Incident Response Procedure

Status	**Draft**
Date	**25 February 2022**
DOI	**10.5281/zenodo.6276064**

Document log

Issue	Date	Description	Author
v. 0.1	08-11-2021	Initial version	Renato Furter
V. 0.2	25-02-2022	Minor textual improvements	Ron Trompert

Terminology

The Science Mesh glossary is available at: https://doi.org/10.5281/zenodo.5038662

For the purpose of this document, the following terms and definitions apply. The key words "MUST", "MUST NOT", "REQUIRED", "SHALL", "SHALL NOT", "SHOULD", "SHOULD NOT", "RECOMMENDED", “MAY", and "OPTIONAL" in this document are to be interpreted as described in RFC 2119.

Table of Contents

Introduction

This document describes the procedure that a Science Mesh participant and their security contact (CERT Team) has to follow in case of a security incident. It has two sections with a procedure for each of the two groups. By joining the Science Mesh, you automatically agree to follow these procedures in case of a security incident.

This document is based on the AARC Policy Development Kit[1].

Security Incident

Security in a distributed collaborative environment like the Science Mesh is governed by the same principles that apply to any other managed IT-system, but is complicated by the diversity of sites - both in terms of hardware and software systems and in terms of local policies and practices that apply.

Procedure for Science Mesh Participants

1. Aim at containing the security incident to avoid further propagation whilst aiming at carefully preserving evidence and logs. Record all actions taken, along with an accurate timestamps.
2. Report the security incident to the Site Security Contact point (CERT Team) as soon as possible but no later than within one local working day of the initial discovery or notification of the security incident.
3. In collaboration with the Security Incident Response Coordinator (identified by the Infrastructure Security Contact):
    a. Collect and strive to identify indicators of compromise (IoCs)
    b. Share incident status reports and IoCs with all affected participants (a “heads-up” and subsequent updates as needed), in the Science Mesh via their security contact and, if needed, in other infrastructures and with any external trusted entity involved.
4. Announce suspension of service (if applicable) in accordance with the Science Mesh Helpdesk. Public announcements should not contain details other than “Security operations in progress”, unless agreed otherwise with the Site Security Contact point.
5. Perform appropriate investigation, system and network analysis and adequate forensics, and strive to understand the exact cause of the security incident, as well as its full extent. Identifying the cause of security incidents is essential to prevent them from reoccurring. The time and effort needs to be commensurate with the scale of the problem and with the potential damage and risks faced by affected participants.
6. Share additional status updates and IoCs as often as necessary to keep all affected participants up-to-date with the security incident and enable them to investigate and take action should new information appear.
7. Respond to requests for assistance from other participants involved in the security incident within one working day and investigate new IoCs being shared.

[1] https://aarc-project.eu/policies/policy-development-kit/

8. Take corrective action, restore access to service (if applicable) and legitimate user access.
9. In collaboration with the Security Incident Response Coordinator, produce and share a report of the incident with all Science Mesh organisations in all affected Infrastructures within one month. This report should be labeled TLP AMBER[2] or higher.
10. Update documentation and procedures as necessary.

Procedure for Science Mesh Participants Security Contact

1. Assist Science Mesh participants in performing appropriate investigation, system and network analysis and forensics, and strive to understand the cause of the security incident, as well as its full extent. The time and effort needs to be commensurate with the scale of the problem and with the potential damage and risks faced by affected participants.
2. Report the security incident to their federation security contact point within one local working day of the initial discovery or notification of the security incident.
3. Coordinate the security incident resolution process and communication with affected participants until the security incident is resolved:
    a. Collect and strive to identify indicators of compromise (IoCs) from all involved entities
    b. Share incident status reports and IoCs with all affected participants (a “heads-up” and subsequent updates as needed), in the Infrastructure and federation via their security contact (and, if needed, in other federations and with any external trusted entity involved). If other federations are affected, the eduGAIN security contact point must be notified, even if affected participants in all other federations have been contacted directly.
4. Ensure suspension of service (if applicable) is announced in accordance with infrastructure, federation and interfederation practices.
5. Share additional status updates and IoCs as often as necessary to keep all affected participants up-to-date with the security incident and enable them to investigate and take action should new information appear.
6. Assist and advise participants in taking corrective action, or restoring access to service (if applicable) and legitimate user access.
7. Produce and share a report of the incident with all Sirtfi-compliant organisations in all affected federations within one month. This report should be labelled TLP AMBER[2] or higher.
8. Update documentation and procedures as necessary.

[2] https://www.cisa.gov/tlp