CALL FOR CONTENT 2025
TERMS & CONDITIONS

CONTENT

PRESENTATION

The call for content aims to provide the audience with relevant information and technical sessions focused on cybersecurity threats and strategies related to protecting and enabling digital transformation. These may include but are not limited to: Threat Intelligence, Data Encryption, SBoMs HBoMs, Zero Trust, Safety Culture, Incident Response, Block Chain, Regulations and Standards, and Security Risk Assessment, within the Space, Energy, Healthcare, Manufacturing, and Process industries, among others.

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:

- **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.

Advancing Technology in Cybersecurity

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:

- **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?

Protecting the Supply Chain

In today's interconnected world, safeguarding the cybersecurity supply chain is crucial to maintaining the integrity of our digital landscape. Protecting the supply chain involves leveraging key elements such as SBoMs for visibility, blockchain technologies for transparency and traceability, risk management for proactive threat assessment, and incident response for swift mitigation. Learn how these components work together to safeguard our software and hardware bills of materials to ensure the security and resilience of our interconnected systems.

Session Topics:

- **SBoMs/HBoMs**

Your supply chain is only as secure as its weakest link. This is true for cybersecurity as well. If you do not understand what is in your software or hardware bill of materials, you may be exposing your organization to unknown vulnerabilities.

- **Incident Response**

  With cyberattacks on the constant rise it is fair to assume at some point your network may be compromised. What you do now, today, to prepare for this contingency will make all the difference in terms of the cost and manpower needed to get your business back online and recover your data.

- **Block Chain**

  Block Chain is not crypto, but it is used in crypto for the same reason it can be helpful in protecting your organization's data. Block chain is a decentralized ledger with each node representing a potential recovery point. It is a secure and immutable chain of transactions that cannot be altered or forged.

- **Risk Management**

  How safe is too safe? At what point does your cybersecurity strategy disrupt the very business it was designed to protect? How much is too much to spend on cybersecurity? What is the real risk of a cybersecurity breach? All of these questions fall under the complex topic of risk management, and the answers themselves change with the evolving threat landscape.

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:** 30 minutes including 20 minutes for the presentation + 10 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.

TIMELINE

The submission process has five major steps:

Abstract Submission: submitted by 15th December 2024 23:59h 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:
Notifications to be sent to abstract authors by mid-February 2025

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://app.oxfordabstracts.com/stages/76449/submitter
Until December **15, 2024 23H59 CET.**

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 perform, being such recording able to be reproduced, as part of the materials of the general conference. 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.

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 & IOTSWC Speaker Office:

iots.technicaloffice@firabarcelona.com