Academic Security SIG

#FiRSTCON22 update

Liliana (Nina) Solha (RNP, Brazil)
Roderick Mooi (GEANT Association, EU)
Academic Security SIG

Worldwide platform for collaboration of Academic and Research security incident response teams

Primary target public:
• NREN & University CSIRTs
• Research & Education CSIRTs in general

Resources:
• SIG mailing list (57 subscribers)
• SIG page @FIRST Portal (members-only)
• SIG meetings (FIRST Zoom platform)
Academic Security SIG

Meeting up with members...
## Academic Security SIG

The SIG in a timeline...

<table>
<thead>
<tr>
<th>Year</th>
<th>Meetings</th>
</tr>
</thead>
</table>
| 2022 | 01 virtual SIG meeting (April)  
      | 01 F2F SIG meeting & 01 F2F SIG Update @FIRSTCON  
      | 01 virtual meeting (September)  
      | 01 virtual SIG meeting (February) |
| 2021 | 01 virtual SIG Update @SIGUpdateWebinars  
      | 01 virtual SIG meetings (September) |
| 2020 | 01 virtual SIG meeting  
      | 01 virtual SIG Update @SIGUpdateWebinars |
| 2019 | 01 F2F SIG meeting @FIRSTCON  
      | 01 F2F SIG Update @FIRSTCON |
| 2018 | 02 virtual SIG meetings  
      | 01 F2F SIG meeting @FIRSTCON |

**FIRST Academic Security SIG Meeting**  
**June 30**  
**(10:15-12:15 UTC+1)**
SIG Working Groups

SIG should focus on:

- Academic CSIRTs/SOCs
- Cooperation with other similar regional and global initiatives
- Cyber Threat Intelligence
- Incident Response Coordination
- Training and Awareness

Description
Scope
Goals/objectives
Deliverables
Timeline
We have had a few meetings. Identified that;

• Not many Universities are formally using Cyber Threat Intelligence
• That there might be space to identify how to use Cyber Threat Intelligence in an Academic environment.
• And signpost where people are currently looking for Cyber Threat Intelligence

For this, we set out a questionnaire, to the following groups;
• FIRST / REN-ISAC / UK Universities

Next steps
• More meetings!
• Analysis of the questionnaire
Incident Response Coordination WG

Purpose: Improve and facilitate cross-organisation incident response by collecting and disseminating relevant information (_not_ an operational WG).

Past activities
Established lines of communication, identified hot topics of interest, started work on those.

Work in progress
A curated contact meta-database with focus on academic players, show-and-tell intros of interesting tools.

Relevance
Incident response coordination was identified as a topic of interest in the Academic SIG.
Academic Security SIG – how to join?

https://www.first.org/global/sigs/academicsec

Participation Policy:

- Open but generally restricted to **academic** CSIRTs (research & education, NREN, University, etc.)
- **Non-academic** CSIRTs at the discretion of the chairs.

Note: it is not a requirement to be a FIRST member to participate in the SIG though we do encourage it.

Request to Join Form:
https://portal.first.org/g/Academic%20Security/join
Thank you!

Liliana Solha (RNP, Brazil)
Roderick Mooi (GEANT Association, EU)

academicsec-chairs@first.org

(Thanks to the WG coordinators Patrick Green and Tobias Dussa for providing the WG update slides).