals must be submitted by February 28, 2025, at 11:59 pm EST using the online call for papers portal. No extension of this date will be granted.
- A maximum number of three (3) proposal submissions is allowed per Speaker.
- Proposals must include all information requested during the submission process to include:
    - Full details of Speaker(s) and/or Panelists(s) including name, title, company, phone, email, and brief bio. Please ensure that Speakers are informed and have agreed to speak prior to submitting their name and details.
    - Selected domain(s), attendee knowledge level and preferred presentation type
    - List of actionable participant takeaways
    - Additional supporting information, including what makes your proposed session original and differentiates it from past or current proposals on the same overall topic
    - Demographic information (optional)

We know that everything is insecure. FUD (Fear, Uncertainty, Doubt) will not work with this audience. Politics and "edgy" humor aren't for everyone: please keep the global audience in mind.

REVIEWS & SELECTION

- Proposals will be reviewed by a selection committee comprised of external cybersecurity professionals and ISC2 staff according to the following criteria:
    - Timeliness and appropriateness of subject matter
    - Practical application and participant engagement tools
    - Clearly stated and achievable takeaways
    - Originality (cutting-edge content not previously presented at other events)
    - Qualifications and expertise of presenter(s)

  - Comprehensiveness and value of presentation objectives
  - If appropriate to the lesson, the inclusion of interactive exercises, gamification or demonstrations (not mandatory)
- ISC2 expressly reserves the right at any time to reject a proposal.

NOTIFICATION OF DECISION

- Submitters and/or Speakers are scheduled to be notified of the decision (Accepted, Declined, Waitlisted) before the close of March 2025. ISC2 expressly reserves the right to amend its timetable as needed.
- If a submission proposal is waitlisted, ISC2 will contact the Submitter and/or Speaker if additional speaking opportunities arise.
- The Speaker must formally accept the invitation to speak no later than April 7, 2025 (date subject to change). After this date, it will be assumed that the Speaker or Panelist no longer wishes to speak, and the session will be cancelled and replaced by another session on the waitlist.
- All Speakers and Panelists must agree to and sign a Speaker Policy Agreement prior to their session being formally included and promoted.
- All speakers and panelists must agree to present in-person in Nashville, TN. ISC2 is not responsible for travel costs or accommodations for speakers.

ADDITIONAL INFORMATION

- ISC2 reserves the right to request/make modifications of content prior to acceptance.
- Please note that ISC2 will be requiring Speakers' permission to live stream + record their presentation if accepted to speak.
- Since the exact day and time of each session is not yet available, please ensure that the presenter(s) is/are available for the duration of the event dates *(October 28-30, 2025)*. Presenter(s) and panelists must be able to attend the event in-person.

ISC2 SECURITY CONGRESS 2025
October 28 - 30 | Nashville + Virtual

Call for Presentations

For more information on submitting your proposal or for assistance with the Submission Portal, please contact:

Bradley Barth
bbarth@isc2.org

DIVERSITY, EQUITY, AND INCLUSION STATEMENT

ISC2 is committed to ensuring the cybersecurity profession is as diverse, equitable and inclusive as the world we serve. This includes being accessible to everyone regardless of gender, ethnic or nationality, disability, religion, sexual orientation, gender reassignment, socio-economic background, or age.

We gather and analyze diversity data to assess the extent to which we are achieving our diversity and inclusion goals. We use this information to review our processes to ensure they are fair and transparent, and do not have an adverse impact on any particular group. We will retain this data for 18 months and no longer beyond the date of consent.

All information provided will be treated as strictly confidential in accordance with the ISC2 Privacy Notice in line with the General Data Protection Regulations (GDPR). The information will only be used for statistical purposes only with access restricted to staff involved in processing and monitoring the data. No information will be published or used in any way that allows individuals to be identified.

We recognize that some people may regard this information as private and have therefore included the option of 'prefer not to say' within. You do not have to complete the form, but it will help us improve representation around the world, our services, and processes if you can complete it as much as possible.

To find out more about why we gather this information contact: inclusion@isc2.org

ACCESSIBILITY

We aim to host events that enable individuals of all abilities to participate fully and equally. We welcome persons with disabilities to submit proposals and will provide, upon request, the necessary reasonable accommodations if they are accepted to speak at any of our events. Examples of such accommodations may be, for example, sign language interpreters, CART, assistive listening devices, sighted guide, Braille, wheelchair access or a scent-free environment. Please contact the event program manager if you have any questions about accessibility.