teiss
Awards2026

Entry Pack

#teissAwards
www.teiss.co.uk/awards

About teissAwards2026

The teissAwards2026 recognise excellence in cyber and information security, with a particular focus on the contributions of vendors and technologies in relation to the use, development, and deployment of information security in the past 12 months.

The categories within the teissAwards2026 are assessed by an independent panel of distinguished judges, and the winners will be announced at the teissAwards2026 gala dinner, held on the 26th February 2026.

The teissAwards2026 are part of a broader portfolio of information security events, which have taken place over the last decade, and represents the largest and most comprehensive cyber security gathering of experts in Europe.

How are the awards organised?

There are 19 Categories within the teissAwards2026, all focused on recognising excellence amongst the information security vendor market.

Who is eligible?

The teissAwards2026 are open to all information security product, service and training providers. Each Category has defined eligibility criteria and guidance on who should apply.

How can we enter?

For each Category, there are a set of questions you must answer in order to make your Round 1 Submission. Your organisation is allowed to enter as many categories as are applicable to you.

You will then need to submit your Round 2 video recording.

Where do we enter?

Entry is done via this site, by clicking "Enter now" and following the instructions. You can start and save your entries before submitting.

Who decides if we've won?

A select panel of industry experts make up our judging panel. Their details can be seen on the following pages. They will score all submitted entries that are shortlisted.

How much does it cost to enter?

Entry is free.

Book a Table

The teissAwards2026 evening will begin at 6.30pm and commence with a drinks reception, include a three course meal with wine, and be accompanied by a celebrity MC and entertainment. Over 250 attendees will convene for an evening of celebration, as the information security vendors gathers to celebrate the very best in the industry.

VIP Tables

We have two VIP tables available at the teissAwards2026

- Welcome champagne
- Preferential position in the Awards room
- 10 seats for your and your colleagues
- 3 course dinner
- Awards ceremony
- Wine, beer, soft drinks with dinner

VIP Table £4,720

Standard Tables

- Welcome sparkling wine
- 10 seats for your and your colleagues
- 3 course dinner
- Awards ceremony
- Wine, beer, soft drinks with dinner

Standard Table £4,195

Individual seats are available at **£524 per seat**, with the standard table package.

The Judges

Steve Furnell

Professor of Cyber Security

University of Nottingham

Steven is a Professor of Cyber Security at the University of Nottingham. His main research interests are broadly linked to the intersection of human, technological and organisational aspects of cyber security, and has authored over 330 papers in refereed international journals and conference proceedings, as well as various books, chapters, and professional articles.

Andrea Cullen

CEO & Co-Founder

CAPSLOCK

Andrea has years of industrial experience as a computer programmer and systems analyst working on projects throughout the UK where she has been responsible for the development and implementation of many software systems. She co-authored, developed, and delivered the GCHQ-certified Cyber Security Master's degree at the University of Bradford, and is also the Co-founder and Head of Research & Development at CAPSLOCK.

Lisa Ventura

Editor & Founder

Cyber Security Unity

Lisa is a keynote speaker, moderator and panellist, and has taken part in numerous conferences and events, both in-person and virtual. She is often asked to write articles, blogs and press features about cyber security, neurodiversity, mental health issues and more.

Thom Langford

Founder

(TL)2 Security

Thom is an industry engaged and sought after information security subject matter expert, speaker, and award-winning security blogger. He is the sole founder of Host Unknown, a loose collective of three infosec luminaries combined to make security education and infotainment films.

Paul Watts

Distinguished Analyst

Information Security Forum

Paul is a senior Information Security and Technology professional with over twenty-six years' experience covering vertical markets including Transportation, Banking and Finance, Manufacturing, Retail and Telecommunications both in Europe and the UK. He was named as one of the top 100 global CISOs in the HotTopics.ht "CISO 100 2017" in 2017 and 2020.

Danny Dresner

Professor of Cyber Security

University of Manchester

Danny is a respectable Professor of Cyber Security at the University of Manchester and a Fellow of the Institute of Information Security Professionals. Whilst at the NCSC, he created the core of SANS' training for BS 7799, edited national security breaches surveys, and wrote the first standards for source code escrow. He has contributed to books, conferences, and appeared on numerous TV channels including the BBC.

David Cartwright

CISO

Santander International

Dave has been based in Jersey since 2009, and is presently head of IT security for an international bank. He is the co-founder and chairman of the Jersey Charitable Skills Pool; deputy chairman of the Channel Islands Information Security Forum; a committee member of the Jersey branch of the BCS; and the Digital Committee of the Jersey Chamber of Commerce.

Edewede Oriwoh

Group IT Information and Cyber Security Manager

Zigup Plc

Edewede has worked in various areas of Information and Cyber Security including in Data, Identity and Access Management, Asset, Cloud, Vulnerability Management, Cyberphysical, Security Awareness, Threat Hunting and Threat Intelligence, Incident Management and Disaster Recovery, among others. She has a keen interest in Proactive, Continuous, Responsive and Reactive Security.

She encourages the support of end users with security awareness guidance, well-configured and managed tools as well as clear Policies, Processes and Procedures so they can play their part as an essential link in any organisation's Cyber Security chain.

She also promotes the importance of remembering the fundamentals such as making security a habit and, more broadly, remembering that, "If it does not exist, there's nothing to secure".

Edd Hardy

SVP Cyber Security

AlixPartners

Edd is a highly experienced consultant assisting organisations, investors and C-suite to manage cyber risk and foster growth. Some of his previous roles include a pentester, ISO27001 Auditor, QSA, Risk Analyst, and advisor.

Ed Tucker

CyberSecurity CTO

Telefonica Tech

Ed is a recognised expert, with a rich history of creating high performance teams, world class capabilities, driving business resilience and confidence. He is a pragmatic, yet passionate individual with a demonstrable record of defining and executing transformational change into businesses of varying maturities.

Paul Holland

Cyber Capability Manager

Royal Mail

Paul has worked in Information Security and IT for over 25 years, across financial, consultancy and managed services, retail, education, manufacturing and logistics plus more, before joining the ISF in 2019 and presently at Royal Mail. He was previously responsible for technical security, including architecture and penetration testing, and awareness programs as well as managing senior stakeholders and incident response.

Jonathan Craven

Data privacy and cybersecurity consultant

XRHA

After first training as a psychologist, Jonathan has spent most of his career working in the 'Holy Trinity' of public sector employers – local authority, NHS and the police service – in privacy, data protection and information governance. Throughout that time, he has led organisational change to raise awareness, improve training, and promote better governance and security processes and behaviours. He is currently the Data Privacy and Cyber security consultant at XRHA.

Keil Hubert

Associate Principal, Security Human Risk Management

OCC

Keil Hubert is the head of Security Training and Awareness for OCC, the world's largest equity derivatives clearing organization, headquartered in Chicago, Illinois. Prior to joining OCC, Keil has been a U.S. Army medical IT officer, a U.S.A.F. Cyberspace Operations officer, a small businessman, an author, and several different variations of commercial sector IT consultant. Keil deconstructed a cybersecurity breach in his presentation at TEISS 2014, and has served as Business Reporter's resident U.S. 'blogger since 2012. His books on applied leadership, business culture, and talent management are available on Amazon.com. Keil is based out of Dallas, Texas.

Chuck Brooks

Adjunct Professor, Georgetown University

Brooks Consulting International

Chuck Brooks is President of Brooks Consulting International and an Adjunct Professor at Georgetown University, teaching risk management and cybersecurity. Named a "Top 5 Tech Person to Follow" by LinkedIn, he has nearly 118,000 followers and manages 10 cybersecurity groups. A recognized thought leader, Chuck has briefed the G20, the Vatican, and USTRANSCOM on cybersecurity, and served on National Academy of Sciences advisory panels for the USAF and biotech. He also contributes to CISA's space systems security efforts. He writes for Forbes, The Washington Post, The Hill, and others, with 57,000 newsletter subscribers. Two of his books on cybersecurity and technology are due out this year. Chuck previously held executive roles at General Dynamics, Xerox, and Rapiscan, and received presidential appointments from two U.S. Presidents. He holds degrees from the University of Chicago and DePauw University, and a certificate from The Hague Academy of International Law.v

Satyam Rastogi

Director of Information Security & DevOps

BAMKO

He is responsible for safeguarding BAMKO's digital assets in accordance with ISO 27001, SOC 2, GDPR, CCPA, and PCI DSS standards whilst bolstering their cybersecurity posture. His role involves leading dedicated teams in vulnerability assessments, penetration testing, and the vigilant monitoring of infrastructures to pre-empt risks and ensure compliance.

Edward Starkie

Director of Cyber Risk

Thomas Murray

Edward adopts a business-centric approach to cyber security, data protection, and digital operational resilience. He leverages best practices gained from interacting with a diverse set of organisations and clients.

Edward is confident in his ability to engage effectively with both technical experts and Board-level stakeholders and ultimately deliver tailored services that empower organisations to identify, assess, and sustainably manage cyber security risks in a pragmatic, results-driven manner.

Lessie Skiba

Deputy Managing Director

Cyber Readiness Institute

Lessie is Global Director of Outreach and Partner Engagement for the Cyber Readiness Institute. Most recently, she worked for a cybersecurity start-up, Nisos, as Chief of Staff and Interim Director of Marketing. She also brings experience in working with new and emerging technology and cybersecurity companies from her previous role with an early-stage venture capital firm.

Sandra Bell

Group Head of Organisational Resilience

Novuna

Sandra is an experienced leader with over 30 years' experience of helping organisations develop the skill, will and grit to succeed regardless of what happens. She has a track record of facilitating organisations achieve and maintain standards together with firsthand experience of managing crisis, emergency and disaster recovery activities. Sandra is also a strong influencer who is able to rapidly assimilate complex regulatory and stakeholder environments and ensure risk and compliance solutions are intimately aligned to corporate strategy. An excellent communicator and business builder who has created and led successful business units and consulting practices.

Janet Bastiman

Chief Data Scientist

Napier AI

Janet is a highly motivated C-level executive with 10 years' experience in leading technical departments, managing process improvements and shaping future technical strategy. She pursued academic achievement to the highest levels with a Ph.D. in computational neuroscience and combine this knowledge and equal determination with my experience to achieve superb results in various sectors of the IT industry. She regularly contribute technical articles, particularly in the areas of deep learning and AI, and also blog on mathematics, technology and 3D printing.

Laurie Gibbett

Cyber Risk Quantification Manager

KPMG

Laurie specialises in security strategy and risk. More specifically, she looks to understand cyber risk exposure in financial terms and identify the priority defence mechanisms to reduce cyber risk. She uses Design Thinking techniques to assess situations and scenarios before deep diving into potential solutions. Laurie is creative at heart, so like to incorporate visual design into her personal and work life. She has an eye for detail however, she likes to bring out key messages and present the bigger picture. She has a strategic approach to most things and purposefully get involved in projects outside her day-to-day work on deals to ensure, she is working on the strategy of the security business unit, implementing initiatives for purposeful change.

Stuart Frost

Head of Enterprise Security and Risk Management

Department for Work and Pensions (DWP)

tuart Frost, BEM, is head of Enterprise Security and Risk Management within the UK Government. A vastly experienced, highly certified Security and Governance, Risk & Compliance (GRC) professional with extensive sector knowledge and significant experience of delivering successful risk-based security programmes, across large scale, multi-disciplined and geographically dispersed organisations. He is also a leading voice on managing risks faced by the burgeoning use of interconnected supply chains. An accomplished speaker, he has taken part in events across the UK, Europe, USA and Asia.
Stuart has won multiple industry global awards for his work in the GRC space and is adept at integrating all security disciplines to enable a holistic approach in support of business objectives. He was named as one of the UK's top 50 Tech Leaders and a top 30 Transformational Change Leader in May 2024 for his role in driving innovation and change across the security sector.
He was awarded the British Empire Medal (BEM) in 2017 for his services to the local community and in 2023 was also the proud recipient of the Coronation medal in recognition of his security input to the Coronation of King Charles III.

Moona Ederveen-Schneider

Advisory Board Member

Cyber London

Moona Ederveen, is a Board Advisor and Innovative Tech Influencer, and most recently, served as Executive Director EMEA in financial services. Visiting international security conferences from age 16, she consulted at global banks and advised on cyber security and risk for nearly two decades. As a multi-lingual brand ambassador to financial services, other sectors, and government stakeholders, she is an avid builder of trusted communities. A strong advocate for cross-sector crisis preparedness and resilience, she also works to encourage the next generation of talent into tech careers.

Award Categories

teiss
Awards2020
The European Information Security Summit
WINNER
Best use of machine learning in security automation
your organisation

We are excited to announce that the following **19 Awards** are all now accepting submissions from prospective teissAwards2026 winners:

1. **Best Cloud Security Solution**
2. **Best Email Security Solution**
3. **Best Incident Response Solution**
4. **Best Endpoint Security Solution**
5. **Best AI Security Solution**
6. **Best Threat Intelligence Technology**
7. **Best Vulnerability Management Solution**
8. **Best Human Risk Solution**
9. **Best Penetration Testing Solution**
10. **Best Security Compliance Solution**
11. **Best New Launch Product**
12. **Best Ransomware Solution**
13. **Best Network Security Solution**
14. **Cyber Security Company of the Year**
15. **Cyber Security Start-up Company of the Year**
16. **Best SIEM Solution**
17. **Best Identity and Access Management Solution**
18. **Best SaaS Security Posture Management Solution**
19. **Best Emerging Security Technology**

1. Best Cloud Security Solution

Eligibility criteria

The entrant must be an organisation that offers a cloud security solution that mitigates risks associated with the protection of information and applications in the cloud environment.

Title of entry

Give your entry a title to attract the judges' attention.

How to enter

Submissions must be no longer than **150 words** on each of the following questions:

- Explain your cloud security solution in simple, non-technical language.
- How effective are your solution's vulnerability management and malware detection capabilities, and how easy are they to improve upon?
- What integration possibilities does your solution provide, and how intuitive and easy to navigate is the interface?
- Why do you consider your solution the best on the market in the past 12 months?

2. Best Email Security Solution

Eligibility criteria

The entrant must be an email security vendor who offers a solution that safeguards the privacy of email messages by filtering against spam, malware and other malicious emails, while providing integrated protection against sophisticated email attacks.

Title of entry

Give your entry a title to attract the judges' attention.

How to enter

Submissions must be no longer than **150 words** on each of the following questions:

- Explain your cloud security solution in simple, non-technical language.
- How does your solution safeguard the privacy of email messages while detecting spam and other malicious web-based content?
- In addition to anti-spam and email encryption capabilities, what other features does your solution offer?
- Why do you consider your solution the best on the market in the past 12 months?

3. Best Incident Response Solution

Eligibility criteria

The entrant must be an incident response provider with a service or software that provides users with the tools to identify and respond to security breaches, as well as reporting and analysing incident data.

Title of entry

Give your entry a title to attract the judges' attention.

How to enter

Submissions must be no longer than **150 words** on each of the following questions:

- Explain your cloud security solution in simple, non-technical language.
- How does your solution detect, track and manage incidents effectively? Does it integrate well with other threat intelligence sources for real-time visibility of the threat and vulnerability landscape?
- How does it leverage advanced reporting and incident data analytics capabilities to provide actionable insights? Does it use any orchestration and automation capabilities to improve quality of analysis or support compliance regulation?
- Why do you consider your incident response solution the best on the market in the past 12 months?

4. Best Endpoint Protection Solution

Eligibility criteria

The entrant must be a provider whose solution continuously analyses endpoints to detect and respond to potential threats in real time.

Title of entry

Give your entry a title to attract the judges' attention.

How to enter

Submissions must be no longer than **150 words** on each of the following questions:

- Explain your detection solution in simple, non-technical language.
- How does your solution provide real-time continuous visibility on endpoints? What endpoint protection suite capabilities does your solution provide to detect and respond to potential threats? To what extent are these capabilities automated?
- Does your solution offer multiple response capabilities? What other optional managed services does your solution provide?
- Why do you consider your detection solution the best on the market in the past 12 months?

5. Best AI Security Solution

Eligibility criteria

The entrant must have a AI-powered solution aimed at detecting, preventing or resolving current cyber-threats.

Title of entry

Give your entry a title to attract the judges' attention.

How to enter

Submissions must be no longer than **150 words** on each of the following questions:

- Explain your AI-powered solution in simple, non-technical language.
- How does it proactively detect, block and remediate cyber-threats? How does it save analysts' time and foster critical decision-making in real time?
- Does it have continuous self-learning and cognitive capabilities that adapt to the evolving threat landscape?
- Why do you consider your AI-powered solution the best on the market in the past 12 months?

6. Best Threat Intelligence Technology

Eligibility criteria

The entrant must be a threat intelligence technology supplier whose solution or product provides organisations with timely intelligence on the latest cyber-threats affecting their IT infrastructure, as well as techniques to combat these threats.

Title of entry

Give your entry a title to attract the judges' attention.

How to enter

Submissions must be no longer than **150 words** on each of the following questions:

- Explain your cyber-threat intelligence technology in simple, non-technical language.
- How does it provide information on emerging threats and vulnerabilities? Does it outline remediation practices for common and emerging threats?
- What integration possibilities does your threat intelligence technology provide? Is its interface-intuitive and user-friendly? How does it analyse anomalies on different types of networks and devices?
- Why do you consider your cyber-threat intelligence technology the best on the market in the past 12 months?

7.

Best Vulnerability Management Solution

Eligibility criteria

The entrant must be a vulnerability management provider whose solution helps organisations identify and manage vulnerabilities associated with system configurations, patches and other information security challenges.

Title of entry

Give your entry a title to attract the judges' attention.

How to enter

Submissions must be no longer than **150 words** on each of the following questions:

- Explain your vulnerability management solution in simple, non-technical language.
- How does it deliver continuous scanning facilities capable of unearthing hidden vulnerabilities? Are there options to conduct compliance-specific scans and reports?
- What integration possibilities does it offer? How is the user interface designed to be easy to navigate?
- Why do you consider your vulnerability management solution the best on the market in the past 12 months?

8.

Best Human Risk Solution

Eligibility criteria

The entrant must be a security awareness training and/or behavioural science specialist offering ready-to-use security training and awareness campaigns and/or behavioural science to better equip organisations against real-world cyber-threats.

Title of entry

Give your entry a title to attract the judges' attention.

How to enter

Submissions must be no longer than **150 words** on each of the following questions:

- Explain your human risk solution in simple, non-technical language.
- How does it better manage and resolve the challenges associated with social engineering, phishing and ransomware attacks? How have you leveraged behavioural science in delivering simulated phishing attacks and policies?
- How does your product or service help organisations save time and reduce cost compliance initiatives? Does it offer analytics and reporting capabilities for better decision- making?
- Why do you consider your cyber-security training and awareness product or service the best on the market in the past 12 months?

9.

Best Penetration Testing Solution

Eligibility criteria

The entrant must be a penetration testing services provider or software vendor that helps organisations detect exploitable vulnerabilities within their IT systems, networks and applications through simulated cyber-attacks.

Title of entry

Give your entry a title to attract the judges' attention.

How to enter

Submissions must be no longer than **150 words** on each of the following questions:

- Explain your penetration testing product or service in simple, non-technical language.
- What are the different types of penetration testing you perform? Do you use any open- source intelligence (OSINT) tools? How do you prove your trustworthiness?
- Do you document and report exploitable vulnerabilities to clients? What assistance do you offer to remediate potential vulnerabilities?
- Why do you consider your penetration testing product or service the best on the market in the past 12 months?

10.

Best Security Compliance Solution

Eligibility criteria

The entrant must be a security compliance vendor whose product enables organisations to manage their security processes, systems and policies to identify areas of compliance and non-compliance.

Title of entry

Give your entry a title to attract the judges' attention.

How to enter

Submissions must be no longer than **150 words** on each of the following questions:

- Explain your security compliance product in simple, non-technical language.
- Does your product come with updated or predefined templates for security frameworks in order to make compliance/non-compliance easier for analysts to determine? Are there automated integration capabilities for gathering and documenting security compliance evidence?
- Does your product provide any risk mitigation insights or generate reports using pre-mapped templates?
- Why do you consider your security compliance product the best on the market in the past 12 months?

11. Best New Launch Product

Eligibility criteria

The entrant must be a security vendor with a new product or service focused on protecting organisations' networks, systems and applications from threats. The product or service must have been launched after 1 July 2024.

Title of entry

Give your entry a title to attract the judges' attention.

How to enter

Submissions must be no longer than **150 words** on each of the following questions:

- Explain your innovative product or service in simple, non-technical language.
- How has your new product or service helped organisations effectively build cyber-resilience while addressing the challenges of the ever-changing threat landscape?
- How have users rated and reviewed your product or service? Is it simple to use and cost-effective?
- Why do you consider your innovative product or service a game-changer?

12. Best Ransomware Solution

Eligibility criteria

The entrant must be an organisation which offers a ransomware protection that assesses and mitigates ransomware risks while aiding enterprises' understanding of their ransomware response capabilities.

Title of entry

Give your entry a title to attract the judges' attention.

How to enter

Submissions must be no longer than **150 words** on each of the following questions:

- Explain your ransomware protection solution in simple, non-technical language.
- How does your solution recognises and actions pre-ransomware deployment strategies to protect enterprises against multi-faceted ransomware campaigns?
- Describe your solution's unique capabilities, specifically designed to reduce the impact of ransomware events.
- Why do you consider your solution the best on the market in the past 12 months?

13. Best Network Security Solution

Eligibility criteria

The entrant must be an organisation which offers a network security solution that defends all forms of information from cyber-attacks, unauthorised access and data loss.

Title of entry

Give your entry a title to attract the judges' attention.

How to enter

Submissions must be no longer than **150 words** on each of the following questions:

- Explain your network security solution in simple, non-technical language.
- Describe how your solution safeguards enterprises from losses resulting from data breaches while reducing overhead expenses.
- Explain how your solution contributes towards enterprises' seamless business operations through reliable access and network performance.
- Why do you consider your solution the best on the market in the past 12 months?

14. Cyber Security Company of the Year

Eligibility criteria

Entrant must be a cyber-security company with a demonstrable history of offering enterprise-level innovative and comprehensive cyber-security solutions with a significant growth in adoption, client base or product/ service effectiveness over the past 12 months.

Title of entry

Give your entry a title to attract the judges' attention.

How to enter

Submissions must be no longer than **150 words** on each of the following questions:

- Explain your cyber-security specialisation – network, endpoint, application or cloud security – in simple, non-technical language. What solutions or services are you primarily known for and what makes these unique on the market?
- Describe your company growth over the past 12 months. Have you undergone any rigorous independent security tests? How have you scored?
- What have you done as a company to bolster innovation and research and development of your product portfolio? How have you consistently measured customer satisfaction with your solution?
- Why do you consider your company the best this year?

15.

Cyber Security Start-up Company of the Year

Eligibility criteria

A company less than three years old who wishes to gain credibility, build industry connections, and establish itself as a rising star.

Title of entry

Give your entry a title to attract the judges' attention.

How to enter

Submissions must be no longer than **150 words** on each of the following questions:

- Describe your product or solution, how it is innovative and what it brings to the cyber-security market.
- Explain your company growth over the past three years. Have you undergone any rigorous independent security tests? How have you scored?
- What have you done as a company to bolster innovation and research and development of your product portfolio? How have you consistently measured customer satisfaction with your solution?
- Why do you consider your company the best start-up this year?

16.

Best SIEM Solution

Eligibility criteria

The entrant must offer a SIEM solution designed to recognise and address security threats and vulnerabilities while meeting compliance requirements using advanced AI/ML and UEBA features.

Title of entry

Give your entry a title to attract the judges' attention.

How to enter

Submissions must be no longer than **150 words** on each of the following questions:

- Explain your SIEM solution in simple, non-technical language.
- How effective are your SIEM solution's AI capabilities and other advanced security analytics in identifying anomalous behaviours and indicators of advanced threat?
- What integration possibilities does your solution provide to facilitate tracking and logging of security data for compliance purposes?
- Why do you consider your solution the best on the market in the past 12 months?

17.

Best Identity and Access Management Solution

Eligibility criteria

The entrant must offer an IAM solution designed to manage users, applications, and users' access to applications within organisations using authentication and single sign-on (SSO) capabilities.

Title of entry

Give your entry a title to attract the judges' attention.

How to enter

Submissions must be no longer than **150 words** on each of the following questions:

- Explain your IAM solution in simple, non-technical language.
- How does your IAM solution leverage multifactor authentication, conditional access policies and passwordless logins to enhance security?
- What integration possibilities does your solution offer? Is it interface-intuitive and user-friendly including a comprehensive dashboard, built-in reporting and automated user on/offboarding?
- Why do you consider your solution the best on the market in the past 12 months?

18.

Best SaaS Security Posture Management Solution

Eligibility criteria

The entrant must offer a SaaS Security Posture Management solution providing visibility into the security posture of SaaS environments and remediating security concerns via automation capabilities.

Title of entry

Give your entry a title to attract the judges' attention.

How to enter

Submissions must be no longer than **150 words** on each of the following questions:

- Explain your SaaS solution in simple, non-technical language.
- How does your SSPM solution continuously identify, assess and mitigate threats and shadow IT risks in real time using automation?
- Describe the key features and capabilities of your SSPM, and how they address organisations' concerns about complex configuration settings for multiple applications and interfaces.
- Why do you consider your solution the best on the market in the past 12 months?

19. Best Emerging Security Technology

Eligibility criteria

The entrant must offer an emerging security technology including AI/ML, blockchain, IoT and quantum computing aimed at enabling organisations to enhance their security posture, mitigate potential risks and safeguard sensitive data.

Title of entry

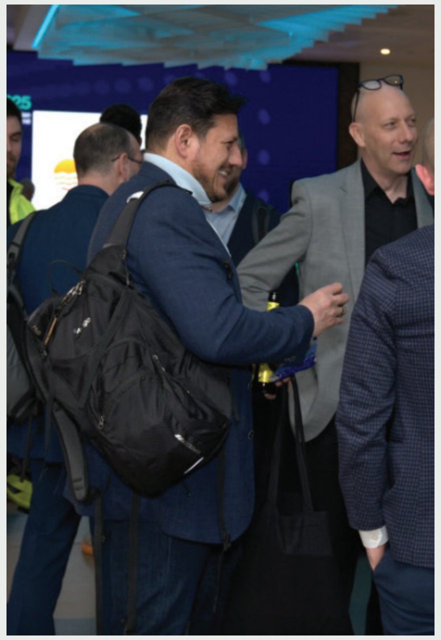
Give your entry a title to attract the judges' attention.

How to enter

Submissions must be no longer than **150 words** on each of the following questions:

- Explain your emerging technology in simple, non-technical language.
- How is your emerging security technology transforming the cyber-security landscape and enhancing data protection?
- Describe the key features and capabilities of your emerging security technology? What integration possibilities does your technology offer? How interface-intuitive and user-friendly is it?
- Why do you consider your solution the best on the market in the past 12 months?

MOMENTS FROM THE 2025 EVENT

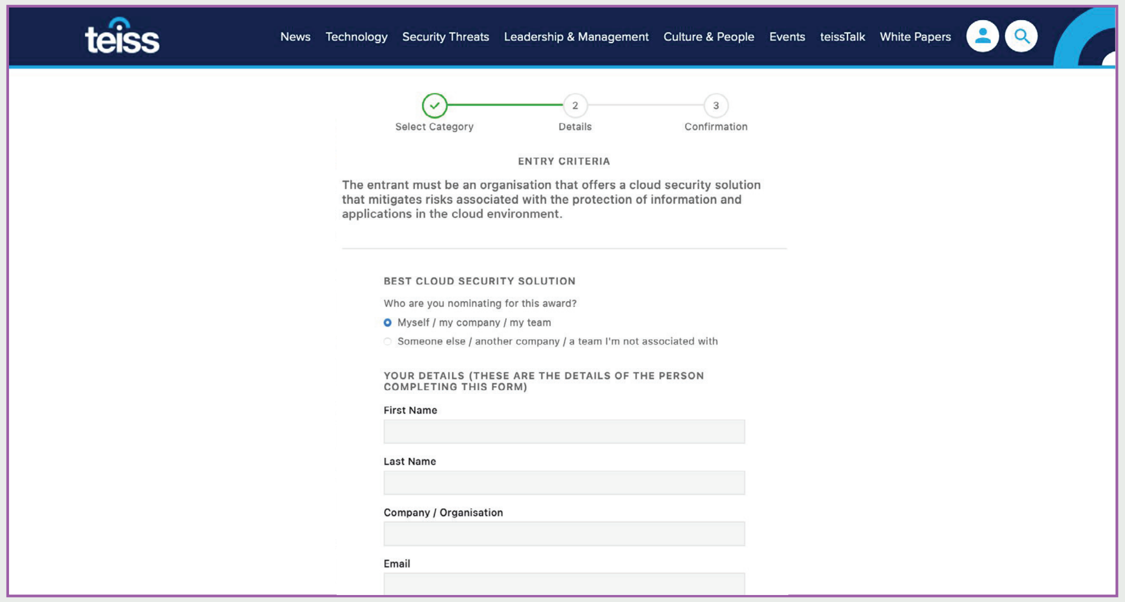


Entering teissAwards2026

Step 1: Writing your entry

Visit www.teiss.co.uk/awards and hit "Enter."

The person completing the entry should complete this form (they may not be the person and organisation being entered).



✓ Select Category — 2 Details — 3 Confirmation

ENTRY CRITERIA

The entrant must be an organisation that offers a cloud security solution that mitigates risks associated with the protection of information and applications in the cloud environment.

BEST CLOUD SECURITY SOLUTION

Who are you nominating for this award?

● Myself / my company / my team

○ Someone else / another company / a team I'm not associated with

YOUR DETAILS (THESE ARE THE DETAILS OF THE PERSON COMPLETING THIS FORM)

First Name

Last Name

Company / Organisation

Email

Step 2: Next steps

We will contact you regarding the next steps in your entry. All submissions are reviewed and clarification of some details may be sought prior to judging. We will also be in contact later in the year to confirm whether your entry has made the shortlist.

Should you need any assistance, or have any questions, email awards@teiss.co.uk

To find out more about teissAwards2026, please contact:

Sponsorship

Marc Morrow Sponsorship Sales Manager
m.morrow@teiss.co.uk
Telephone:
+44 (0)20 8349 6453
Mobile:
+44 (0)7977 926 736

Grant Scheffer Sponsorship Sales Manager
g.scheffer@teiss.co.uk
Telephone:
+44 (0)20 8349 6478
Mobile:
+44 (0)7811 010 102

Jean Philippe Le Coq Sponsorship Sales Manager
jp.lecoq@teiss.co.uk
Telephone:
+44 (0)20 8349 5592
Mobile:
+44 (0)7494 705170

Submissions

Joseph Yiadom Submissions Manager
awards@teiss.co.uk

Updated: July 2025
www.teiss.co.uk