ISC2 SECURITY CONGRESS 2026

October 24 - 28, 2026 | Gaylord Rockies + Virtual

Call for Presentations

Call for Presentations Guidelines

Presentation proposals (maximum three per Speaker) must be submitted online by March 13, 2026, at 11:59 pm EST using the Call for Presentations Portal.

ISC2 is accepting presentation proposals for shared insights, best practices, emerging trends, groundbreaking research, case studies and critical updates in the cybersecurity industry for ISC2 Security Congress 2026, October 24-28 at the Gaylord Rockies Resort & Convention Center in Colorado + Virtual.

Pre-Conference is October 24-25, Main Conference is October 26-28.

ABOUT THE EVENT

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

EVENT FORMAT

Security Congress 2026 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 Aurora, CO.

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 more than 265,000 certified members, and associates, 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 educates those most vulnerable. Learn more, get involved or become an ISC2 Candidate to build your cyber career at ISC2.org. Connect with us on X, Facebook and LinkedIn.

ISC2 SECURITY CONGRESS 2026

October 24 - 28, 2026 | Gaylord Rockies + Virtual

Call for Presentations

TARGET AUDIENCE

Security Congress is open to cybersecurity professionals in all stages of their careers. We are seeking a mix of sessions that cater specifically to early-career, mid-career and senior-level cyber pros or all of these.

CONTENT AREAS

Priority will be given to session submissions that align with one or more of the content areas listed below. 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 defend 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 hybrid or multicloud 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.)
- Has your ISC2 CCSP certification for cloud helped advance your career? Does your organization value CCSP certification when hiring? Consider sharing your story in a session.

2. Cyber Leadership and 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 boards 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 management titles.)

3. Frameworks, Standards and 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 they have and operate sound governance principles.
- Compliance with international, federal and state laws and regulations.
- Risk quantification and mitigation and risk-based decisions.
- Striking a balance between risk/compliance obligations and business goals.
- Third- and fourth-party risk policies and practices.
- Has your ISC2 CGRC certification for GRC helped advance your career? Does your organization value CGRC certification when hiring? Consider sharing your story in a session.

5. SecOps and Threat Response. Topics include:

- Optimization and integration of the processes, practices and technologies used by organizations to identify and manage cyberthreats.
- 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 life cycles and other secure app development practices/policies.
- Securing APIs.
- Using AI, open-source code and other conveniences and emerging technologies responsibly when developing applications.
- Vulnerabilities, patching and bug bounties/mitigation. (If your session is only from the end-user perspective, this might get recategorized as a Network Security session instead.)
- Software supply chain security.
- Web app security (e.g., defenses against e-skimming, bots, DDoS, malvertising, etc.).
- Has your CSSLP software security certification helped advance your career? Does your organization value CSSLP certification when hiring? Consider sharing your story in a session.

7. Careers.

Sessions in this category may adopt the perspectives of cybersecurity/IT employee, hiring organizations 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.
- Has your ISC2 certification (CISSP or otherwise) helped advance your career? Does your organization value ISC2 certification when hiring? Consider sharing your story in a session.

MAIN CONFERENCE SESSION FORMATS

The following session formats are open for submission.

BREAKOUT – SLIDESHOW LECTURE (60 minutes)
50-minute classic slideshow presentation, followed by a 10-minute moderated Q&A. One to four speakers.

BREAKOUT – PANEL/FIRESIDE CHAT (60 minutes)
50-minute panel or fireside chat presentation, followed by a 10-minute moderated Q&A. Panel should include three to four participants including moderator. Fireside chats generally have one moderator and one speaker.

BREAKOUT – WAR STORIES (60 minutes)
50-minute presentation, followed by a 10-minute moderated Q&A. Presentation should be a detailed account or case study of a cyber incident or challenge that was overcome or a key operation undertaken by a user organization/client (e.g., data breach, ransomware attack, a takedown of an APT group, merger/acquisition, change in leadership, etc.) One to four speakers.

BRIGHT IDEAS ROUNDTABLE (60 minutes)
A 60-minute, small-group roundtable discussion (maximum of roughly 50-60 audience members) on a specific topic. In-person audience only - no virtual attendees. Speakers will facilitate the discussion. Presentation slide materials are generally minimal. Two facilitators maximum.

TABLETOPS AND GAMIFIED EXERCISES (60 - 120 minutes)
Short-format, small-group tabletop exercises and other gamified, interactive sessions. For in-person audience only - no virtual attendees. Speaker/facilitator will present using their personal laptop and may leverage hardcopy materials and in-room polling to run exercises. Please, no

exercises that require audience members to use their own laptops/devices. Examples of sessions could include a ransomware incident response walk-through, a choose-your-own-adventure session, a quiz show that tests attendees on spotting phishing emails or deepfakes, an interactive live demo, etc. Ideal length is 60 minutes; however, we will consider assigning a double session for a total of two hours, if needed. Exercises that require more than two hours should be considered a Pre-Conference Workshop. One to three facilitators.

PRE-CONFERENCE WORKSHOPS

For the first time, the Security Congress Call for Presentations process is open to one-day and two-day Pre-Conference Workshops in addition to Main Conference sessions. When you open a new submission entry, you will be asked whether you intend to submit a Pre-Conference workshop session concept or a Main Conference session concept.

Pre-Conference Workshops provide attendees with an in-depth, hands-on learning experience. These workshops should focus on innovative, timely or highly relevant topics and be highly engaging and interactive. Sessions should equip participants with practical skills, frameworks and actionable takeaways they can apply immediately in their work. As indicated by the name, these workshops take place from October 24-25, before the main conference.

PRESENTATION STYLES

Attendees learn best in settings where they can actively participate, relate new information or techniques to their experiences and practice new skills. Presenters are encouraged to incorporate these components. Preference will be given to 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. No more than four speakers total (including panel moderators) per session.

SPEAKER BENEFITS

The following benefits will be enjoyed by all speakers:

- Complimentary All Access pass to Security Congress 2026
- Speaker Challenge Coin
- Promotion in conference marketing materials, on event website and on social media
- Unique attendance discount(s) to share with your 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 events value quality CPE-eligible education sessions free from commercial influence or bias. They are critical of content that seeks to advertise, promote or market products or organizations. Presenters are prohibited from using conference sessions for commercial sales pitches or self-promotion. Speakers may not 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 PRESENTATIONS OPENS: January 30, 2026
CALL FOR PRESENTATIONS CLOSES: March 13, 2026
FINAL SELECTION: Mid-to-Late April 2026 (subject to change)
SPEAKER ACCEPTANCE DUE: Mid-May 2026 (subject to change)

SUBMISSIONS

- Proposals must be submitted by March 13, 2026, at 11:59 pm EST using the online Call for Presentations portal. A brief extension is possible but is not guaranteed.
- Maximum of three proposal submissions per Speaker.
- Proposals must include all information requested during the submission process:
    - Full details of speakers and/or panelists including name, title, company, phone, email and brief bio. Please ensure speakers are informed and have agreed to participate prior to submitting their name and details.
    - Selected domains, 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 topic
- Demographic information (optional)

Please keep the global audience in mind. FUD (fear, uncertainty, doubt) will not work with this audience. Politics, edgy humor and coarse language aren't for everyone.

REVIEWS & SELECTION

- Proposals will be reviewed by a selection committee comprised of external cybersecurity professionals and ISC2 staff according to the following criteria:
  - Timeliness, appropriateness and practicality of subject matter.
  - 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) by mid-to-late April, or early May. 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.
- Speakers must formally accept the invitation to speak no later than May 18, 2026 (date subject to change). After this date, it will be assumed that the speaker no longer wishes to participate, and the session will be cancelled and replaced by another session on the waitlist.

- All speakers and panelists must sign a Speaker Policy Agreement before their session is formally included and promoted as part of the event.
- All speakers and panelists must agree to present in-person in Aurora, Colorado. ISC2 is not responsible for travel costs or accommodations for speakers, unless otherwise agreed upon in writing with ISC2.

ADDITIONAL INFORMATION

- ISC2 reserves the right to request/make modifications of content prior to acceptance.
- Please note that ISC2 requires speaker permission to live stream and record their presentation.
- Since the exact day and time of each session is not yet available, please ensure speakers are available for the duration of the event. Presenters and panelists must be able to attend the event in-person.

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

Bradley Barth
bbarth@isc2.org

INCLUSIVITY STATEMENT

At ISC2, we believe a safer and more secure digital world depends on everyone having the opportunity to belong, contribute and thrive. That's why we are committed to fostering a qualified, resilient cybersecurity profession where everyone's future is secured. 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 demographic data to assess the extent to which we are achieving our 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 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 are not required 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.