SEKOIA.IO CERT
RFC 2350

Date : 15/05/20223

Version: 2.0

SEKOIA.IO – RFC2350

1. DOCUMENT INFORMATION

This document contains a description of the SEKOIA.IO CERT in accordance with RFC 2350 specification. It provides basic information about our team, describes its responsibilities and services offered.

1.1. DATE OF LAST UPDATE

This is the version 2.0 released on 15th May 2023.

1.2. DISTRIBUTION LIST FOR NOTIFICATIONS

There is no distribution list for notifications.

1.3. LOCATIONS WHERE THIS DOCUMENT MAY BE FOUND

The current and latest version of this document is available at: https://sekoia.io/rfc2350

1.4. AUTHENTICATING THIS DOCUMENT

This document has been signed with the PGP key of the SEKOIA.IO CERT and can be found at this URL: https://sekoia.io/rfc2350

1.5. DOCUMENT IDENTIFICATION

Title: Sekoia.io CERT RFC 2350
Version: 2.0
Document Date: 15/05/2023
Expiration: this document is valid until superseded by a later version

2. CONTACT INFORMATION

2.1. NAME OF THE TEAM

Short name: CERT SEKOIA.IO
Full name: CERT SEKOIA.IO

2.2. ADDRESS

SEKOIA.IO CERT
PARIS:
54 rue des Petites Ecuries
75010 PARIS

2.3. TIME ZONE

CET/CEST: Europe/Paris (GMT+01:00, and GMT+02:00 on DST)

2.4. TELEPHONE NUMBER

+33-183-641-661

2.5. FACSIMILE NUMBER

None available

2.6. OTHER TELECOMMUNICATION

None available

2.7. ELECTRONIC MAIL ADDRESS

cert@sekoia.io

2.8. PUBLIC KEYS AND ENCRYPTION INFORMATION

PGP is used for functional exchanges with external CERT / CERT.
User ID: SEKOIA.IO CERT <CERT@sekoia.io>
Key ID: DA65 4831 D746 85ED
Fingerprint: 898C C45E 856E FC8A 0AEF 6CDA DA65 4831 D746 85ED
It can be retrieved from one of the usual public key servers.

2.9. TEAM MEMBERS

The Sekoia.io CERT representative is François Deruty (COO) (substitute Nicolas Caproni)
The full list of the team members is not publicly available.
The team is made of Cybersecurity analysts.

2.10. OTHER INFORMATION

None

2.11. POINTS OF CUSTOMER CONTACT

SEKOIA.IO CERT prefers to receive incident reports via e-mail through the email address mentioned in 2.7.
Please use our PGP key to ensure integrity and confidentiality.
In case of emergency, please specify the [URGENT] tag in the subject field in your e-mail.
SEKOIA.IO CERT operates during regular business hours (9:00 AM-7:00 PM from Monday to Friday).

3. CHARTER

3.1. MISSION STATEMENT

The SEKOIA.IO CERT Team's activities are non-profit and fully funded by SEKOIA.IO SAS.

The SEKOIA.IO CERT Team operates as an internal CERT.

The mission of the SEKOIA.IO CERT is to:

- Investigate, respond and coordinate cybersecurity incident that can affect constituency
- Provide cyber threat intelligence report to constituency
- Deploy and maintain tools related to the security incident response
- Maintains relationship with different CERTs

3.2. CONSTITUENCY

Our constituency includes:
- SEKOIA IT system
- SEKOIA digital assets
- SEKOIA.IO solution

3.3. SPONSORSHIP AND/OR AFFILIATION

SEKOIA.IO CERT is a private CERT in the cybersecurity sector. It is owned, operated and financed by SEKOIA.IO SAS

3.4. AUTHORITY

The SEKOIA.IO CERT operates with the authority delegated by the SEKOIA's CEO. The SEKOIA.IO CERT is responsible for coordinating the incident response and investigating artifacts for the Sekoia group's assets.

4. POLICIES

4.1. TYPES OF INCIDENTS AND LEVEL OF SUPPORT

SEKOIA.IO CERT manages all types of cybersecurity incidents that occur, or threaten to occur, within its constituencies.

SEKOIA.IO CERT does not have a formal level of support mapped with incident categories. Upon its authority. SEKOIA.IO will be asked to ensure different tasks depending on the impacted assets.

4.2. CO-OPERATION, INTERACTION AND DISCLOSURE OF INFORMATION

SEKOIA.IO CERT exchanges all necessary non-restricted information with other CERTs / CERTs as well as with other affected parties involved in the incident or incident response process.

Incident or vulnerability related information would not be publicly disclosed without the agreement of all involved parties.

4.3. COMMUNICATION AND AUTHENTICATION

SEKOIA.IO CERT recommends sending all information through encrypted email.
SEKOIA.IO CERT supports the TLP (Traffic Light Protocol) in order to classify information sharing ability.

5. SERVICES

5.1. INCIDENT RESPONSE

The SEKOIA.IO CERT provides the following incident response services:

- Alerts and warnings
- Incident handling
- Incident analysis
- Incident response
- Crisis management
- Incident coordination
- Vulnerability analysis
- Vulnerability coordination
- Forensic analysis

5.1.1. INCIDENT TRIAGE

When an incident is declared to SEKOIA.IO CERT, triage is performed first to assess the seriousness of the impacted assets. Then the incident gets a criticality score. The score can be reviewed during the incident handling and defines the priority of the treatment.

5.1.2. INCIDENT COORDINATION

The incident coordination involves the following services:

- Provide a quick treatment action plan after the incident's detection
- Collection of technical evidence
- Identification of the perimeter impacted by the incident
- Proposition of immediate corrective measures
- Determining the initial cause of the incident

5.1.3. INCIDENT RESOLUTION

At the end of an incident, SEKOIA.IO CERT provides:

- Proposition of long-term corrective measures
- Informal feedback to the team concerned by the incident
- A forensic investigation report, when necessary

5.2. PROACTIVE ACTIVITIES

SEKOIA.IO CERT offers the following proactive activities services:

- Cyber Threat Intelligence
- Threat Hunting
- Technology watch
- Cyber security alerts publication / blogposts
- Knowledge gathering on cyber threat actors

6. INCIDENT REPORTING FORMS

SEKOIA.IO CERT does not have a public incident reporting form.

7. DISCLAIMERS

N/A