इलेक्ट्रॉनिकी एवं सूचना प्रौद्योगिकी मंत्रालय
MINISTRY OF ELECTRONICS AND INFORMATION TECHNOLOGY

www.isea.gov.in

DSCI
PROMOTING DATA PROTECTION
A nasscom Initiative

CYBER SECURITY INNOVATION CHALLENGE 1.0

DRIVING SECTOR-RELEVANT & FUTURE-READY CYBERSECURITY SOLUTIONS

The **Cyber Security Innovation Challenge 1.0 (CSIC 1.0**) under the Information Security Education and Awareness (ISEA) program of MeitY aims to foster indigenous, research-driven cybersecurity solutions from the academic ecosystem. The Data Security Council of India (DSCI), as the Nodal Agency for the Ideation and Innovation Component, leads the overall coordination and management of the Challenge, supported by C-DAC Hyderabad and a network of 50 premier academic and autonomous institutions organized into 10 clusters, as leads and co-leads under ISEA project, the initiative encourages collaboration between academia, industry, and government.

Through its five-stage structure, CSIC 1.0 nurtures promising ideas from conception to Minimum Viable Product (MVP), strengthening India's cybersecurity innovation ecosystem.

The Challenge plays a pivotal role in building a robust cybersecurity innovation ecosystem by fostering a product building mindset from the early-stage ideas. It is specifically designed for student- and researcher-led innovators as well as student-led startups.

The inaugural Challenge focuses on 10 key clusters, including:

1. Computer & Network Security
2. Mobile Device Security (incl. malware analysis)
3. Systems & Software Security
4. Hardware Security
5. Security in Futuristic Technologies (AI/ML, AR/VR, etc.)
6. Cryptography
7. Security in distributed wireless networks (IoT/CPS, 5G, etc.)
8. Cyber Forensics
9. Governance, Operations & Services
10. Fintech Security (incl. Blockchain)

With its robust structure and focus on academic innovation, CSIC 1.0 aims to accelerate the time-to-market for cybersecurity innovations by bridging the gap between research and deployment.

Key highlights:

- **Exclusive Focus on Academic Innovation:** The Challenge is dedicated to nurturing cutting-edge solutions built primarily by the academic ecosystem (students and researchers). It aims to create a security product building mindset right from the early stages.
- **Seed Funding for Initial Development (Top 20):** A total of 20 teams are selected in the interim stage and each receives a ₹50,000 prize money to support the purchase of hardware, software, cloud credits, and other operational expenses for MVP development.
- **Dedicated Mentorship for Finalists**: The Top 20 Finalists receive expert-led webinars on technical topics, pitching, along with hands-on mentorship sessions from industry leaders.
- **Significant Total Prize Pool:** The Challenge offers total prizes of up to 40 Lakhs.
- **Targeting Critical Sector Solutions**: Solutions are focused on becoming sector-relevant and scalable, catering to critical Indian sectors like BFSI, telecom, healthcare and other critical sectors. Participants work on solving real-world cybersecurity problems.
- Rewarding Diversity and Unique Ideas: Special awards are included to recognize unique contributions like
  - ✓ Most Innovative Idea Award

- ✓ Women-in-Tech / Diversity Award.
- ✓ Jury’s Choice Award

Stages

The Cyber Security Innovation Challenge 1.0 features an innovative five-stage structure designed to guide innovators from the ideation phase to the development of a Minimum Viable Product (MVP). The stages include Ideation and Proposal Submission (all initial entries), Preliminary Evaluation and Shortlisting of Top 50 Ideas, Prototype Development and Evaluation (Top 50 teams leading to the Top 20 shortlisting), Mentorship, Capacity Building, and MVP Enhancement (for the Top 20 finalists), and finally, the Final Evaluation of Product and Winner Announcement, where the Top 3 winners are selected.

. Stage	Stage Description	Teams Remaining
Stage 1	Ideation and Proposal Submission	All Initial Entries
Stage 2	Preliminary Evaluation and Shortlisting of Top 50 Ideas	Top 50 Teams
Stage 3	Prototype Development and Evaluation	Top 20 Teams
Stage 4	Mentorship, Capacity Building, and Prototype Enhancement	Top 20 Teams
Stage 5	Final Evaluation of MVP and Winner Announcement	Top 3 Winners

Prize Money

Category	**Award**	**Amount** (INR Lakh)	**Amount** (INR Lakh)
Final Winners	1st Prize	10	22
	2nd Prize	7	
	3rd Prize	5	
Special Recognition	Most Innovative Idea Award	3	8
	Women-in-Tech / Diversity Award	3	
	Jury’s Choice Award	2	
Interim Support	Finalists (Top 20 Teams)	0.50	10
	Total		**40 Lakh**

Problem Statements for Cyber Security Innovation Challenge 1.0

Sr No	Cluster	Problem Statement	Description
1.	Computer & Network Security	Cloud Misconfiguration (Security Scanner)	Develop a tool to audit cloud infrastructure configurations and detect security misconfigurations across AWS, Azure, and GCP environments, enabling early identification of risky exposures.
2.	Mobile Device Security	Ransomware Early Warning System for Android Devices	Develop a behaviour-based detection framework to identify and block ransomware like activity on Android before major damage occurs.
3.	Systems & Software Security	DDoS Mitigation System	Develop a machine learning based DDoS mitigation system capable of distinguishing legitimate traffic spikes from malicious floods, providing adaptive and automated defences against hyper volumetric attacks.
4.	Hardware Security	HSM Tampering Detection System	Build a real-time monitoring system to detect, log, and respond to tampering attempts on Hardware Security Modules (HSMs), aligned with FIPS 1403 Level 3+ requirements.
5.	Security in Futuristic Technologies	Lightweight Post Quantum Messaging	Build efficient PQC-secure messaging for mobile & IoT, ensuring confidentiality and forward secrecy in the quantum era.

6.	**Cryptography**	Privacy Preserving KYC Verification System	Design a privacy preserving KYC verification system leveraging applied privacy-enhancing technologies (PETs), such as zero-knowledge proofs (ZKPs), that allows users to prove identity attributes (e.g., 'over 18', 'valid Aadhaar') without revealing sensitive personal identifiable information (PII).
7.	**Security in distributed wireless networks (IoT/CPS, 5G, etc.)**	Wireless Protocol Fuzzing	Develop an automated fuzzing tool to discover protocol level flaws in distributed wireless systems such as IoT, CPS, Wi-Fi, Zigbee, Bluetooth etc
8.	**Cyber Forensics**	AI-based Log Investigation Framework	Develop an AI powered system to ingest, parse, and analyze logs from diverse devices and applications, enabling rapid correlation, anomaly detection, and actionable forensic insights
9.	**Governance, Operations & Privacy**	Consent Management System	Build a transparent, user-friendly platform that enables individuals to track, grant, and revoke consent for data sharing, ensuring compliance with India's DPDP Act and global regulations (e.g., GDPR).
10.	**Fintech Security**	Mule Accounts & Collusive Fraud in UPI	Build a real-time fraud detection system using graph analytics, device fingerprinting, and risk scoring to identify mule accounts and collusive fraud rings in UPI and instant payments.