RFC 2350 CYBERLOOP CSIRT

CYBERLOOP

Author	Cyberloop
Date	02/02/2024
Version	1.0.0
Classification	**TLP:WHITE**

1 Document Information

This document contains a description of CYBERLOOP CSIRT, according to RFC 23501. It provides basic information about the CYBERLOOP CSIRT team, its channels of communication, its roles, and responsibilities.

1.1 Date of Last Update

Version 1.0.0, 2024/04/02.

1.2 Distribution List for Notifications

There is no distribution list for notifications.

1.3 Locations where this Document May Be Found

The current version of this document can be found at https://cyberloop.it/rfc2350-current.pdf

The digital signature of this document can be found at https://cyberloop.it/rfc2350-current.sig

1.4 Authenticating this Document

This document has been signed with the PGP key of CYBERLOOP CSIRT.

See section 2.8 for more details.

2 Contact Information

2.1 Name of the Team

CYBERLOOP CSIRT

2.2 Address

Viale Mario Angeloni, 437
47521, Cesena (FC), Italy

2.3 Time Zone

CET/CEST

2.4 Telephone Number

None available.

2.5 Facsimile Number

None available.

2.6 Other Telecommunication

None available.

2.7 Electronic Mail Address

The mailbox csirt@cyberloop.it is monitored by the CYBERLOOP CSIRT team.

CYBERLOOP S.R.L.
HQ: Via Mario Angeloni, 437
47521, Cesena (FC), Italy
VAT ID: IT 04502170402
CODE: FC 04502170402

QUALITY ISO 9001
SECURITY ISO 27001
E-MAIL: info@cyberloop.it
WEBSITE: www.cyberloop.it

2.8 Public Keys and Encryption Information

The current CYBERLOOP CSIRT Team has a PGP key, whose fingerprint is 42F7F10A158BA3ECB0EFC1C5EFC8500EA76FBB4B and can be found at: https://cyberloop.it/cyberloop-csirt-publickey.asc

2.9 Team Members

CYBERLOOP CSIRT is operated by Cyberloop srl staff. The team is made up of Cyber Security Consultants, Cyber Analysts and Incident Responders.

2.10 Other Information

None available.

2.11 Points of Customer Contact

The method for contacting the CYBERLOOP CSIRT is via e-mail at csirt@cyberloop.it; e-mail sent to this address are handled by internal Cyberloop staff belonging to the CSIRT team.

3 Charter

3.1 Mission Statement

Cyberloop specializes in a comprehensive range of cybersecurity services designed to enhance organizational security and resilience. Our offerings include Incident Response, proactive Cyber Threat Intelligence, Threat Hunting, Digital Forensics, and Cybersecurity Consultancy and Advisory. These services are tailored to fortify customers protective measures and facilitate robust remediation strategies.

Cyberloop provides services based on two deeply integrated pillars: high human competences and expertise, and advanced technologies based on artificial intelligence to effectively identify anomalies and secure against threats.

Cyberloop is dedicated to fostering a cybersecurity culture that emphasizes the importance of knowledge exchange and information dissemination.

3.2 Constituency

CYBERLOOP CSIRT constituency consists of all the organizations having a defined relationship, partnerships or business with Cyberloop srl.

3.3 Sponsorship and/or Affiliation

-

3.4 Authority

CYBERLOOP CSIRT operates on cybersecurity incidents and handles delivered services for its constituency when agreed.

CYBERLOOP S.R.L.
HQ: Via Mario Angeloni, 437
47521, Cesena (FC), Italy
VAT ID: IT 04502170402
CODE: FC 04502170402

4 Policies

4.1 Types of Incidents and Level of Support

CYBERLOOP CSIRT handles all types of cybersecurity incidents which occur or threaten to occur in its constituency when agreed with constituency members.

4.2 Co-operation, Interaction and Disclosure of Information

CYBERLOOP CSIRT handles the information received with TLP:RED classification by default unless otherwise agreed upon.

4.3 Communication and Authentication

Regular communications that do not contain sensitive data are handled through traditional channels unless otherwise agreed upon.

For communications containing sensitive data, the use of end-to-end encryption via PGP key (see 2.8) or other predetermined encrypted communication methods are recommended.

5 Services

5.1 Incident Response

CYBERLOOP CSIRT provides services to handle, to coordinate and to support its constituency during and after a cyber security incident.

5.1.1 Incident Triage

Investigating occurred incidents and determining the extension and potentials impacts.

5.1.2 Incident Coordination

Determining and coordinating appropriate response actions, facilitating contact and communication to users, third parties and law enforcement.

5.1.3 Incident Resolution

Identifying the initial cause of the incident, collecting evidence, supporting to eradicate the threat, helping to restore the operability, writing incident response reports, informing stakeholders, defining proactive measures and prioritizing them to improve the overall level of cybersecurity.

5.2 Proactive Activities

CYBERLOOP CSIRT gathers information about malware campaigns, threat landscape, exploited vulnerabilities, cybersecurity standards, normative and directive about sensitive data and cyber security laws to better protect and increase security awereness of its constituency.

6 Incident Reporting Forms

To report an incident, it is possible to use an Incident Reporting Forms of your choice or plain text.

7 Disclaimers

While every precaution will be taken in the preparation of information, notifications and alerts, CYBERLOOP CSIRT assumes no responsibility for errors or omissions, or for damages resulting from the use of the information contained within.

CYBERLOOP S.R.L.
HQ: Via Mario Angeloni, 437
47521, Cesena (FC), Italy
VAT ID: IT 04502170402
CODE: FC 04502170402