CALL FOR CONTENT 2026
TERMS & CONDITIONS

CONTENT

BARCELONA CYBERSECURITY CONGRESS

PRESENTATION

The Barcelona Cybersecurity Congress Call for Content aims to deliver high-impact, technically rigorous, and strategically relevant sessions addressing today's most critical cybersecurity challenges and innovations. The Congress focuses on real-world security implementations, emerging threats, advanced defense strategies, and governance frameworks that enable secure digital transformation across critical industries and digital ecosystems.

We invite cybersecurity leaders, practitioners, researchers, and end-user organizations to submit proposals that provide actionable insights, measurable outcomes, and practical experience in protecting modern infrastructures. Priority will be given to submissions that demonstrate applied cybersecurity in operational environments, supported by real use cases, measurable risk reduction, or demonstrated security maturity improvements.

Key thematic areas include, but are not limited to:

- Threat Intelligence, Threat Hunting, and Cyber Defense Operations
- Zero Trust Architecture and Identity-First Security Models
- Cloud Security, Multi-Cloud Risk Management, and Cloud-Native Protection
- Software and Hardware Supply Chain Security (SBOM, HBOM, firmware security)
- Incident Detection, Response, and Cyber Resilience Strategies
- Data Protection, Encryption, Confidential Computing, and Privacy Engineering
- AI Security, including protection of AI systems and use of AI in defense
- Regulatory compliance, governance, and risk management (NIS2, DORA, GDPR, CRA)
- Operational Technology (OT), Industrial Control Systems (ICS), and Critical Infrastructure Security
- Security for emerging technologies including edge computing, IoT, and connected systems

Submissions are particularly encouraged from organizations operating in critical and strategic sectors such as energy, healthcare, manufacturing, finance, transportation, telecommunications, smart cities, and digital infrastructure.

The objective of the Call for Content is to ensure the Congress delivers practical, implementation-focused, and strategically relevant knowledge to cybersecurity professionals, executives, and decision-makers across Europe and globally.

We welcome submissions from original papers/abstracts relevant to these themes. Barcelona Cybersecurity Congress receives hundreds of proposals for the available speaking slots. To improve the likelihood of selecting your proposal, we recommend focusing your proposal on one or more real-world implementations: **use-case/business-case oriented with a confirmed *end-user speaker.**

DEFINITION OF USE/BUSINESS CASE PRESENTATION

Use case/business case definition: solutions or applications that deliver lessons learned, collaboration strategies, and the latest approaches in **applied solutions to new or existing challenges**, with the metrics of a positive outcome to the customer clearly defined and illustrated.

Outcomes can be defined as improved efficiency, security, reliability, asset management, remote monitoring, increased productivity, decreased downtime, increased profit, enhanced safety, reduced costs, etc.

Use/business cases with a confirmed customer speaker will be rated higher and have a better chance of being selected for the program. Please note that the complete contact information of the customer/end-user must be provided in this proposal.

We also encourage multiple speakers of collaborating companies to present in a co-presentation or panel discussion format.

DEFINITION OF **END-USER** IN A USE/BUSINESS CASE PRESENTATION?

The end-user, as referred to in the term “use case” and “business case,” **is the company or organization receiving the business value** created by the technology.

The **end-user directly benefits** from the solution(s)/outcomes, i.e., improved productivity, remote monitoring, predictive maintenance, improved security, reduced costs, new revenue streams, asset management, improved safety, etc.

The end-user is not a solutions provider, partner, or integrator; instead, **they are the recipient of the solution**. Therefore, if you sell your technology to another solution provider who then wraps it into a more robust solution, they are not the company from which to build your use case presentation. Instead, the use case should be built on the industry customer they then sell the solution to, including your technology.

THE AUDIENCE

Our audience is interested in hearing the outcome metrics of these end-user companies and hearing directly from the end-user customer. End-users tend to favor sessions presented by their peers. These "customers" speak more freely about projects and in general, generate more and higher quality discussions during the Q&A.

CATEGORIES FOR USE CASE SUBMISSIONS

Includes but is not limited to:

Business Introduction to Cybersecurity

A strong foundation in cybersecurity begins with robust frameworks and strategies to help your organization stay ahead of evolving threats. Discover the essential tools, tactics, and skills needed to protect your organization from attack, and ensure swift recovery after an attack. These include cultivating a cybersecurity-conscious workforce, implementing a robust Zero Trust security framework, adopting and adhering to cybersecurity standards, and staying abreast of the ever-changing threat landscape.

Session Topics:

The 2026 Congress is structured around six core pillars of modern cybersecurity. Authors should align their submissions with one of the following validated thematic areas:

Pillar A: strategic governance

Culture: moving beyond "Social Engineering" awareness to building a proactive "Safety Culture" where employees are the first line of defense rather than the weakest link.

Zero Trust: deep dives into micro-segmentation, continuous verification, and the practical pros/cons of a "Never Trust, Always Verify" architecture.

Regulations & Policy: navigating the complex web of industrial cybersecurity legislation and future global compliance trends.

Pillar B: Technological Evolution

Generative AI & ML: exploring the "Adversarial AI" arms race, including deepfake detection and using Machine Learning for high-speed computation and threat hunting.

Edge & neuromorphic computing: securing the expanded attack surface created by low-latency remote devices and hardware-level security for next-gen processors.

Quantum & future-proofing: preparing for the post-quantum era with Quantum Cryptography and advanced encryption standards.

- **Culture**

  The number one cybersecurity vulnerability of any organization is its employees, and contractors. So called “Social Engineering” attacks target unsuspecting or complacent individuals. Learn how to safeguard your network from the most common attack scenarios, and what each of us can do to ensure we don’t become the weakest link in the security chain.

- **Zero Trust**

Sometimes the best defense is a good offense. That is the theory behind "Zero Trust". Assume everyone is a potential cybersecurity threat. Micro segment your network to ensure no single person has too much access. Explore the pros and cons of this popular, but controversial approach to cybersecurity.

- **Regulations and Policy**

  Regulations, Standards, and Policies protect the public interest, but these guardrails can also be a great source of cybersecurity strategies and tactics for private companies. We will look at the industrial cybersecurity legislation, discuss future trends and compliance.

WORKSHOPS - HACKING VILLAGE

The Hacking Village provides a highly technical, hands-on environment designed for practical demonstrations, live security testing, research presentations, and interactive technical sessions. This environment enables cybersecurity professionals to showcase offensive and defensive techniques, vulnerabilities, exploit research, security tools, and applied cybersecurity methodologies in a collaborative setting.

The Hacking Village emphasizes:

- live demonstrations of attack and defense techniques
- technical deep dives into vulnerabilities and exploit mitigation
- cloud, infrastructure, and application security testing methodologies
- reverse engineering and malware analysis
- hardware and embedded systems security
- AI and machine learning security testing
- red team, blue team, and purple team operational techniques

This unified submission model ensures that all cybersecurity contributions—whether strategic, operational, or deeply technical—are evaluated consistently and placed in the most appropriate format to maximize value for participants.

Submissions for the main congress and the Hacking Village are now unified under a single Call for content. All proposals will be evaluated by the Program Committee and assigned to the most appropriate stage based on their format and technical depth.

- The congress program: focused on strategic business cases, use-case presentations with end-user metrics, and panel discussions.
- The Hacking Village: designed as a hands-on, interactive environment. This stage is reserved for technical showcases, live exploits, hardware hacking, and "how-to" demonstrations. If your proposal focuses on practical application, live testing scenarios, or applied cybersecurity exercises, it will be prioritized for this immersive format.

As technology rapidly evolves, so do the methods and tools required to protect our digital assets. Explore the cutting-edge advancements revolutionizing the cybersecurity landscape, from the integration of Generative AI and Machine Learning to Edge and Neuromorphic Computing. Learn about the critical role these advancements play in fortifying our digital infrastructure and bolstering our defenses and explore the possibilities for their practical application in safeguarding our increasingly connected world.

Session Topics:

Artificial intelligence and cybersecurity

Artificial intelligence is transforming both cyber defense and cyber threats. This track explores how AI is used to enhance detection, automate response, and strengthen resilience, as well as the emerging risks associated with AI systems, including adversarial attacks, model poisoning, prompt injection, and AI supply chain risks.

Machine learning for threat detection and security operations

Machine learning enables real-time analysis of massive data streams to identify anomalies, detect threats, and automate security operations. Sessions will explore practical implementations in SOC environments, fraud detection, behavioral analytics, and predictive security models.

Edge security and distributed infrastructure protection

As computing shifts to the edge, organizations face new attack surfaces and operational challenges. This track focuses on securing distributed systems, IoT ecosystems, industrial environments, and edge computing architectures while maintaining performance and operational continuity.

- Generative AI

  Generative AI has become synonymous with the concept of deep fakes. At the end of the day, Generative AI is just another tool. It can create new cybersecurity vulnerabilities, but it can also be used to spot fraud and block attacks.

- Machine Learning

  Your organization is constantly under cyber attack. Most of these efforts are harmless, but occasionally a serious threat comes through. To identify and block such sophisticated attacks requires a massive number of computations made in a miniscule amount of time. This is where machine learning can be very useful.

- Edge Computing

Edge computing enables remote devices to perform complex tasks with low latency. But, each edge device increases the cybersecurity attack surface. How do you protect these devices and the network they are connected to?

TECHNOLOGIES INVOLVED

For each proposal, you must select the top 3 technologies/use cases/themes that your session will be most focused on:

Cybersecurity:

- Network security
- Endpoint security
- Data encryption
- Threat intelligence
- Identity and access management
- Security analytics

Supply Chain Security:

- Software Bill of Materials
- Quantum computing
- Incident response
- Risk management
- Hardware Bill of Materials

Business Strategy:

- Culture
- Workforce development
- Zero Trust security
- Policy
- Regulations
- Standards

5G technology:

- Ultra-low latency communication
- Massive IoT connectivity
- Enhanced mobile broadband
- Mission-critical applications
- Network slicing
- Data sharing
- Edge computing integration

Artificial Intelligence (AI):

- Machine learning
- Deep learning
- Natural language processing
- Computer vision
- Expert systems
- Neural networks
- Cognitive computing
- Data Integration
- Data Sharing
- Risk vs. Regulation of advanced AI applications
- Neuromorphic Computing

Augmented reality (AR):

- Marker-based AR
- Marker-less AR
- Projection-based AR
- AR headsets and glasses
- AR in gaming and entertainment
- AR in healthcare and education
- AR in professional development training

Big data analytics:

- Data mining

- Predictive analytics
- Prescriptive analytics
- Real-time analytics
- Text analytics
- Social media analytics

Blockchain:

- Cryptocurrencies
- Smart contracts
- Decentralized Applications (DApps)
- Supply chain management
- Identity verification
- Asset tokenization

Cloud computing:

- Infrastructure as a Service (IaaS)
- Platform as a Service (PaaS)
- Software as a Service (SaaS)
- Serverless computing
- Hybrid cloud
- Cloud-native technologies

Cognitive computing:

- Natural language processing
- Speech recognition
- Machine learning
- Knowledge representation and reasoning
- Cognitive agents
- Decision automation
- Deep Fake Detection

Edge computing:

- Edge analytics
- Edge AI
- Edge devices and gateways
- Edge security
- Edge-based data processing
- Edge-based IoT applications
- Neuromorphic Computing

Internet of Medical Things (IoMT):

- Connected medical devices
- Remote patient monitoring
- Health wearables
- Telemedicine platforms
- Electronic Health Records (EHR)
- Healthcare data analytics
- Applying blockchain to protect healthcare data integrity

Internet of Things (IoT):

- Smart sensors
- Wearable devices
- Industrial IoT
- Connected homes
- Smart cities
- IoT platforms
- Alarm Management Systems
- Edge computing

Mobile technology:

- 5G networks
- Connectivity/Service Areas
- Mobile apps
- Mobile payments

- Location-based services
- Augmented reality apps
- Mobile health technologies

Virtual Reality (VR):

- Immersive VR
- Non-immersive VR
- VR headsets and devices
- VR in gaming and entertainment
- VR in training and simulation
- VR in therapy and rehabilitation

Robotics:

- Industrial robots
- Service robots
- Collaborative robots (cobots)
- Autonomous robots
- Surgical robots

Quantum computing:

- Quantum bits (qubits)
- Quantum algorithms
- Quantum cryptography
- Quantum simulation
- Quantum supremacy
- Quantum annealing

PRESENTATIONS FORMAT

Submissions must adhere to the following guidelines to be evaluated for inclusion on the agenda.

- The Program Committee requires all submissions to be use-case/business-case focused, highlighting measurable business outcome metrics.

- Use cases/business cases with a confirmed customer (end-user) presenter will be scored higher in the evaluation process and therefore have a higher chance of being selected for inclusion in the program. We welcome submissions by solutions providers if they include an end-user presenter.

- Session proposals that discuss technology but don't illustrate real use-case/business-case stories with measurable business outcome metrics will not be evaluated.

- Submissions must be complete as the Program Committee is considering the proposal based on the participants and the topic collectively—if any part of that is missing, they cannot make an informed review.

- BCC is committed to diversity and inclusion. You are strongly urged to consider the diversity of speakers, including gender, ethnicity, orientation, nationality, and religion, as well as the diversity of experience brought to bear by job position, responsibilities, and industry represented.

- All abstracts must be submitted and presented in English; please note that the Congress's primary language is English, and translation services are not available.

The program committee will not evaluate abstracts that do not comply with the above requirements.

The time allotted for each presentation will be:

- **Use case Presentations:** 25 minutes including 20 minutes for the presentation + 5 minutes for Q&A.

- **Panel discussion:** 60 minutes including 45 minutes for the presentation +15 minutes for Q&A (includes three or more presenters with differing opinions and perspectives for debate). This will be a moderated discussion with time set aside for questions from the audience.

BARCELONA CYBERSECURITY CONGRESS

TIMELINE

The submission process has five major steps:

Abstract Submission: Until March 31st, 2026 23H59 CET.

Program Director Review:
The Program Director will first review all papers to ensure that the submission meets the general criteria.

Revision:
Authors may be asked to revise their proposals to meet the requirements as needed.

Committee Review:
The Program Committee will review the submitted papers; authors may again be asked to provide additional information.

Notification:
To ensure a realistic review process and high-quality program preparation, the following 2026 cutoff dates apply:

- abstract submission deadline: March 31, 2026, at 23:59 CET.
- review & revision period: April 1 – May 15, 2026.
- author notification: May 22, 2026. (notifications will be sent via email to all primary authors regarding their selection status).
- final program publication: June 15, 2026.

Format	Duration	Structure
use case presentation	25 Minutes	20 min presentation + 5 min Q&A; must include end-user.

Format	Duration	Structure
panel discussion	60 Minutes	45 min debate + 15 min Q&A; requires 3+ diverse perspectives.
Hacking Village demo	30-45 Minutes	Interactive, hands-on demonstration of technical application.

BEFORE SUBMISSION

Please read the T&C carefully and ensure that your abstract/paper does meet the criteria and main requirements.

Please note that the short abstract is requested for marketing purposes and must be no more than 600 characters spaces included. The submission form will only accept submissions within the character limits for each section.

SUBMISSION

Papers can be submitted online at link:
https://statics.teams.cdn.office.net/evergreen-assets/safelinks/2/atp-safelinks.html
Until March 31st, 2026 23H59 CET.

For any questions regarding submissions, speaker guidelines, or program content, please contact:

Barcelona Cybersecurity Congress Speaker Office
Email: iots.technicaloffice@firabarcelona.com

All submissions must be completed via the official submission platform:

https://app.oxfordabstracts.com/stages/76449/submitter

The submission deadline is:

March 31, 2026 at 23:59 CET

Late submissions will not be accepted.

All submitted papers/abstracts will be published in an open database with access granted to the Program Director and Program Committee. The author(s) agree with its publication in this open-access database by submitting a paper.

ACCEPTED PAPERS/ABSTRACTS

The conference registration fee for presenting speaker(s) will be waived. Once your paper has been accepted, you will receive instructions to register for a complimentary **speaker pass** with **full VIP access to the Congress**, including all sessions and event areas.

Once your session **has been accepted,** you will receive official communication from the Technical Office with all the relevant information, you will also find your session date, session guidelines and recommendations, and all necessary instructions for the onsite event.

Bearing in mind the various security measures and firewalls, please ensure that emails can reach you by adapting your spam filter accordingly.

INTELLECTUAL PROPERTY

The Speaker authorizes FIRA DE BARCELONA to record and photograph the speech he/she performs, being such recording able to be reproduced for any means, including streaming or video on demand services and social networks, as part of the materials of the general conference. Also, the image and/or the recordings may be used for the promotion of future editions of the Call for Papers activity. The Speaker will in every case maintain the intellectual property rights related to his/her own work.

Moreover, the Speaker grants FIRA DE BARCELONA the right to reproduce copies of the speaker's presentation (for example, PowerPoint slides or supporting

documents) in paper and/or electronically, allowing the referred materials to be published in the media, magazines, broadcast streamed on the Event's website, or posted on web pages related to the theme of the Event, for a minimum period of one (1) year since the date of publication.

Likewise, the Speaker represents and warrants to FIRA DE BARCELONA that the papers/abstract and all materials used in the presentation are original and authentic, and that such materials do not infringe any intellectual property rights or other rights of third parties. The Speaker shall be solely responsible for any claims or actions brought against FIRA DE BARCELONA arising from a breach of this commitment.

PERSONAL DATA

- Data Controller

FIRA INTERNACIONAL DE BARCELONA, Tax Code (CIF) Q -0873006 - A, and registered address Av. Reina Maria Cristina, s/n, 08004 Barcelona;

- Purpose and lawful basis of the processing

Your personal data will be processed, in compliance with the provisions of the European General Data Protection Regulation (GDPR) and Organic Law 3/2018 on the Protection of Personal Data and the Guarantee of Digital Rights (LOPDGDD), for the purpose of managing your participation as Speaker in the Call for Speakers activity, organized by the Barcelona Cybersecurity Congress, and for the promotion and communication of your content, including the promotional content for this and future editions of the Congress.

This may include publication on official websites, social media platforms, streaming and video on demand platforms, press releases, media coverage, and promotional materials (both digital and printed).
The lawful basis of the processing is the execution of the contractual relationship as a Speaker; and the legitimate interest in the promotion and dissemination of the Congress and the activity.

- Data recipients

Your data will not be sold, rented or otherwise made available to third parties.

In certain cases, access to your data may be granted to specific service providers that render services to FIRA DE BARCELONA, but in all cases, such providers will not process the data for their own purposes. These service providers will process your data to strict confidentiality obligations and in compliance with the requirements set out in the applicable data protection legislation.

Likewise, where applicable, your data may be shared with the police or judicial authorities that need this data or have officially requested them.

- International data transfer

In the event that any of the service providers of FIRA DE BARCELONA process personal data in a third country, FIRA DE BARCELONA will implement all measures and controls within its power to protect your personal data.

The principal measures adopted by FIRA DE BARCELONA when carrying out an international transfer of personal data include the execution of Standard Contractual Clauses approved by the European Commission, adherence to international agreements or adequacy decisions,

- **Data retention period**

Your data will be retained for the time necessary to manage the activity and, subsequently, for the period during which liabilities may arise from such data processing, duly blocked. Once the period during which such liabilities may be claimed has expired, your data will be destroyed.

The audiovisual material may be retained for as long as it maintains informational or promotional value, unless you object.

- Data protection rights

You may exercise your rights of access, rectification, erasure, objection, restriction of processing, and portability of your data before FIRA DE BARCELONA, as well as withdraw your consent, by sending a communication to dpo@firabarcelona.com, with the reference “Personal Data”.

You also have the right to lodge a complaint with the Data Protection Authority.

- Additional information

Should you wish to obtain further information regarding the processing of your data, you may consult the Privacy Policy of FIRA DE BARCELONA: https://www.firabarcelona.com/en/privacy-policy-2/

If you have any questions about the processing of your data, you can contact the DPO by email at: dpo@firabarcelona.com

ADDITIONAL INFORMATION

Submission of an abstract constitutes a formal commitment by the author to present the abstract in the session and at the time decided upon by the BCC Program Committee. Any change in the presenting author/speaker line-up needs to be communicated in writing to the Program Director. Confirmation of the replacement speaker is at the discretion of the Program Director and is not guaranteed.

If the original presenting speaker(s) are unavailable to present the abstract, it is the original author's responsibility to ensure that a qualified speaker from the same company can speak at the session. Failure to present the abstract as submitted may result in the rejection of an abstract submitted for future BCC events.

CONTACT

BCC Speaker Office:

bcc.congress@firabarcelona.com