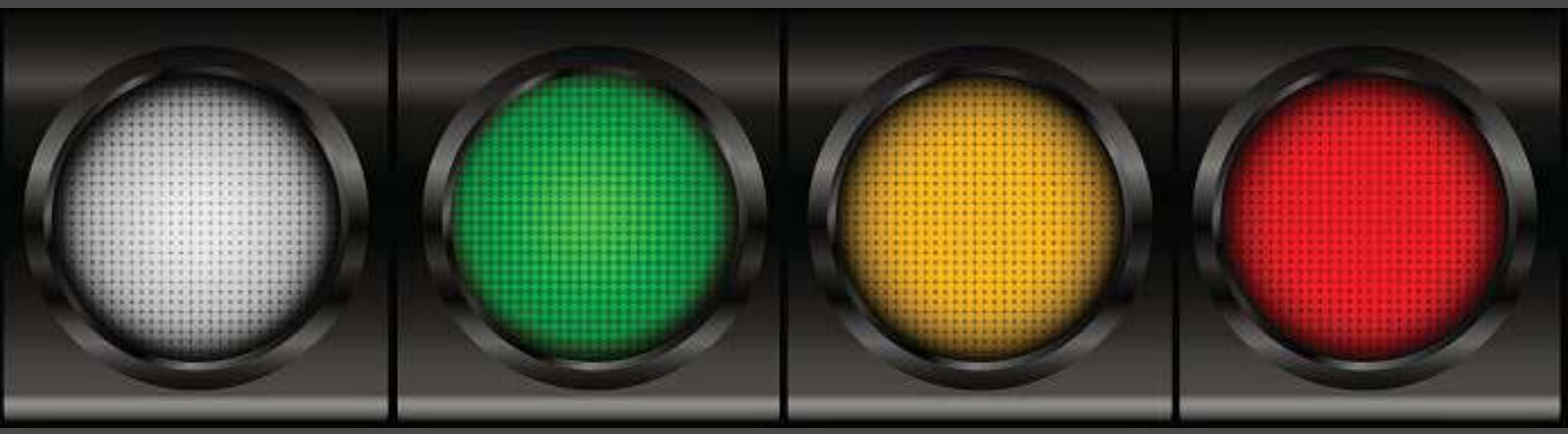
Oct - Dec 2022

FIRST POST

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

Traffic Light Protocol Version 2.0 is Now Available



This summer, the FIRST TLP Special Interest Group (SIG) updated the globally renowned Traffic Light Protocol (TLP), which organizations worldwide use to share sensitive information. The TLP SIG standardized and unified it, modernized the content and language, and improved the supporting materials. The new version was released after a thorough consultation with over 50 security industry experts over three years.

The original TLP was created in 1999 by the National Infrastructure Security Coordination Center (NISCC) in the UK. In 2015, FIRST took the lead to unify and standardize it for a global audience. In 2019, over 50 security incident professionals established the FIRST TLP Special Interest Group (FIRST TLP-SIG) to collaborate and improve it, finalizing TLP 2.0 this year.

FIRST TLP-SIG made the following significant changes:

- ***Removed synonyms and colloquialisms to improve accessibility for non-native English speakers and ease of translation.***
- ***Focused on consistent language and terminology, adding community, organization, and client definitions.***
- ***Added a colors table to include RGB, CMYK, and hexadecimal color codes.***
- ***TLP:WHITE has become TLP:CLEAR.***
- ***Added the TLP:AMBER+Strict label to only highlight information restricted to the recipient's organization.***

FIRST TLP-SIG co-chair Don Stikvoort (Open CSIRT Foundation) said: “We are increasingly spreading more confidential and sensitive information inside our community, inside companies, inside business sectors, inside countries, and worldwide. We need systems that are easy to use, simple to understand, and straightforward enough that translation does not impact the meaning to ensure that we share sensitive information with the appropriate audience. The updated and modernized TLP version 2.0 does just that.

Some of the changes in the TLP version 2.0 may impact the industry’s current tools. However, FIRST hopes the industry embraces this update quickly and will be fully in use by January 2023. Indeed major players such as CIRCL or CISA have already announced that they will be switching to the new standard. The more people accept the protocol, the more smoothly incidents can be coordinated and resolved with minimum anxiety.

Interested parties can find more information and the TLP **here**.

"Since release, we are grateful to the FIRST members who have volunteered to provide us with translations of TLP version 2.0 into Brazilian Portuguese, Dutch, French, Japanese, Norwegian, Romanian, Spanish, and Swedish. And no doubt, more to follow. As SIG chairs, we are more than happy with this quick uptake."

Don Stikvoort, FIRST TLP-SIG Co-Chair

FIRST delivers training in Uganda, and the Western Balkans

Volunteers deliver several training sessions throughout the year on behalf of FIRST. This training occurs at events and conferences or due to requests from members and organizations who share our objectives.

Last month (September), our volunteers delivered training in Uganda and the Western Balkans to educate new CSIRTs and enhance the capabilities of current teams.

Pawel Pawlinski (CERT Polska/NASK PL) and Jaroslaw Jedynak (Broadcom/Symantec) gave training in Threat Intel Pipelines and Building Malware Analysis Pipeline using Open Source Tools at the Operator Technical Cybersecurity Training. The Uganda Communications Commission (UCC) hosted the event. It’s the second time we have cooperated with the UCC, and it is always a pleasure to experience the hospitality of the Uganda teams.

We trained the attendees to

- ***Find valuable sources of information***
- ***Design and implement effective processes to handle collected information***
- ***Choose the best approaches to combine data***
- ***Apply automation to achieve the optimal results in the relevant environment***
- ***Analyze malware using tools and frameworks like MWDB and Karton***

In late September, Toomas Lepik (Tallinn University of Technology) and Leone Viru undertook Malware Analysis training for CSIRTs in the Western Balkans in cooperation with DCAF, Geneva Centre for Security Sector Governance, who we have worked with several times over the years.

FIRST board member Mona Østvang and training liaison said: "We appreciate members and nonmembers who work with FIRST around the world and the organizations that allow us to reach teams with our training. Building a common language and understanding for incident responders is an important part of our mission, and trainers also obtain valuable experience. We encourage experts from all over the community to contact us if they are interested in becoming a trainer."

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

Peter Lowe speaks about DNS Abuse at ICANN75 AGM in Kuala Lumpur

Peter Lowe, newly appointed FIRST DNS Abuse Ambassador, recently did a presentation entitled 'The Challenge of Defining DNS Abuse' at the ICANN75 AGM, organized by the Internet Corporation for Assigned Names and Numbers (ICANN) in Kuala Lumpur, Malaysia in September. ICANN is an internationally organized non-profit corporation responsible for Internet Protocol, and this is the first time that FIRST has been invited to speak at one of its events.

DNS Abuse featured heavily during the AGM, even highlighted by the ICANN president and CEO during the opening meeting. Peter's presentation was well received, and many attending industry specialists asked good questions, especially about FIRST's work. He also made valuable connections, including people from ICANN, the DNS Abuse Institute, registries, registrars, CERTs, commercial companies, government organizations, and many more.

Members can find out more about, and are welcome to join the DNS Abuse SIG here.

"It was very advantageous for FIRST to have a presence at this conference as it enabled us to share our expertise, raise awareness of our work, and build relations with influential people and organizations who will help us to fulfill our vision. I met many people from our industry and spread the word about the excellent work that FIRST does. Many people were curious about what we do, especially in our DNS Abuse Special Interest Group.

"I look forward to participating in future events and making progress on the relationships I built at this one,"

Peter Lowe, FIRST DNS Abuse Ambassador

FIRST Chair Sherif Hashem participates in the Cyber Diplomacy and Norms panel at The Second Community of African Cyber Experts

Our Chair, Sherif Hashem was recently invited to provide input on cyber strategies and policies at the virtual Second Community of African Cyber Experts (ACE) Meeting, which took place 28-29 September 2022. Sherif's spot was on the panel entitled Cyber Diplomacy and Norms. The event was co-organized by the Global Forum for Cyber Expertise (GFCE), the African Union Development Agency (AUDA-NEPAD), and the Ministry of Posts, Telecommunications, and the Digital Economy of the Republic of the Congo.

During the panel, Sherif spoke on the roles of incident response and security teams in supporting the implementation of cyber norms and confidence building measures (CBMs). He highlighted the importance of global and regional cooperation, especially in the area of cyber capacity building, and that FIRST plays a central role in empowering and strengthening cooperation and knowledge exchange among incident response and security teams across the world, as well as supporting partnerships with various stakeholders.

In addition Sherif emphasized that adopting an open and inclusive multi-stakeholder approach is essential for the successful implementation of cyber norms and CBMs.

The World Opens - FIRST Events Round Up

FIRST is delighted to share that we are almost back to normal now in terms of delivering events, collaborating with other event organizers and participating in industry-related conferences.

The past two months saw two successful events occur - the 2022 PSIRT SIG Technical Colloquium, hosted by SAP and FIRST, which was held in Pennsylvania, and the UNDP FIRST Valencia Technical Colloquium, hosted by UNDP in Spain, where board member Serge Droz was invited to give a well-received keynote on 'Incident Response in Difficult Times'.

This month, the Oslo 2022 FIRST Technical Colloquium: Cold Incident Response will take place. This event was fully booked in six days, a testament to the FIRST Norway team's dedication to putting on a program of great interest to the industry.

This month also saw the **FIRST Virtual Symposium** for the Asia Pacific Regions, hosted by APCERT and FIRST, which took place October 20-21, 2022.

There is also an opportunity to attend the in-person 2022 FIRST Cyber Threat Intelligence Symposium on ***November 1-3, 2022***. In Berlin, the event will feature a one-day training session followed by two days of plenary sessions. This event is open to members and non-members. Members can find more information **here**.

In November, our chair Sherif Hashem and board member Michael Hausding will represent the cybersecurity industry at the **10th Regional Cybersecurity Summit in Oman & the FIRST & ITU-ARCC Regional Symposium for Africa and Arab Regions *6 – 9 November 2022*** in the Sultanate of Oman. Sherif's presentation is entitled 'Cybersecurity Innovation Ecosystem, Government, Academia & Industry' and Michael's the Evolution Of Cyber Security Response Against Emerging Threats'. OIC-CERT has a mandate that covers 57 countries, while ITU-ARCC's covers 22 countries. The FIRST Regional Symposium attracts participants from over 100 countries. Registration for this event is now closed.

Looking at next year, the TF-CSIRT Meeting & 2023 FIRST Regional Symposium Europe will be held January 31 - February 2, 2023. The event host is the Basque Cybersecurity Centre in Bilbao, Spain. You can find more information **here**.

FIRST chair, Sherif Hashem said: "FIRST is committed to strengthening cooperation and facilitating knowledge exchange among incident responders and security teams regionally and globally. Such events further enhance capacity building and contribute to building trust and confidence. We intend to emphasize the importance of building bridges to support networking and empower cooperation across the globe."

You can find the full list of upcoming events **here**.

Désirée Sacher-Boldewin

Olivier Caleff

Special Interest Groups Update and New NETSEC SIG Formed

New board members Désirée Sacher-Boldewin, and Olivier Caleff are now board liaisons for the FIRST's Special Interest Groups (SIG's), which exist to provide a forum for FIRST members to discuss topics of common interest. Over the next few months, Désirée and Olivier will focus on creating clear instructions for the SIG chairs on publishing their SIG results, providing improved tools and operational guidance, and tips on running a SIG meeting efficiently. Désirée and Olivier will refine these instructions further over the coming months and create templates to enable SIG chairs to run their activities more efficiently. Some of these new instructions are already available on the members portal. In addition, tools for supporting hybrid SIG meetings during conferences are in development.

A new SIG, NETSEC, was formed in June at our Annual Conference in Dublin. NETSEC-SIG will focus on sharing information to encourage the adoption of inter-AS security Best Current Practices, facilitate response coordination of inter-AS BGP routing issues and abuse, promote inter-AS DDoS traceback and mitigation as well as encourage inter-AS security incident event sharing. Members can find more information and details on how to join this SIG on our **website**.

Katie Noble and Tom Millar are the new chairs for our Ethics SIG, and Raja Jasper and James Potter volunteered to co-chair the Malware Analysis SIG (MA-SIG) after Olivier Caleff stepped down when he joined the FIRST board.

Members can find details of all SIGs **here**.

The Board meets in Davos

The Board met face-to-face in September in Davos, Switzerland, to assess and review FIRST's business plan and work on our future strategy.

The Board spent the first morning of the three-day meeting conducting a wide-ranging discussion on the existing mission, goals, and strategy, followed by a capacity and community-building session. We also examined communications in detail. We confirmed the current mission and goals, and the plans to meet those goals were reviewed and updated. The new members of the board were able to both evaluate these existing plans and bring their thoughts and experiences to the meeting.

The Board also discussed and finalized which members will take responsibility for specific areas of our work - listed in the following article.

This was the first face-to-face meeting with all Board members since the pandemic, and it was very productive. Having all the members in one place, at the start of the year, for three days allowed us to understand each other better professionally and socially. It also enabled us to build a business plan that all Board members had a part in finalizing.

Board of Directors Organization and Roles for 2022/23

The FIRST Board comprises incident response, and security professionals voted in by our members worldwide. The new Board members bring skills unique to their own country or region. Each member has volunteered to take on a specific role related to FIRST's work, from Special Interest Groups (SIG) to Training. Our virtual monthly meetings are a place to discuss current and prospective affairs related to this work and build the 2023 business plan and budget.

As detailed in the previous FIRST POST, ***Sherif Hashem*** was appointed Chair immediately after the AGM. Sherif has asked ***Serge Droz*** to fill the role of Vice-Chair, which he accepted.

In another vote immediately after the AGM, ***Michael Hausding*** was voted as Chief Financial Officer and Treasurer. ***Olivier Caleff*** volunteered to act as Vice CFO and Treasurer.

Audrey Mnisi Mireku has volunteered for Outreach, focussed on Africa and the Middle East, and joined the Diversity & Inclusion group.

Désirée Sacher-Boldewin will take over SIG liaison with Olivier Caleff.

Mona Elisabeth Østvang has volunteered for Education and Training, and Outreach, focusing on Europe. Mona will also join the Diversity & Inclusion group.

Olivier Caleff will take on the Communications role and the Membership Committee Liaison role and assist with Hall of Fame, and Fellowship liaison roles, alongside his Vice Treasurer/CFO role.

Tracy Bills will lead the Fellowship Program, support Olivier as Membership Committee liaison, and joins the Diversity & Inclusion group. Note that Tracy is also the Conference Chair for the conference in Montreal 2023.

Trey Darley will lead on Governance & Bylaws and Standards and join the Diversity & Inclusion group.

Serge Droz will also focus on the Policy work with Sherif, on top of his Vice Chair role.

Yukako Uchida will lead on the Hall of Fame, Outreach for APAC and join the Diversity & Inclusion group.

Lastly, a team of four support the Board – ***Chris Gibson***, CEO, ***Nora Duhig***, ***Dave Schwartzburg***, and ***Klée Aiken*** - whose roles and responsibilities are in the table below.

	PRIMARY	ALTERNATE / VICE
Chair / Vice Chair	Sherif Hashem	Serge Droz
CFO / Vice CFO	Michael Hausding	Olivier Caleff
Secretariat	Nora Duhig	
Membership Liaison	Olivier Caleff	Tracy Bills
Fellowship Program	Tracy Bills	Olivier Caleff
Hall of Fame	Yukako Uchida	Olivier Caleff
Standards (FIRST/ISO)	Trey Darley	Désirée Sacher-Boldewin
Governance/Bylaws	Trey Darley	
Conference Chair	Tracy Bills	
Outreach:(Symposia Liaison, TC Liaisons, Training Delivery, Membership)	*Africa, Middle East*:Audrey Mnisi Mireku	Klée Aiken
	APAC: Yukako Uchida	Klée Aiken
	Europe: Mona Elisabeth Østvang	Klée Aiken
	Americas,Oceania: Tracy Bills	Klée Aiken
SIGs	Désirée Sacher-Boldewin	Olivier Caleff
Privacy Officer	Dave Schwartzburg	
Education & Training	Mona Elisabeth Østvang	Tracy Bills, Olivier Caleff
Policy	Serge Droz	Sherif Hashem
Communications/PR	Olivier Caleff	Chris Gibson
Sanctions	Sherif Hashem	Serge Droz, Chris Gibson
Diversity & Inclusion	Audrey Mnisi Mireku	Mona Elisabeth Østvang, Yukako Uchida, Trey Darley
Volunteer Management	Chris Gibson	
Alternative Revenue	Trey Darley	Michael Hausding, Sherif Hashem
Infrastructure	Dave Schwartzburg	

Twenty new members join FIRST

We now have 651 teams in 101 different countries worldwide in our membership. Existing members can find the complete list of members on the FIRST portal.

July - August

- Pfeiffer Vacuum CSIRT, DE sponsored by CERT-Bund and ComCERT
- Mallory Knodel, US sponsored by Zendesk
- Martin Nagel, CH sponsored by Swisscom CSIRT
- LEGO CSIRT, DK sponsored by OxCERT and NCSC UK
- CSIRT-SATEC, ES sponsored by INCIBE-CERT and BCSC
- Health-ISAC, US sponsored by Team Cymru and Z-CERT
- Global CERT Atos, PL sponsored by Siemens-CERT and CERT Polska
- VOID SOC, SK sponsored by SK-CERT and DNSC

September

- Art Manion (Liaison), US sponsored by Panasonic PSIRT
- AQUA INTERACTIVE CERT, MX sponsored by TIC-Defense-CERT and CSIRT-RD
- TI America CSIRT, MX sponsored by CSIRT-CEDIA and BA-CSIRT
- CERT Nameshield, FR sponsored by CERT Credit Agricole and Orange-CERT-CC
- SOFISTIC-CSIRT, ES sponsored by INCIBE and NUNSYS-CERT
- Kyndryl CSIRT Iberia, ES sponsored by INCIBE and CCN-CERT
- POLI-CERT, IT sponsored by ESACERT and CERTBI
- Aitu PSIRT, KZ sponsored by KZ-CERT and NBRK KZ CERT
- CERT CM EI, FR sponsored by CERT Credit Agricole and CERT SG
- Sophos Security Team , GB sponsored by NCSC UK and Mandiant Security
- AXUS-CSIRT, PE sponsored by CSIRT-CEDIA and BA-CSIRT
- Onevinn MDR, SE sponsored by CERT-SE and LiU IRT

If you are not yet a member of FIRST and are interested in joining you can find more information **here**.