FIRST™
Improving Security Together

ANNUAL REPORT

Board Members

Audrey Mnisi Mireku
Carlos Alvarez
Carlos Leonardo
Graciela Martinez Giordano
Michael Hausding
Mona Elisabeth Østvang
Nadia Yousef
Olivier Caleff
Serge Droz
Tracy Bills
Yukako Uchida

2025

Dear Reader,

Welcome to the tenth Annual Report of the Forum of Incident Response and Security Teams (FIRST). As we reflect on 2025, we are proud to share the story of a year marked by significant growth, expanded impact, and a deepening commitment to our mission of fostering a safer internet.

Our global community thrived in 2025. Membership grew by 8%, reaching over 834 teams across 113 countries. We also introduced **Associate membership**, welcoming organizations — including non-profits — that share our goals but are not operational incident response teams.

FIRST's reach was unprecedented. We organized or co-organized **15 events** and delivered **over 40 training sessions** in 40 countries across all regions. Through the **FIRST CORE initiative**, we further expanded our Community & Capacity Building activities, supporting 41 additional training workshops in 29 countries, and representing an average of nearly one event or training per week throughout the year.

The cybersecurity landscape continued to evolve rapidly. International cyber conflict became the norm, with growing potential to escalate into the physical realm, while policymakers' understanding of our technical work often lagged behind. Our community-driven working groups - or Special Interest Groups (SIGs) - played a major role in addressing these challenges. The Public Policy, DNS Abuse, and Multi-Stakeholder Ransomware SIGs advanced critical discussions, while new SIGs emerged to tackle pressing issues, including:

- Time Security, raising awareness of the 2036–2038 epoch rollovers — the 'Epochalypse';
- Detection Engineering and Threat Hunting; and
- Cybersecurity Communications, recognizing the essential role of internal and external communications in incident response.

Several SIGs also published new standards or updated previous ones to support our community. Additionally, we addressed the growing impact of emerging technologies by publishing a Policy Brief on artificial intelligence, exploring its uncertain but potentially transformative effects on our work.

Our voice grew stronger in 2025. Media coverage nearly doubled year-over-year, with over 200 features in leading cybersecurity and mainstream outlets, as well as podcasts and TV interviews. Our social media channels also saw substantial growth, amplifying our message to a broader audience.

The year also brought important governance developments. Two new members joined the Board, and I assumed the role of Chair, reflecting our commitment to strong and adaptive leadership.

A highlight of 2025 was the induction of Richard (Rich) D. Pethia into the prestigious Incident Response Hall of Fame during FIRSTCON25. Rich's groundbreaking contributions, including founding the CERT® Coordination Center (CERT/CC) in 1988, have left an indelible mark on the field of cyber incident response.

The following pages detail these and other milestones from our tenth year. I encourage you to learn more about our 2025 activities and identify areas where you can contribute based on your expertise.

Thank you for your continued support.

Best regards.

Olivier Caleff
FIRST Chair, 2025-2026

Vision

FIRST aspires to bring together incident response and security teams from every country across the world to ensure a safe internet for all.

An effective response is a global task, mirroring the global nature of the internet. Based on a peer-to-peer network governance model, Computer Security Incident Response Teams (CSIRTs), Product Security Incident Response Teams (PSIRTs), Sharing and Analysis Centers (ISACs), and Security Operations Centers (SOCs) independent security researchers work together to limit the damage of security incidents. This response requires a high level of trust. FIRST fosters trust-building among members through a variety of activities. Incidents are not restricted to one cultural or political corner of the internet, nor do they respect borders or boundaries. FIRST thus promotes inclusiveness, inviting membership from all geographic and cultural regions.

FIRST Mission

1 **Global Coordination - You can always find the team and information you need.**

FIRST provides platforms, means, and tools for incident responders to always find the right partner and to collaborate efficiently. This implies that FIRST's reach is global. We aspire to have members from every country and culture.

2 **Global Language - Incident responders around the world speak the same language and understand each other's intents and methods.**

During an incident, it is important that people have a common understanding and enough maturity to react in a fast and efficient manner. FIRST supports teams through training opportunities to grow and mature. FIRST also supports initiatives to develop common means of data transfer to enable machine-to-machine communication.

3 **Policy and Governance - Make sure others understand what we do and enable us rather than limit us.**

FIRST members do not work in isolation but are part of a larger system. FIRST engages with relevant stakeholders in technical and non-technical communities to ensure teams can work in an environment conducive to their goals.

Security teams need to collaborate - especially during a crisis. FIRST, as a community, works tirelessly to build an inclusive and high-trust environment between our members before such a crisis.

Our vision statement is a challenging target - but we have a plan of action to bring this to reality.

Strategy and Governance

In 2025, the FIRST Board of Directors launched the organization's first Strategy Framework, a foundational step in the ongoing transition from a volunteer-driven association to a structured, strategically focused entity. Central to this work was the finalization and publication of the FIRST Strategic Plan 2025-2028, a three-year roadmap organized around five strategic objectives and ten strategic areas, dedicated to strengthening member value, expanding global reach, and ensuring long-term financial sustainability.

To support this commitment to transparency with the membership, the Board established a dedicated Strategic Planning section on the FIRST website, providing a centralized location where members can access the strategic framework and, in time, related plans and progress reports. The Strategic Plan sets the direction for FIRST's work through 2028. The translation of this direction into activities, timelines, responsibilities, and measurable indicators is the focus of the operational planning work that follows the plan, led by the Executive Director.

Throughout 2025, the Board engaged in internal discussions, in collaboration with the Rules Committee, on aspects of FIRST's governance model. These conversations considered Board composition, term lengths, and election procedures, and reflected the Board's broader effort to align its structure with the needs of an evolving, global cybersecurity organization. The outcomes of this work formed the basis of the proposed bylaw amendments brought to the membership at the June 2026 Annual General Meeting.

Incident Response Hall of Fame

In 2025, FIRST announced the induction of Richard (Rich) D. Pethia into its prestigious Incident Response Hall of Fame during FIRSTCON25. Pethia was recognized for his foundational contributions to the field of cyber incident response – most notably, creating the world's first Computer Emergency Response Team (CERT/CC) and helping ignite a global movement to build resilience through coordinated response.

As the founding director of the CERT® Coordination Center (CERT/CC), now part of the CERT Division of the Carnegie Mellon University Software Engineering Institute (CMU SEI), Pethia's vision and leadership helped shape the modern practice of cybersecurity incident response. Under his tenure, CERT evolved from a single response team into a world-renowned hub for technical research, workforce development, and global capacity building.

"Rich's vision is woven into the DNA of FIRST," said Chris Gibson, CEO of FIRST. "His belief in collaboration, transparency, and capacity building helped turn a technical response team into a global movement. The network of CSIRTs we see today is a direct result of the path he carved."

CERT/CC was among the founding members of FIRST in 1990 and hosted the organization's earliest meetings. Pethia was one of the authors of the original FIRST Operational Framework and was elected by the founding members to be the organization's Steering Committee Chair. Under Pethia's direction, the team created the first training courses and the widely adopted Handbook for CSIRTs, laying the groundwork for how incident response is practiced today. CERT/CC played a vital role in establishing teams around the world, including US-CERT (now part of DHS CISA), AusCERT, JPCERT/CC, and many others.

Beyond incident response, Pethia expanded CERT/CC's work into areas such as malware analysis, insider threat, risk and resilience management, and vulnerability research. His influence helped embed core principles into the FIRST CSIRT Services Framework, a lasting contribution that continues to guide teams globally.

"Countless people and organizations, including myself, have benefited from Rich Pethia's leadership, technical acumen, and strategic vision," said Brigadier General (Ret.) Greg Touhill, current CERT Division Director and former U.S. Federal CISO. "He did not just create the world's first CERT, he arguably launched the entire cyber incident response discipline. Few people have had such a profound positive effect on making the world a safer place."

Pethia joins a distinguished group of Hall of Fame inductees including Cristine Hoepers, Andrew Cormack, Jeffrey Carpenter, Dan Kaminsky, Ian Cook, Don Stikvoort, and Klaus-Peter Kossakowski.

"I am deeply honored to be recognized by FIRST and included among so many respected incident response leaders," said Pethia. "Creating the CERT Coordination Center was never about building a single team, it was about sparking a global community. Seeing how far that community has come is the greatest reward of all."

Strategy and Policy

Cyber operations have become an integral part of statecraft, dominating espionage and playing an essential role in modern warfare. Furthermore, cybercrime now leads global crime statistics. FIRST and its members remain at the forefront of these developments. Incident responders play a crucial role in preventing spillover and excessive collateral damage from breaches, and through its Special Interest Groups (SIGs)—such as the DNS Abuse SIG and the MSR SIG—FIRST helps security professionals stay ahead of the curve.

This vital role is increasingly recognized by states: most UN members now perceive FIRST as a global, neutral organization that provides the platform necessary for incident responders to connect to effectively mitigate breaches. However, many policymakers still lack a comprehensive understanding of our technical work. To bridge this gap, members of the Public Policy SIG continue to engage with decision-makers, demonstrating the value of our work and providing the technical nuance required for meaningful dialogue.

Cyber conflict has become the norm. While these conflicts rarely cross the threshold of armed attack, they possess significant potential to escalate, potentially spilling over into the physical realm. FIRST is collaborating with partners such as the HD Centre to ensure cyber topics are integrated into relevant strategic discussions.

Amidst these developments, artificial intelligence threatens to significantly impact our work, though its precise effects remain uncertain. The Public Policy SIG has published a Policy Brief addressing these challenges (**https://www.first.org/global/sigs/policy/library/Policy-Brief-on-AI**).

Financials

The 2025 activity report shows total revenues of $7,778,679 and total expenses of $7,054,425 resulting in a change of net assets of $724,254.

Event attendance and sponsorship are contributing factors to FIRST's surplus. Membership continues to grow, and revenue diversification through grants and the FIRST CORE program have supported community and capacity building efforts.

FIRST engaged an external auditor who found no issues. More detailed information on FIRST finance is available on our **public Website**.

Training & Education

As an international organization with plenty of cybersecurity experts, it is also crucial for FIRST to continue sharing its technical expertise both within and outside the community. Training is a significant opportunity for such knowledge sharing and also Community and Capacity Building (CCB), which is also an important mission for FIRST. FIRST delivers training at its own events including the Annual Conference, Regional Symposia and TCs. In achieving this goal, FIRST endeavors to develop training opportunities in wider regions and ensure to align the training program with the events lineup.

In 2025, FIRST has organised training in the following FIRST events (including programs under CCB):

- FIRST Regional Symposium Europe
- Balkan Cybersecurity Days
- FIRST VulnCon
- FIRST CTI Conference
- FIRST-AfricaCERT Regional Symposium
- Annual FIRST Conference

In 2025, outside of FIRST events, our community trainers and CCB supported 41 training workshops in 29 countries and more remotely. This includes The Bahamas, Bahrain, Benin, Brazil, Cameroon, China, Costa Rica, Dominican Republic, The Gambia, Ghana, Kenya, Lesotho, Malawi, Mauritius, Mongolia, Montenegro, Morocco, Mozambique, Nigeria, Oman, Poland, Republic of the Congo, Sierra Leone, South Africa, Spain, Switzerland, Trinidad and Tobago, United Arab Emirates, and the United States.

ITU Regional Cyber Drill - Nassau, BS (January 2025)

Many of these events were organized in collaboration with partner organizations including the following:

- ASEAN-Japan Cybersecurity Capacity Building Center (AJCCBC)
- OAS-INCIBE Cybersecurity Bootcamp
- ICT4Peace
- International Telecommunication Union (ITU) Regional Cyber Drills
- ITU Arab Regional Cybersecurity Centre (ITU-ARCC)
- Latin America and Caribbean Cyber Competence Centre (LAC4)
- Middle Eastern Cyber Diplomacy Initiative (MECDI)
- The Organization for Security and Co-operation in Europe (OSCE)

FIRST training program has been supported by volunteer contribution by FIRST training community. Any individual who is interested in delivering the training or developing the training materials are welcome to join the FIRST training community.

In addition, FIRST is always open for any request to invite FIRST trainers to events organised by partners. If you wish to plan a training session by FIRST trainers, please refer to our **Training webpage** for further details and contact the training team.

Community & Capacity Building

Community and Capacity Building (CCB) activities help FIRST realize our vision and mission. Since the establishment of FIRST, the community has engaged in a wide range of both formal and informal capacity building activities. These have included organized initiatives such as training, advice and mentorship, the Suguru Yamaguchi Fellowship Program, the sharing and development of standards and good practices, and indirectly through platforms, forums, networking, and events.

A selection of the initiatives delivered through CCB in 2025 include:

FIRST CORE

In 2025, FIRST launched the FIRST CORE, a program designed to rally resources to expand the breadth and impact of CCB activities. FIRST CORE officially kicked off with our Launch Partner and Founding CORE Supporter, Fortinet, at the June 2025 FIRST Annual Conference in Copenhagen, Denmark.

Through CORE, FIRST worked across several workstreams in 2025, including support for:

- Incident Response TTX for the Women in International Security and Cyberspace Fellowship (WiC) with Women of FIRST (WoF) SIG at the UN Open-Ended Working Group (OEWG) (July 2025)
- Actioning Alerts and Advisories (A4) with CTIR Government Brazil (Dec 2025)
- Africa Community engagement including the AfricaCERT-FIRST Remote Cyber Drill (Oct 2025) and support for fellows at ThreatCON in South Africa (Nov 2025) and the Africa Regional Symposium (Dec 2025)
- Mobile Training Lab Pilot with FIRST community trainers (ongoing)
- The FIRST CORE track at the Annual Conference (June 2025)
- Back-of-house support to enable all FIRST CCB and training activities

Africa Regional Liaison Threat Intelligence Workshop - Accra, GH (October 2025)

Africa Regional Liaison (ARL) Initiative

The FIRST Regional Liaisons are essentially active network builders and hubs. The Liaisons have a dual role of training and increasing capacity in a region while also bringing people together to create working, long term networks where collaboration can continue to grow well beyond the ARL initiative.

The Africa Regional Liaison (ARL) Initiative was launched in November 2023 and was made possible through the generous support of UK International Development as part of the Africa Cyber Programme.

In 2025, the ARL team worked in: Benin, Cameroon, Djibouti, The Gambia, Ghana, Kenya, Lesotho, Liberia, Malawi, Mali, Mauritania, Mauritius, Mozambique, Nigeria, Sierra Leone, South Africa, and Tanzania.

Actioning Alerts and Advisories (A4)

The basis of A4 is about increasing the impact of threat intelligence by ensuring national CSIRTs are able to access it, process it, and communicate it across all sorts of stakeholder audiences. And most importantly, making it more likely the stakeholders will do something with that information.

FIRST technical and communications SMEs worked side-by-side with teams to understand the work of each team, provide informal mentorship and advisory support for team initiatives, and, at the discretion and guidance of the local partner, meet with key stakeholders, and deliver a community training workshop with selected participants

Launched in October 2024, in 2025 the A4 team worked with the national CSIRTs of The Bahamas, Trinidad and Tobago, Malawi, and Cameroon through the support of the UK Government and with CTIR Brazil supported by FIRST CORE.

Actioning Alerts and Advisories (A4) working with TT-CSIRT - Port of Spain, TT (March 2025)

Western Balkans Capacity Building

The Geneva Centre for Security Sector Governance (DCAF) launched the Enhancing Cybersecurity Governance in the Western Balkans program in 2018. The program brings together private and public CSIRTs to build cyber diplomacy capacity in the region.

FIRST has been collaborating with DCAF since 2022 and together we have been organizing the annual Balkan Cyber Security Days. The 2025 event was hosted in Podgorica, Montenegro from 18 to 20 March and brought together the public and private sectors to discuss policy and technical issues, followed by two days of training.

FIRST co-hosted the Regional Workshop for Young Women in Cybersecurity in November with DCAF, the Western Balkans Cyber Capacity Centre (WB3C), UK FCDO, and the British Council. The two-day workshop in Podgorica brought together 70 participants that featured hands-on practice in CTF drills organized by FIRST.

FIRST also expanded its partnerships in the region, signing an MoU with the e-Governance Academy (eGA) to lay the groundwork for further collaboration. FIRST worked with eGA to support their fellowship program that helped bring incident responders from Western Balkan national CSIRTs to the FIRST Annual Conference in Copenhagen.

Supporting NGOs and Civil Society

FIRST worked with ICT4Peace to deliver a Cybersecurity Capacity Building Workshop for Geneva-based International Organizations and Non-Government Organizations during the inaugural Geneva Cyber Week 2025 in May.

This workshop was the second in a series, focussing on practical implementation of key security practice. It parallels the CCB team's collaborations with NGOs and civil society, through the Non-Profit Cyber network and Common Good Cyber initiative.

Regional Workshop for Young Women in Cybersecurity - Podgorica, ME (November 2025)

ASEAN-Japan Cybersecurity Capacity Building Centre

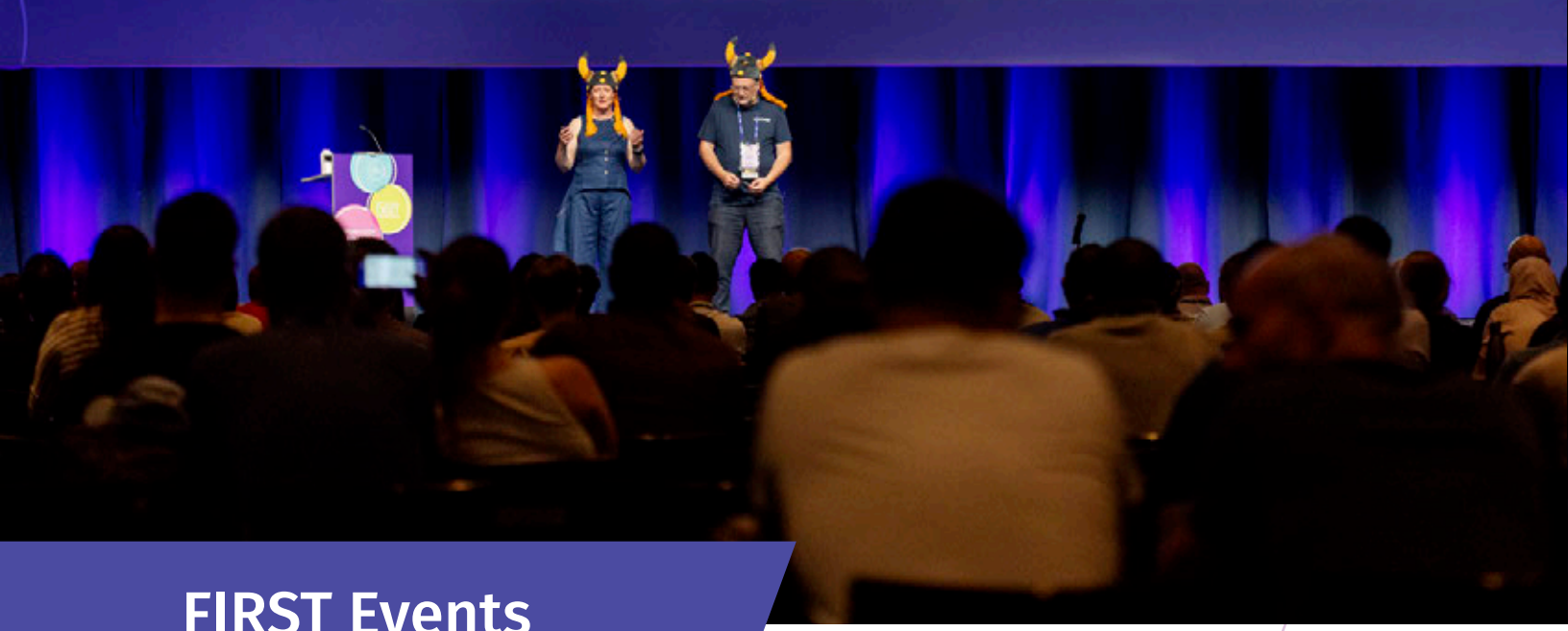
This workshop series is a collaboration between FIRST and the ASEAN-Japan Cybersecurity Capacity Building Centre (AJCCBC) located in Bangkok, Thailand.

In 2025, we supported a remote Capture-the-Flag (CTF) competition for women students and young cybersecurity enthusiasts from ASEAN member states. It was created to encourage women's engagement in cybersecurity and support the formation of a "Team ASEAN" for the International Cybersecurity Challenge (ICC).

The CTF was designed and delivered by trainers from the FIRST SecLounge SIG and delivered in July 2025 for 499 participants from Brunei, Cambodia, Indonesia, Laos, Malaysia, Myanmar, Philippines, Singapore, Thailand, and Vietnam.

The 2025 AJCCBC collaboration was made possible with the support of the Swiss Confederation.

More information on the FIRST Community and Capacity Building program and our 2025 activities can be found at: **first.org/community**



FIRST Events

FIRST events are organized worldwide throughout the year. In 2025, FIRST hosted, co-hosted, and supported 15 events. These activities depend significantly on the strong collaboration among organizational partners and member teams.

As always, the Annual Conference in June remains FIRST's most attended event. The 37th Annual Conference in Copenhagen, Denmark, saw participation from 1,056 delegates from 103 economies. Special thanks to our 2025 local host, Danish Defense Intelligence Service (DDIS), who provided our delegation with a warm welcome and a wonderful week. Our heartfelt thanks go to the 2025 Program Chair, Henrik Larsen, and the 2025 Program Committee for their hard work and dedication. We would also like to recognize our session chairs for volunteering their time to guide us through the week's agenda.

For FIRST, events are essential. They serve as a vehicle, bringing our members and community together to work toward our organizational objectives.

Conferences (3)

Annual Conference | June 22-27, 2025

- www.first.org/conference/2025
- Copenhagen, Denmark
- Local Host: Danish Defense Intelligence Service (DDIS)
- 1,056 in-person delegates
- 103 economies

Cyber Threat Intelligence Conference (hybrid) | April 21-23, 2025

- www.first.org/conference/firstcti25
- Berlin, Germany
- 347 in-person delegates
- 46 economies

Vulnerability Management Ecosystem Collaboration, Ideation, and Action Conference (aka "VulnCon") (hybrid) | April 7-10, 2025

- **www.first.org/conference/vulncon2025**
- Raleigh (NC), United States of America
- Co-Host: CVE Program
- 448 in-person delegates
- 31 economies

Regional Symposia (3)

Regional Symposium – Africa and Arab Regions | December 2-5, 2025

- **www.first.org/events/symposium/africa-arab-regions2025**
- Ebene, Mauritius
- Co-Hosts: AfricaCERT, CERT-MU

Regional Symposium - Latin America & Caribbean | October 8-9, 2025

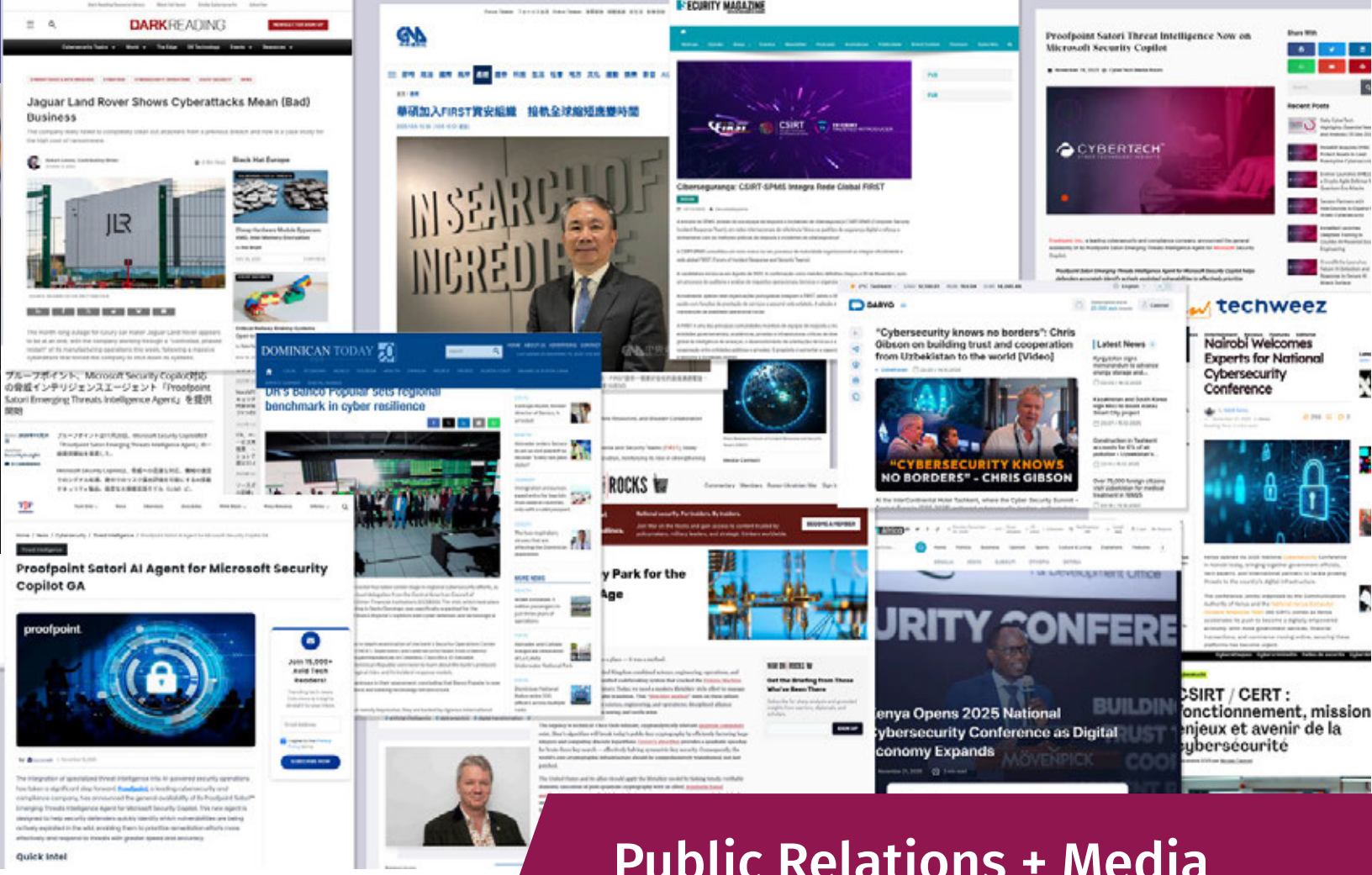
- **www.first.org/events/symposium/latam2025**
- San Salvador, El Salvador
- Hosts: LACNIC, LACNOG, CERT.br/NIC.br
- 70 delegates
- 20 economies

Regional Symposium – Europe | January 14-16, 2025

- **www.first.org/events/symposium/monaco2025**
- Monte Carlo, Monaco
- Co-Host: CERT-MC
- 233 delegates
- 44 economies

FIRST Technical Colloquium (9)

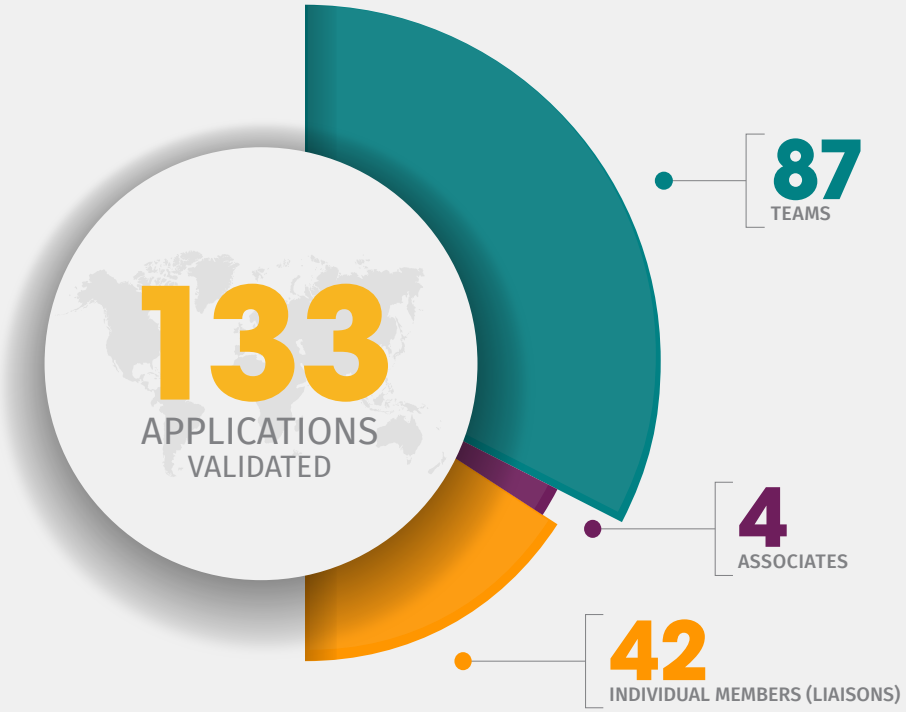
- Ljubljana TC in Ljubljana, SI | December 9-10, 2025
- Annual Cybersecurity Conference and TC in Nairobi, KE | November 21, 2025
- UNDP TC, Virtual | October 30, 2025
- Mexico City TC in Mexico City, MX | October 27-29, 2025
- Cold Incident Response TC in Oslo, NO | October 7-9, 2025
- Vulnerability Forecasting (Vuln4Cast) TC in Cambridge, GB | September 25-26, 2025
- APNIC TC in Da Nang, VN | September 9-11, 2025
- Amsterdam TC in Amsterdam, NL | March 25-27, 2025
- Balkan Cybersecurity Days in Podgorica, ME | March 18-20, 2025



Public Relations + Media

In 2025, FIRST secured and tracked 215 pieces of earned media coverage, a roughly 172% year-over-year increase compared to 2024. Coverage appeared in leading cybersecurity and mainstream outlets including Dark Reading, CSO, Cyberscoop, SC Media, TechTarget, and Infosecurity Magazine. This growth was fueled by campaigns tied to major research (the Vulnerability Forecast, EPSS v4), flagship events (VulnCon25, FIRSTCTI25, FIRSTCON25), and milestone news, including FIRST surpassing 820 member teams across 110+ countries, while international outreach expanded FIRST's footprint into French, German, Japanese, Spanish, and Danish media.

Social channels grew substantially as well. LinkedIn added roughly 3,372 new followers across the year, a nearly 27% increase over FIRST's 2024 base of 12,291, pushing the community well past 15,000. YouTube gained over 750 new subscribers, growing from a 2024 base of 4,220, while X added roughly 190 followers on top of an already substantial base of over 13,000. Newer platforms Bluesky and Mastodon also gained early traction, adding 316 and 141 followers respectively. The year's standout content included the Detection Engineering and Threat Hunting SIG launch, the FIRSTCON25 recap video, and the "Improving Security Across Nations with FIRST" video series, which completed its nine episode first season and repeatedly drove some of FIRST's highest engagement of the year.



JAN - DEC **2025**

834
TEAMS

205
INDIVIDUAL MEMBERS (LIAISONS)

115
COUNTRIES

Membership

Membership in FIRST enables computer and product security incident response and security teams that work together voluntarily to deal with computer security problems and their prevention.

There are three types of members:

- Full members represent organizations who assist an information technology community or other defined constituency in preventing and handling computer security-related incidents and product focused teams.
- Liaison (individual) members are individuals or representatives of organizations other than incident response or security teams with a legitimate interest in and value in FIRST.
- Associate membership was introduced in 2025 for organizations that are not operational incident response teams but who have a valid interest in participating in the FIRST community, including non-profit organizations.

Applications received by the FIRST Secretariat are reviewed by the Membership Committee and sent to the FIRST Community for comment. If the applications have not been opposed in the process, the Board of Directors vote to approve the applying Teams or Liaisons to join the FIRST community.

Between January 1 and December 31, 2025 133 new applications were accepted - 87 new teams, 4 associates and 42 individual members (liaisons). Over the same period, some FIRST members left for various reasons - lack of dues payment, mergers, change in activities.

Overall, membership to FIRST continues to grow and amount to 834 Teams, 4 Associates and 205 Individual members with a coverage of 115 countries as of the end of 2025.

FIRST Partners and Collaboration

The internet is a global infrastructure comprised of many different components that must work together for the whole to function. While incident response is often a last resort, Chris Inglis emphasized the critical role of first responders in his 2026 keynote. We do not operate in isolation; we are all embedded in larger organizations with diverse goals and areas of expertise. FIRST's motto, "Improving Security Together," applies not only within our own community but also outwardly. Rather than attempting to develop capacity in every relevant field, FIRST partners with leading organizations that share our goal of making the internet a safer place for users.

As a global organization with members in 115 countries, FIRST sometimes faces challenges in understanding regional nuances. To address this, we work closely with regional organizations such as OIC-CERT, the Open CSIRT Foundation, and APNIC. Collaborations vary in scope: sometimes we simply cross-post to our respective communities, while other times we partner more closely, such as through joint events. The Board strives to participate in these events and aligns some of its in-person meetings with regional gatherings. While some collaborations proceed smoothly with a mutual understanding of shared goals, others are more challenging or nascent. Consequently, the Board has decided to focus on active collaboration and will only sign Memorandums of Understanding (MoUs) where a strong foundation already exists.

However, not everything can be planned. Often, the most fruitful collaborations happen spontaneously and may only occur once or twice. A prime example was the Capture the Flag (CTF) event for women in cyber, conducted in collaboration with our long-standing partner DCAF but initiated by the British Council. The event was a great success, receiving outstanding feedback from participants. While a second edition is not yet planned, it serves as a reminder that we must seize opportunities when the stars align. This is particularly important in today's world, where cross-border collaboration is increasingly complex.

Ultimately, this is a call to invest in collaboration and joint efforts, even when they present challenges.

Partners and MoUs

Special Interest Groups

FIRST Special Interest Groups (SIGS) are member-led initiatives based on community support. A FIRST member can propose a new SIG to explore an area of interest or specific technology area with a goal of collaborating and sharing expertise and experiences to address common challenges. The new SIGs approved in 2025 were:

Cybersecurity Communications SIG - Communications, both internal and external, is an essential piece of incident response, awareness, and readiness. The Communications SIG is a communications-focussed group from around the world to share ideas and achievements. Short term goals include:

- standardised terminology;
- standardised translations from English; and,
- a database of acronyms, initialisms and technical terms

Longer term goals include:

- networks for sending international alerts;
- contact list in different business sectors;
- a shared resource library (similar to A4 project).

Detection Engineering and Threat Hunting SIG - Security teams are constantly facing evolving threats, complex infrastructures, and an expanding set of detection tools. Many SOCs and CERTs are building Detection Engineering capabilities, but without a strong peer network, they often work in isolation, reinventing solutions to shared challenges. Similarly, Threat Hunting efforts uncover new attack techniques, but without structured collaboration, insights can be siloed rather than feeding back into detection improvements. The SIG seeks to enhance Incident Response effectiveness by strengthening the upstream disciplines of Threat Hunting and Detection Engineering and create a global knowledge-sharing space that fosters:

- Collaboration on detection R&D, enabling teams to develop and refine detection rules more efficiently.
- Knowledge exchange on tools, infrastructure, and threat specifics, helping teams navigate emerging challenges.
- Structuring of best practices, definitions, architectures, and methodologies to standardize and accelerate progress.
- Creation of a shared repository of detection content, supporting scalable and effective detection coverage.
- Continuous feedback loops between Threat Hunting, Detection Engineering, Threat Intel, and Incident Response, transforming unknown threats into known detections while tuning false positives through automation and investigation insights.

Time Security SIG - this SIG raises awareness of the 2036–2038 epoch rollovers (the 'Epochalypse') and promotes resilience in time synchronization across critical systems.
By coordinating research, testing, and outreach on time integrity, the SIG connects CSIRTs,vendors, and standards bodies to strengthen resilience across critical infrastructure. The goal is to ensure the world's clocks keep running securely long past 2038 by:

- Identifying where critical systems rely on fragile timekeeping
- Communicating the risks posed by upcoming epoch rollovers
- Equipping FIRST teams with practical guidance for time integrity: authenticated sources, resilient architectures, and verifiable controls.

The Time Security SIG aims to:

- Enable FIRST teams to assess 2036–2038 rollover risks in their infrastructure
- Create a knowledge base for sharing sector-specific vulnerabilities and mitigation strategies
- Establish coordination channels among CSIRTs, vendors, and standards bodies
- Reduce time-to-remediation through shared intelligence and validated mitigation patterns

Standards SIG - the Standards Committee transitioned to a SIG and focuses on effective, interoperable, and widely adopted standards are essential to FIRST's mission. articularly to our pillar of Global Language: ensuring that incident responders worldwide speak the same operational language and understand each other's intent, methods, and expectations. As the systems underpinning our digital world become increasingly diffuse, interdependent, and cross-border in nature, the need for coherent standards grows sharper. Strong, reality-based standards directly increase public safety by improving the speed, clarity, and coordination of international incident response. They also raise the overall professionalization of the cybersecurity field.TheFIRST Standards SIG brings together practitioners from around the world with deep experience in standards development, each able to bridge between the FIRST community and external standards development bodies. The SIG provides:

- A single, authoritative point of contact for external SDOs seeking operational insight and reality checks.
- A mechanism to prevent the cybersecurity community from being bound to ineffective, conflicting, outdated, or non-viable standards.
- A resource for FIRST SIGs to improve the quality, visibility, and adoption of their own standards work

FIRST recognizes and thanks all SIG chairs and participants for their ongoing effort and support on behalf of the community.

Infrastructure

In 2025 the FIRST infrastructure team focused on implementing improvements to solidify and secure core services and operations to better support members, volunteers and the board, the operations team, and the security community. This includes:

- Completion of the migration of FIRST services to AWS:
  - This crucial project involved relocating all FIRST services to Amazon Web Services (AWS). By leveraging the scalability, reliability, and flexibility of AWS, FIRST aimed to improve the overall performance, security, and efficiency of its services.
- Portal Enhancements
  - Improved Liaison and Team privacy controls: To better safeguard sensitive information and maintain confidentiality, the team implemented enhanced privacy controls and permissions systems within FIRST portal.
  - Group management enhancements: As part of this initiative, the team developed new features for managing groups, teams, and collaborations within the FIRST community.
- DDoS Protection
  - The team implemented protection measures to safeguard against DDoS threats. By leveraging this solution, FIRST aimed to mitigate potential disruptions and ensure continuity of critical services.
- Support Platform Migration
  - This project aimed to provide an intuitive platform to better support the needs of members, volunteers, and staff.
- NatCSIRT directory and tools
  - Through this initiative the team provided enhanced functionality that would better allow for administration and management of NatCSIRTs.

www.first.org
support.first.org

Forum of Incident Response and Security Teams, Inc

2500 Regency Parkway, Cary, North Carolina, 27518
United States of America