eduGAIN Security

The eduGAIN CSIRT's main duty is to provide a central coordination point at the inter-federation level for the security incident response. Moreover, the team will share information on security threats relevant for the eduGAIN community.

While each Federation Operator and Federation Participant provides security support within their respective domain of responsibility, inter-federation remains everybody's responsibility, which means no entity is effectively accountable to do the necessary work. Yet, when defending against global attacks targeting global services, inter-federation must be at the core of incident response strategy.
The eduGAIN CSIRT supports this collective responsibility in inter-federation incident response within eduGAIN.

The eduGAIN CSIRT is a central contact and support point for security incidents, and coordinates the investigation and resolution of suspected security incidents that affect Federation Operators and Federation Participants. This includes notifying Federation Participants and Federation Operators or any other relevant entity about attacks potentially affecting them.

The collective expertise and experience accumulated by the eduGAIN community as it defends against attacks is invaluable. The eduGAIN CSIRT ensures that lessons learned, statistics, and other useful information are disseminated appropriately to improve our security posture as a global, united community.

eduGAIN Security Incident Response Handbook

The eduGAIN CSIRT in collaboration with the REFEDS Sirtfi WG developed an eduGAIN Security Incident Response (SIR) Handbook, which after REFEDS consultation (see https://wiki.refeds.org/x/-oCNAw) is now promoted across eduGAIN community for adoption.

The eduGAIN SIR handbook defines the process for resolving security incidents affecting eduGAIN participants involving all key stakeholders. In particular, it is essential to involve the federation in security operations or possible intrusions affecting eduGAIN entities.

Federation Security Contact

Each eduGAIN Member should provide a federation security contact that can act as the contact and technical support point for security incidents affecting the federation, as further defined in the eduGAIN SIR handbook. The contact must be capable of operating according to the eduGAIN SIR handbook and maintain a level of confidentiality suited to the information received. Trusted, well defined and well maintained security contact information is crucial to allow all involved parties to collaborate and exchange sensitive data during a crisis.

This role is expected to be fulfilled by the security contact point as expressed in each federation profile and it will be published on the eduGAIN Member Status page (https://technical.edugain.org/status). In order to communicate the security contact for your identity federation follow the procedure on https://technical.edugain.org/joining_checklist.

Security threats information sharing

The eduGAIN CSIRT will share information on potential and actual security threats with the federation security contacts and if needed with the entities's Sirtfi security contacts.

This includes vulnerabilities, malicious indicators and exposed or compromised credentials. Whenever possible the eduGAIN CSIRT will notify entities when information about exposed credentials surfaces. Although the origin of the compromise or its context may not be known, the available data is made available to the possibly affected entity, so that they can make their own determination.

Trust is an essential part of threat information sharing and in eduGAIN, rely on two pillars by :

- Strictly abiding to the Traffic Light Protocol (TLP, https://www.first.org/tlp/), which is used in most communications to mark information being shared according to its sensitivity and the audience with whom it may be shared.
- Urging all entities to adopt (and update their metadata accordingly) the Sirtfi framework (https://refeds.org/sirtfi). Federation Participants that support the Sirtfi framework (https://refeds.org/sirtfi) will receive full Incident Response information, more details on vulnerabilities or ongoing attacks, and support. Federation Participants that do not support Sirtfi will receive limited information and support.

Contacts

For computer security emergencies or in case a security incident is suspected:

Contact the eduGAIN CSIRT: abuse@edugain.org

PGP key fingerprint: F9FF B82B 9700 72D1 F753 25CF 5E3C 31D7 CE43 BCB8