THREAT 2026

Submission Guidelines

CONTINUUM: Securing Modern Supply Chains

THREAT 2026 invites contributions that address the conference theme: **CONTINUUM: Securing Modern Supply Chains**.

The conference welcomes both research-based and experience-based contributions. THREAT recognises that important cybersecurity knowledge does not originate solely from academic research and that some of the most important knowledge is developed in practice: through implementation, response, governance, failure, recovery, adaptation, and organisational learning.

1 Submission Formats

Authors should select one of the following submission formats.

1.1 Research Paper

Research Papers are intended for academic, technical, postgraduate, and research-oriented contributors.

They should be prepared using the IEEE A4 conference paper format: https://www.ieee.org/conferences/publishing/templates.

Suggested length: 5–6 pages, excluding references.

Research Papers should clearly state:

- the problem or research question;
- the approach, method, framework, design, or analysis;
- the main findings, argument, contribution, or technical insight;
- the relevance to **CONTINUUM: Securing Modern Supply Chains**; and
- the implications for research, policy, practice, governance, operations, or technology.

1.2 Professional Insight Paper

Professional Insight Papers do not need to follow a conventional academic research paper structure. They should, however, be clear, evidence-informed, reflective, and useful to others.

Suggested length: 3–5 pages.

Professional Insight Papers should address:

- the professional, sector, organisational, or operational context;
- the cybersecurity challenge, risk, incident, decision, or issue;
- what was observed, done, changed, or learned;
- the evidence or professional experience on which the insight is based;
- the relevance to **CONTINUUM: Securing Modern Supply Chains**; and

- the implications for practice, policy, governance, operations, or technology.

Professional Insight Papers must not be vendor marketing papers. Commercial organisations are welcome to submit evidence-based case insights and lessons learned, but submissions that primarily promote a product, service, platform, or company will not be accepted as papers.

1.3 Poster Submission

Poster Submissions are intended for concise contributions, early-stage work, postgraduate work, focused case insights, emerging ideas, visual summaries, or work that is better suited to direct discussion.

Suggested initial submission length: 500–800 words.

Poster Submissions should state:

- the topic or problem;
- the main idea, finding, insight, lesson, or argument;
- the relevance to **CONTINUUM: Securing Modern Supply Chains**; and
- the value for the THREAT audience.

Accepted poster authors will be required to prepare a poster for display and discussion at the conference. Authors whose presentations are not accepted may be invited to submit posters.

2 Review Outcomes

Submissions may receive one of the following outcomes:

- Accepted for Roundtable Presentation;
- Accepted for Poster Presentation;
- Revise and Resubmit; or
- Not Accepted.

The THREAT Programme Committee's decision is final.

3 Review Criteria

Submissions will be reviewed using the following criteria:

- relevance to **CONTINUUM: Securing Modern Supply Chains**;
- clarity of contribution;
- quality of evidence, analysis, experience, or argument;
- practical, policy, operational, technical, or scholarly value;
- suitability for roundtable or poster discussion; and
- responsible handling of sensitive material.

Academic and technical submissions will also be considered in relation to conceptual clarity, method, structure, and contribution to knowledge.

Professional Insight Papers will also be considered in relation to authenticity, practical significance, reflective value, and usefulness to others.

4 Presentation Model

THREAT does not use standard conference presentation formats.

Papers accepted for presentation will be grouped into thematic roundtables. Each accepted paper author will have four minutes to communicate the most important contribution of the paper. This may be a key finding, argument, case insight, lesson learned, policy implication, technical contribution, or practical recommendation.

Authors should not attempt to present the full paper.

The short author inputs will be followed by a facilitated discussion with the panel and audience. This format is intended to promote serious engagement between academia, industry, government, logistics, policy, and cybersecurity practice.

Poster authors will present their work visually and engage with delegates during the poster session.

5 One-Page Summary for Accepted Papers

Authors of accepted papers will be required to submit a tight one-page summary after acceptance.

This summary is separate from the final paper submitted for the proceedings. It will support the roundtable or poster discussion and may be used in the conference programme, website, printed delegate materials, or post-conference communications.

The one-page summary should clearly communicate:

- the problem or issue addressed;
- the main contribution;
- the relevance to **CONTINUUM: Securing Modern Supply Chains**; and
- the implications for research, practice, policy, governance, operations, or technology.

The summary should not simply repeat the abstract. It should explain what the paper contributes and why it matters.

6 Proceedings

Accepted Research Papers and Professional Insight Papers will be considered for inclusion in the official THREAT 2026 Conference Proceedings, which will carry an ISBN.

The proceedings will be made available digitally. Printed copies may be made available on request and at a fee.

Poster submissions may be included in the proceedings as abstracts.

Inclusion in the proceedings requires submission of the final accepted version by the stated deadline and compliance with conference formatting, editorial, copyright, and disclosure requirements.

Authors retain copyright in their work. By submitting a final accepted paper, authors grant THREAT permission to include the paper, abstract, author details, and one-page summary in the conference proceedings, website, digital programme, and related conference materials.

7 Responsible Disclosure and Confidentiality

Authors are responsible for ensuring that submissions do not disclose confidential, proprietary, sensitive, or security-sensitive information without permission.

Case studies should be anonymised where necessary.

Submissions involving incidents, vulnerabilities, operational systems, or organisational security practices should be handled responsibly.

8 Use of Generative AI

Authors may use generative AI tools for language editing or drafting assistance, but they remain fully responsible for the accuracy, originality, integrity, and authorship of the submission.

Any substantive use of generative AI should be disclosed. Any evidence of indiscriminate AI use will lead to immediate disqualification of the submission.

9 Submission Dates

Milestone	Date
Call for papers opens	20 May 2026
Submission deadline	31 July 2026
Review period	1–28 August 2026
Notification of acceptance	31 August 2026
Final revised submission deadline	30 September 2026
Programme finalised	7 October 2026
Conference	28–30 October 2026

Enquiries

For enquiries, contact: maharajms@cybersecinafrica.com.