Jan - Mar 2022

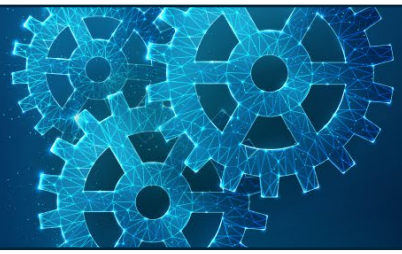
FIRST POST

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

Three new Special Interest Groups created by FIRST members

One of the key ways that FIRST supports its members is by providing forums in the form of Special Interest Groups (SIG). The goal of SIGs is for the incident response community to collaborate and share expertise and experiences to address common challenges. FIRST SIGs consist of Working Groups, Standard Groups, and Discussion Groups. Current groups include Ethics, Common Vulnerability Scoring System, and Industrial Control Systems. Many of these SIGs collaborate on other projects. Members have created three new Special Interest Groups (SIGs) this year, taking the number of active groups to 26.

Automation SIG



Every incident response team globally is facing a severe increase in workload. As attackers scan and penetrate networks via automation, defenders must look at automation more closely. Sadly, there is no single magical solution for "automating away" the incident response on the defenders' side. So a team of incident responders and FIRST members have created a new SIG focused on improving security together. The SIG will focus on sharing knowledge, learning from each other, and disseminating the condensed expertise to the FIRST community.

The SIG will first examine what already exists, gathering incident responders' experiences, both successes and, more importantly, failures, to not repeat the same mistakes. Next, the group will build a list of proven effective tools (both commercial and open-source), strengths and weaknesses, and applicability.

Collaboration will be critical to the success of the Automation SIG, so the group is open to contributions from the industry, and they welcome individuals or teams that can help establish links with other communities like IHAP (Incident Handling Automation Projects group) and TF-CSIRT. The group will send a short survey to potential collaborators about their needs, experiences, and possible input.

The SIG will have quarterly calls starting end of January 2022. In addition, documentation and knowledge will be stored in FIRST's membership portal - you can join here too! The chairs of this group are David Durvaux, Aaron Kaplan, and Benoît Roussille all of EC DIGIT CSIRC.

You can find more information about the Automation SIG at **https://www.first.org/global/sigs/automation/**. The team looks forward to welcoming you.

The new FIRST Muli-Stakeholder Ransomware (MSR) SIG aims to foster international and intentional collective action among FIRST stakeholders and taskforces. The SIG will appeal to those whose focus is ransomware response, mitigation, remediation, investigation, and prevention. In the summer of 2021, several seasoned FIRST community members created the MSR SIG. Having banded together to create a cross-functional working group, they found many gaps in the current ransomware task force environment.

The first goal is to collect and collate tools, data, resources, and feedback while at the same time giving tools to the community to track and record the impact of ransomware attacks. Feedback so far from the ransomware frontlines indicates that teams are regularly in crisis mode and do not have the time or capacity to innovate on the spot during an attack. The SIG aims to solve this problem by providing a platform for taskforces to collaborate and source tools, tactics, and procedures and quickly choose the right joint action while under extreme pressure.

"We hope that the creation of this SIG will drive down the number of ransoms and the amount paid but also make restoration cheaper, faster, and easier to deploy. Cyber risk analysis always supports good defense-in-depth and is probabilistic. We specifically saw a gap in quantifying some of these probabilities, the effectiveness of different responses or preventative measures, and replicating effective programs instead of copying advice from marketing programs. Estimating the overall size of the ransomware problem alone requires strategic collaborations," says Barry Greene, the SIG Chair.

The Multi-Stakeholder element would include M3AAWG, APWG, and other allied efforts. The needs of the FIRST community will be the initial focus, with dialog sessions used as a basis for short-term deliverables. Other organizations similar to FIRST will be approached to participate and coordinate efforts - the intention is to optimize activities, minimize overlap, duplication, and not overtax limited people and resources.

Multi-Stakeholder Ransomware SIG is inviting you to participate!

- Join the SIG at **https://www.first.org/global/sigs/msr/**
- Join the bi-weekly consultation calls where dialog, suggestions, and collective help is welcome to gear up activities. Just sign up for the SIG **here**.
- Sign up for the SIG's focused breakout working groups that focus on specific areas of the ransom -ware risk. These will be announced on the MSR mailing list, the MSR Slack (on the FIRST Slack), and the MSR Wiki.
- Sign up for dialog and listening sessions, where curated sessions to listen, learn and identify ransom -ware risk areas that need the FIRST community's attention.

In 2019, female members teamed up during the FIRST Annual Conference in Edinburgh to encourage more women to participate in the conference and enter the field of cybersecurity. Since then, the team has met monthly to discuss topics of interest and learn from each other. This year, due to increased interest, the women decided to expand these informal meetings into a newly created SIG to develop a buddy program for security conference attendance and provide a forum for women to network and learn cybersecurity skills.

Women interested in joining the SIG can follow the specially created **LinkedIn page** for updates; a new round of meetings will start in January 2022. Meanwhile, the SIG will continue to develop its goals.

More details will be available in the following newsletter.

FIRST participates in several important UN activities

By Serge Droz

FIRST has been very active in many UN initiatives these past few months.

On November 24, FIRST, together with several partners, including the International Telecommunication Union (ITU), launched the second edition of the '**Guide to Developing a National Cybersecurity Strategy**.' Board member Yukako Uchida and former board member Koichiro 'Sparky' Komiyama contributed substantially to the document over the past year. During the virtual launch, I stressed the importance of preparedness, highlighting FIRST's continuous engagement in capacity and community building. The guide emphasizes the importance of CSIRTs and their role in building a meaningful cyber security strategy. We were proud to be invited to contribute to the NCS as a recognized leader in incident response.

The United Nations Institute for Disarmament Research (UNIDIR) flagship '**2021 Cyber Stability Conference: Towards a More Secure Cyberspace**' took place the following week. I participated in a panel about 'Existing and potential threats.' I stressed how recent state-run operations caused enormous collateral damage and exhausted incident response capacity, which meant incident response and security teams were unable to fulfill their obligations elsewhere. Most state-run operations are conducted as espionage operations, which are, a priori, legal under international law. However, there is an expectation that such acts will be limited to their intended target. There is a widespread view that the SolarWinds and Hafnium incidents were significantly more extensive and more indiscriminate than needed.

The topic was picked up again during the 2021 Internet Governance Forum in Katowice, Poland; board members Sherif Hashem and myself participated in several online sessions. During this session, there was a consensus that state-run operations increasingly cause problems for innocent bystanders, who already suffer from the effects of cybercrime.

Subsequently, during an informal **UN Open-Ended Working Group** consultation, FIRST stressed the importance of not attacking Incident response teams during cyber conflicts. Furthermore, cyber operations must respect the principle of proportionality and not cause any harm to everyday internet users.

FIRST feels strongly that the Internet can only remain free, open, and secure if all stakeholders, states, and the private sector, work together at eye level.

FIRST will continue to engage in policy matters in 2022, kicking off participating in the UN ad hoc committee on fighting cybercrime in January 2022.

19 events organized in 2021 - registration opens for FIRST Annual Conference in 2022

Despite many challenges, FIRST organized nearly 20 events in 2021, from workshops and training to a virtual FIRST Annual Conference. The year started with the first of our Regional Virtual Lightning Talk Sessions in February, featuring conversations between a wide range of global experts in the field, and ended this month with the FIRST & AfricaCERT Virtual Symposium for Africa and Arab Regions. The latter was held online from December 7-9, 2021. Nearly 130 people participated, made up of global FIRST Member Teams and CSIRTs from the African and Arab regions, network operators, anti-abuse teams, and other security professionals.

While most of this year's events were virtual, FIRST members based in Norway organized an in-person technical colloquium in Oslo, attracting nearly 190 attendees - more of which you can read about in our blog **here**.

Our annual conference is, of course, an important event for our community. This year's conference is scheduled for Dublin, Ireland, from June 26 to July 1, 2022. Registration opens soon at **https://www.first.org/conference/2022/registration-info**.

Members and non-members should keep our 2022 **events calendar** bookmarked to see what's coming up this year!

Twelve more member teams join FIRST

Please extend a welcome to the 12 new security teams who have joined us since the last edition of the FIRST Post.

October:

- Marc Rogers (liaison) sponsored by NVIDIA PSIRT
- Sigitas Rokas (liaison) sponsored by NRD CIRT
- Sopra Steria SOC Nordics, NO sponsored by TCERT and Nordic Financial CERT
- Kongsberg Cyber Security Center (KCSC), NO sponsored by NCSC-NO and KraftCERT
- Tigo T-CERT, GT sponsored by Team Cymru and RedIRIS

November:

- Avast CERT, CZ sponsored by CSIRT.CZ and GovCERT.CZ
- Western Digital PSIRT, US sponsored by NVIDIA PSIRT and Auth0 Detection and Response Team
- Sysmex-CSIRT, JP sponsored by JPCERT/CC and NTT-CERT

December:

- Zack Allen (liaison), US sponsored by Zendesk
- VNPT Cyber Immunity, VN sponsored by Team Cymru and VNCERT
- Utility Warehouse, GB sponsored by CrowdStrike and NCSC UK
- GBM Cyber SOC, CR sponsored by JackSecurity and Team Cymru

Get more details about how to become a member **here**