



COMMERCIAL BANK OF ETHIOPIA

3rd Annual Cybersecurity Awareness Month Conference 2026

"Don't Make It Easy for Them: AI-Powered Defense, Zero Trust Mindset"

Building Human Cyber Resilience for 48 Million Digital Lives.

29-30 October 2026 | Addis Ababa, Ethiopia

In Partnership with CIO Africa

EXPRESSION OF INTEREST (EOI)

Call for Cybersecurity Start-ups, Researchers, CTF Teams & Practitioners

The Commercial Bank of Ethiopia (CBE) invites cybersecurity start-ups, researchers, Capture The Flag (CTF) teams, practitioners, innovators, university teams, and emerging cybersecurity professionals to submit an Expression of Interest (EOI) to participate in the 3rd Annual Cybersecurity Awareness Month Conference 2026.

Under the approved theme, the conference will bring together cybersecurity leaders, financial-sector professionals, regulators, technology practitioners, researchers, students, innovators, and emerging cybersecurity talent to exchange knowledge, demonstrate practical capabilities, and strengthen cybersecurity resilience.

CBE is opening a dedicated platform for selected participants to present, demonstrate, or showcase cybersecurity solutions, research, prototypes, tools, techniques, and practical innovations relevant to the conference objectives.

1. Who Should Apply?

Expressions of interest are welcomed from:

- Emerging Cybersecurity start-ups and innovation teams
- Cybersecurity researchers and academic teams
- CTF teams
- Cybersecurity practitioners and professionals
- University cybersecurity students

Applicants may participate individually or as a team, research group, start-up, university team, or other appropriate entity.

2. Conference Participation Tracks

DAY 1 - EXECUTIVE FORUM - 29 October 2026

Leading Resilience in the Age of AI-Driven Threats

- AI-enabled cyber threats, AI governance and security
- Cybersecurity governance, risk and compliance
- Cyber fraud and digital financial security
- Identity and access management
- Executive-level cybersecurity research and case studies

Selected contributors may be invited to deliver a presentation, executive briefing, solution showcase, or demonstration appropriate for the senior-level audience.

DAY 2 - PRACTITIONERS & FUTURE CYBERSECURITY TALENT - 30 October 2026

Practicing Readiness - Real-World Skills for an AI-Powered Threat Landscape

- Ethical Hacking, Penetration Testing, Digital Forensics, and Incident Response
- CTF activities
- Cloud, network, Application and API security
- AI and cybersecurity in Combating Cyber fraud and financial crime
- Security awareness and human cyber resilience
- Cybersecurity research and innovation

3. What Can Be Presented or Showcased?

Cybersecurity Solution Showcase: Demonstration of an existing cybersecurity product, platform, tool, or solution.

Prototype & Innovation Showcase: Presentation or demonstration of a working prototype, proof of concept, or emerging cybersecurity innovation.

Research Presentation: Presentation of relevant cybersecurity research, findings, methodologies, or innovations.

Technical Demonstration: Live or controlled demonstration of a cybersecurity tool, technique, capability, or practical use case.

CTF / Hands-on Activity: Practical cybersecurity challenges, CTF demonstrations, or interactive technical activities.

Practitioner Presentation: Presentation of a practical cybersecurity experience, implementation, lesson learned, or technical case study.

CBE will determine the appropriate participation format based on the relevance, quality, maturity, demonstrability, and suitability of each submission, as well as available program capacity.

4. What Selected Participants Receive

Selected participants will receive an opportunity to present or showcase their work to a distinguished cybersecurity audience, including financial-sector leaders, cybersecurity professionals, researchers, practitioners, students, innovators, and other conference participants.

- A dedicated presentation or demonstration slot
- A designated prototype or solution showcase space
- Opportunities for professional networking and knowledge exchange
- Certificate of Participation, where applicable

Important

This EOI is intended to provide a platform for knowledge sharing, practical demonstration, innovation, and professional visibility.

No cash prize, financial award, or payment is associated with this EOI.

Selection for participation does not constitute CBE procurement, endorsement, certification, or a commitment by CBE to purchase any product or service.

Any future commercial, technical, or institutional engagement will be subject to applicable CBE policies and procedures and, where required, a separate evaluation process.

5. Submission Requirements

Interested applicants should submit the following:

- Name of individual, team, start-up, or organization
- Name and contact details of the focal person
- Short profile/background
- Title of proposed presentation, demonstration, or showcase
- Description of the proposed work - maximum 500 words
- Current development or maturity stage, where applicable
- Target audience - executive, practitioner, student, researcher, etc.
- Technical, space, equipment, or logistical requirements
- Links to relevant work, where available (website, research paper, GitHub repository, prototype, demonstration video, portfolio)

6. Selection Considerations

Submissions will be reviewed based on considerations including:

Criteria	Consideration
Relevance	Alignment with the conference theme and program
Innovation	Originality and innovative value
Practical Value	Demonstrable cybersecurity application
Technical Merit	Technical quality and credibility
Impact	Potential contribution to cybersecurity resilience
Demonstrability	Ability to provide a meaningful presentation or demonstration
Audience Value	Relevance to the intended conference audience
Maturity	Appropriate development stage for the proposed format

CBE reserves the right to select submissions based on program relevance, quality, available capacity, and overall conference requirements.

Submission of an EOI does not guarantee selection.

7. Technical and Security Requirements

For technical demonstrations, CTF activities, ethical hacking, penetration testing, vulnerability research, or similar activities:

- Demonstrations must be conducted in an approved and controlled environment
- Participants must not conduct unauthorized scanning, testing, exploitation, or access against CBE systems, third-party systems, or other live infrastructure
- No activity should disrupt or degrade operational systems, networks, services, or data
- Participants are responsible for obtaining all necessary permissions relating to systems, software, research, content, and intellectual property used in their demonstrations
- CBE reserves the right to review and approve the technical setup of demonstrations before the event

The conference is a platform for responsible cybersecurity knowledge sharing and practical learning.

8. Participation Conditions

Selected participants are expected to:

- Comply with CBE's conference rules and applicable security requirements
- Provide presentation or demonstration materials within the timeline communicated by the organizing team
- Observe applicable laws, ethical standards, intellectual-property requirements, and responsible disclosure principles
- Ensure that demonstrations are safe, controlled, and appropriate for the conference environment

- Coordinate all technical and logistical requirements with the designated conference team

9. Submission Deadline

Deadline: September 15, 2026

How to Apply: Please submit your EOI to informationsecurity@cbe.com.et

Subject: "EOI - 3rd CBE Cybersecurity Awareness Month Conference 2026"

10. Join the Cybersecurity Community

CBE welcomes innovative thinkers, researchers, practitioners, start-ups, university teams, CTF teams, and emerging cybersecurity professionals whose work contributes to a safer, more resilient digital ecosystem.

If your work helps organizations and individuals detect threats, reduce cyber risk, strengthen human resilience, protect digital services, respond to incidents, or recover from cyber threats, we encourage you to submit your Expression of Interest.

"Don't Make It Easy for Them: AI-Powered Defense, Zero Trust Mindset"

Building Human Cyber Resilience for 48 Million Digital Lives.

29-30 October 2026 | Addis Ababa, Ethiopia

In Partnership with CIO Africa