Jan - Mar 2023

FIRST POST

Bringing together Security and Incident Response teams from around the globe.

Upcoming Events - Bilbao, Kigali, Amsterdam

Bilbao
Jan 31 - Feb 2

Kigali
Feb 28 to Mar 3

Amsterdam
April 17-19

TF-CSIRT Meeting & 2023 FIRST Regional Symposium Europe

The TF-CSIRT Meeting & 2023 FIRST Regional Symposium Europe will be held January 31 - February 2, 2023, in Bilbao, Spain at the Basque Cybersecurity Centre. The Symposia will feature meetings, presentations, and a full day of hands-on training. It will be of high interest to members and non-members throughout Europe. The networking reception at the exceptional Guggenheim Museum on the first evening is not to be missed.

Guggenheim Museum, Bilbao

TF-CSIRT meetings will take place on day one along with presentations comprising of 'UEBA Prevention Framework for Enterprise Security', 'TLP and PAP: Just the Two of Us and The Recent Evolutions of CSIRTs Cooperation in France' and 'MALMALWINA - Malware in a Box - the Road from a Set of Malware Analysis Tools to an Automated Malware Data Lake Supporting CERT/CSIRT Operations'.

Other interesting discussions and presentations include 'Tracking Attackers in Open Source Supply Chain Attacks: The New Frontier,' 'Breaking the Ransomware Tool Set – When a Threat Actor Opsec Failure Became a Threat Intel Goldmine', and 'Cyberwar – Lessons Learned from Russia's War in Ukraine'.

Leading security experts will conduct small workgroup training on day three, which participants can sign up for in advance when registering. There will be 16 training sessions covering a range of topics made up of 'DNS: Prevention, Detection, Disruption, 'Defense' and a 'CSIRT Manager's Course – CSIRT KPIs, CSIRT Annual Report Writing, CSIRT Mandate Clarification, CSIRT Manager Time Allocation'.

Sigita Jurkynaite, TF-CSIRT Steering Committee member, said: "The joint FIRST and TF-CSIRT meeting creates a unique opportunity for the communities to gather together and exchange ideas, success (and failure) stories in a trusted environment. We are especially looking forward to the meeting in Bilbao because this is the first joint in-person meeting after the pandemic years. It will be great to see familiar faces but also meet many new people who joined the community in the meantime, whom we have not yet had a chance to see face-to-face. Collaboration is key in our work area, and this event is about that - on a personal and organizational level."

Open to members and non-members, the complete program, including speakers, can be found **here**.

Note that some meetings are by invitation only.

Registration for the upcoming symposium is now **open**.

2023 FIRST & AfricaCERT Symposium: Africa and Arab Regions

Taking place in Rwanda, the 2023 inaugural FIRST & AfricaCERT Symposium for the African and Arab Regions will be held at the Marriott Hotel in Kigali, from February 28 to March 3, 2023. Co-hosted by AfricaCERT and the National Cyber Security Authority (NCSA) of Rwanda, this is our inaugural event in the country.

The first two days of the symposium will comprise training, day three will be a plenary session, and there will be a closed event for AfricaCERT on the final day. You can find the program **here**.

FIRST Member Teams and CSIRTs from the African and Arab regions, network operators, anti-abuse teams, and other security professionals will find this event advantageous.

The event will be in a hybrid format, with in-person and virtual admission available. Experts will present sessions in English with French translation services available.

Date for your Diaries - Amsterdam 2023 FIRST Technical Colloquium, April 17-19

The FIRST Technical Colloquia & Symposia in Amsterdam this April will provide a discussion forum for FIRST member teams and guests. Hosted by HumanSecurity and LinkedIn, the discourse will cover vulnerabilities, incidents, tools, and other issues that affect the operation of incident response and security teams.

Keep an eye on the **website** for updates, call for speakers, and registration.

Don't forget that the biggest FIRST event of 2023, the Annual Conference, will be held in Montreal, Canada, in June. Registration is now available on the conference website.

Chair Sherif Hashem and Board Member Michael Hausding participate in the FIRST & ITU-ARCC Regional Symposium for Africa and Arab Regions

Sherif Hashem and Michael Hausding participated in the joint **Regional Symposium for the Arab Region and Islamic countries** in Muscat-Oman, November 8-9 2022 hosted by the ITU-ARCC and organized jointly with the OIC-CERT within the Omani Regional Cybersecurity Week. Over 600 professionals from over 45 countries attended this popular event.

Sherif gave an opening keynote speech, and Sherif and Michael participated in two panel discussions on behalf of FIRST and our industry. The panel discussions covered 'Cybersecurity Innovation Ecosystem Government, Academia & Industry' and 'Evolution of Cyber Security Response Against Emerging Threats'. They conveyed a global partnership message, highlighting FIRST's efforts to support networking and cooperation among incident response and security teams.

Several participating teams from the Arab region and Islamic countries expressed interest in joining FIRST.

Chair Sherif Hashem also participated in the informal, inter-sessional meetings of the United Nations Open-ended Working Group (UN OEWG) on security of and in the use of information and communications technologies, held at the UN Headquarters in New York from Dec 5-9, 2022. Sherif gave three interventions during the meetings. He emphasized the role of FIRST as the leading organization that brings together over 5,500 professionals from 663 incident response and security teams in 102 countries. He highlighted that FIRST champions capacity building and knowledge exchange among incident responders, and produces cybersecurity standards such as CVSS and TLP. FIRST also organizes numerous conferences, symposia, technical colloquia, in addition to cyber drills and table-top exercises, across the world bringing together thousands of professionals, to further knowledge exchange, capacity building and cooperation at the global and regional levels.

Finally Sherif asserted that FIRST and its members are eager to continue sharing our experiences with the UN OEWG community; contributing towards the implementation of the UN Program of Action. He affirmed that FIRST is uniquely positioned to maintain a Global Technical Directory of Points of Contact (PoC) of incident responders and security teams based on its existing outreach and membership, and with a multi-stakeholders, inclusive and open approach.

Other Policy & Governance Activities

In addition, FIRST board member Olivier Caleff represented our community in person at the **Paris Peace Forum** on a round-table about **ransomware**, and Serge Droz contributed papers about sanctions and their limitations to the UN Open-ended Working Group on security of and in the use of information and communications technologies.

First 100 days on the FIRST board

Board Member Audrey Mnisi Mireku *- CISRO, Ghana Association of Banks*

We asked Audrey Minisi Mireku about her experience as a new board member at FIRST.

1. Tell us a little about yourself - how long have you worked in incident response?

I have been working in incident response for several years - currently, I am the Chief Information Security Risk Officer at the Ghana Association of Banks (GAB). I lead and coordinate engagements on Information security, compliance, fraud prevention, and information sharing in the banking sector. My engagements include member banks, industry regulators, the media, law enforcement, and policymakers. In 2019, I led the National CERT of Ghana to join FIRST.

2. What experience did you have with FIRST before you joined?

I heard about FIRST for the first time in 2015 during the Africa Symposium in partnership with FIRST, Africa CERT, and Ghana's Ministry of Communications through the National Communications Authority, which led to the set-up of the first CERT in the Telecommunications sector.

In 2019, the SEI / CERT CC Team painted a different picture of FIRST as the premier organization and force to reckon with; as recognized global leader in incident response that brings teams such as ours together across the world to foster cooperation and coordination in incident prevention; stimulate rapid reaction to incidents; and to promote information sharing among members and the community at large through trust. Seeing how important FIRST was, I listed joining FIRST as one of my goals, and I achieved this objective in 2021.

3. What made you want to be a board member? What was your journey?

I was interested after getting to know more about FIRST, what it stands for, what it seeks to achieve, and the threat landscape and gaps, taking into consideration the massive investment that African governments are making in digitalization.

Based on the above, I took up the challenge of applying for Board Membership. I reached out to everyone I knew with links to FIRST, to get more understanding of board responsibilities, time commitment, term length, and committee expectations, among others. During the process, I identified the gaps that needed addressing such as influencing policy direction; and improving the efficiency and effectiveness of Africa's incident response teams through capacity building, training, and outreach; whilst pushing the mission of FIRST towards bringing together incident response and security teams from countries across the world to ensure a safe internet environment for all.

4.What responsibilities do you have over the next year or two? What are you looking forward to contributing?

I have volunteered to lead engagements with teams in African and Arab regions. In my first year, I am engaging teams in the fellowship program; those that have just been given the authority or mandate to establish National CERT; and to engage with existing FIRST members. During these engagements, the teams' needs are assessed; and recommendations are proffered. Based on these recommendations, teams are linked to application sponsors; this would directly influence the planned program of activities for 2023/2024. I have received tremendous support from my fellow board members and FIRST full-time staff. The teams appreciate the engagements very much and are excited to have direct access to FIRST. It is my fervent belief that this would fast-track the teams on the fellowship program to complete the application process.

I intend to ensure FIRST establishes a vibrant presence in Africa through collaborations and membership. I am looking forward to building a robust, but fluid incident response ecosystem in Africa; which would make use of the opportunities in FIRST to share experience; and learn from other teams.

5.How many events have you participated in - online and virtual? Please tell us a little about your experience of these events. Any highlights?

One of my highlights dates back to 2015, during the Africa Symposium in Accra; back then, web defacement attacks were a menace to both government and private sector websites. A two-day training was organized, but I couldn't join the training session due to the limited number of seats and high demand for the training. However, my colleagues who did organized sessions and we all benefited from the knowledge they gained from the original training. Insights from the training led to the introduction of OWASP Ghana Chapter, which still remains a very vibrant group.

Audrey Mnisi Mireku

6. Is being a board member different from what you expected?

Everyone takes their role very seriously. It is refreshing to state, the board comprises experienced professionals. This has given me the opportunity to learn a lot, ranging from strategic planning to budgeting, discussing uncomfortable issues, and making difficult and life-changing decisions.

7. Would you recommend being a board member to others, and how should others prepare for applying?

Most definitely, doing what I am passionate about, I have been given the opportunity to work with highly motivated and intelligent people; having a strong

brand such a FIRST behind one is a big deal; it has opened doors for me in my career growth, and I get invited to bigger platforms, the most recent one being an invitation to the Marshall Center-State Department for Economic Community of West African States (ECOWAS) in Germany as an "expert speaker;" and fully funded by the State Department. I missed attending the 2022 Conference in Berlin because of VISA issues.

8. Incident Response comes with a lot of pressure and stress, how do you relax?:

I ride motorbikes, which started as a hobby but has become a lifestyle. I ride with a group of female riders, BikerGirlsGH; we ride for fun and charity. Riding has taught me many life lessons, including but not limited to self-discipline, commitment, always keeping an open mind, being spontaneous, and always enjoying life.

Are you interested in becoming a future board member?

Chris Gibson, FIRST CEO

FIRST CEO Chris Gibson said, "Serving on the board of directors is an exciting opportunity to develop your personal and professional life. But it is also challenging work and requires diverse skills and a consistent commitment in time and effort.

"We seek volunteers passionate about FIRST. They must be committed to the success of FIRST and have integrity, excel working in teams and management functions, take responsibility for their actions, think strategically, and help advance and professionalize FIRST. You will need to communicate well and be fluent in English. You will be expected to devote 5+ hours weekly. As a member of the Board, you take on responsibility for the whole organization and its well-being. As FIRST is increasingly recognized as an expert organization on incident response by third parties, you will represent the organization internally and publicly within the security and wider community."

Details of the 2023 Call for Nominations for the FIRST Board of Directors will be available on the FIRST Membership Portal in due course.

Be a FIRST trainer! David Rüfenacht, Senior Threat Intelligence Analyst, provides a first-hand account

As FIRST calls for more volunteer trainers, David Rüfenacht, Senior Threat Intelligence Analyst from InfoGuard AG provides a first-hand account of why he decided to volunteer.

"I believe that FIRST training is essential for multiple reasons. As FIRST members, we are part of a community, and as such, we should strive to help and support each other. Moreover, by training, I discover how other teams tackle many challenges we all face. I'm convinced that getting input from different teams across the globe with individuals from many backgrounds allows for thinking of innovative solutions. Meeting practitioners face-to-face allows for building trust, which is crucial in our CSIRT activities.

The training we developed aimed to enable a methodological approach to Cyber Threat Intelligence. It is an introductory course aimed at participants from various backgrounds, not only incident response practitioners but also policymakers, general IT managers, or anyone interested in this relatively new discipline in Information Security.

Over the last 20 years, the Internet has become a pillar of our society, and sharing our knowledge as practitioners/experts with a wider public is, for me, quite important. I've been a trainer for several years. In addition to the training I do for FIRST, I collaborate with DiploFoundation on Information Security training. I've also given training in my local community on general Information Security and Internet-related issues. So when FIRST requested trainers in my field of expertise, I was quite excited and enthusiastic about getting involved!

Teaching is a great way to structure one's ideas and learn to present them clearly and concisely - an essential skill for CTI practitioners! I believe that exchanging and learning from one another is essential. Preparing a course and providing training is not only an excellent way to anchor one's knowledge but the feedback and questions from participants are beneficial. On a personal note, exchanging with participants from various backgrounds is enriching.

I invite anybody who enjoys exchanging with individuals, who enjoys a good presentation challenge, to help foster the FIRST community. Giving training is a means of discovering the world through our information security community."

Find out more about our training initiatives **here**. If you are interested in working with us on hosting a training session, please get in touch with us through **training@first.org**.

Special Interest Groups Update

The members of the FIRST Security Lounge (SecLounge) SIG initially started organizing the Capture the Flag (CTF) event at the 24th Annual FIRST Conference in Malta in 2012. The CTF consists of a series of technical exercises (challenges) where the participants must find an answer or flag and submit it to a unique Security Lounge platform. The challenges cover a range of areas: network, web, ICS, cryptography, reverse engineering, programming, miscellaneous, puzzle, etc. CTF not only measures incident response capabilities but also provides training for members.

Developed by FIRST members and operated by volunteers, CTF now features up to 500 cybersecurity challenges. The Security Lounge SIG, in close collaboration with Dave Schwartzburg, are currently in the process of creating a standalone platform that will make the challenges available all year long. The new platform will be made available in 2023. Members will be informed once the platform goes live.

The DNS Abuse SIG has completed the first version of its *Model for DNS Abuse Stakeholders* document, which will provide incident responders with a matrix indicating which stakeholders can assist in DNS Abuse incidents on the level of detection, prevention, and mitigation. The SIG has been actively collecting feedback on the document from members and will release it in 2023.

The PSIRT SIG services Framework, the services Framework for product security, is now available in Japanese. Thank you to everyone who volunteered in this labor of love.

The advancement of the official CVSS v4.0 standard is under progress. All new and existing metrics and metric values have been defined and approved by the voting participants and formally recorded in the FIRST membership wiki.

The estimated completion dates for the official CVSS v4.0 Public Preview and Standards Publication will potentially be in line with the 2023 Annual FIRST Conference in Montreal.

“Now that the CVSS v4.0 is nearly completed, the SIG co-chairs are holding regular meetings to optimize the training delivery. The training looks like it's going to be awesome, with specific focus on Scoring Provider assessment, Scoring Consumer assessment, I.T., and O.T,” said Dave Dugal, the SIG Co-Chair.

You can find more about FIRST SIGS **here**.

Messaging Malware and Mobile Anti-Abuse Working Group (M3AAWG) and Forum of Incident Response and Security Teams (FIRST) Join Forces to Address Global Internet and Security Issues

The Messaging Malware and Mobile Anti-Abuse Working Group (M3AAWG) and FIRST announced on December 19, 2022, that they will work together to develop and train abuse desk and incident response teams in best practices of DNS abuse and incident response. Find out more **here**.

Twenty More Members Join FIRST

Last quarter saw twenty members join FIRST.

October 2022

- HRDF-DFIR, SA sponsored by CMA and STC DFIR
- Truesec CSIRT, SE sponsored by Swedbank CDC and CERT-SE
- Improsec CSIRT, DK sponsored by Orsted CDC and DKCERT
- SP-CERT, NO sponsored by HelseCERT and mIRT
- A2A-CERT, IT sponsored by TERNA-CERT and CERT-ENAV

November 2022

- Citrix CSIRT, US sponsored by BCSC and RedIRIS
- Pure Storage CIDR, US sponsored by Juniper SIRT and Palo Alto Networks
- RwCSIRT, RW sponsored by CERT-MU and bjCSIRT
- TurkishAirlines CERT, TR sponsored by Turkcell CDC and TR-CERT
- GCB Bank Plc SOC, GH sponsored by CERT-GH and bjCSIRT
- Xylem PSIRT, US sponsored by Cisco Systems and NVIDIA PSIRT
- Michael Murray, US sponsored by CERT/CC
- Cameron Brown, GB sponsored by Deloitte ECC

December 2022

- NuCSIRT, BR sponsored by Team Cymru and CAIS/RNP
- CANVIA-CSIRT, PE sponsored by CSIRT-RD and NRD CIRT
- NextEra, US sponsored by Team Cymru and RedIRIS
- ICT-CSIRT, SA sponsored by Saudi Central Bank_Cyber Security and CMA
- MOI-CERT, AE sponsored by aeCERT and ETISALAT-CERT
- CSIRT-MULTISOFT, CO sponsored by S21sec CERT and INCIBE-CERT
- SBB CERT, CH sponsored by SWITCH-CERT and CERT-Post

Thanks for reading!

Remember to follow us on our social media channels Facebook, Twitter and LinkedIn for regular updates!