# RFC 2350 YOROI-CSDC

**Expectations for Computer Security Incident Response**

| | |
|---|---|
| **Title** | RFC 2350 YOROI-CSDC |
| **Document Type** | Specification |
| **Date** | 2018/03/26 |
| **Version** | 1.0 |

Yoroi S.r.l.
Parte del gruppo MAM
www.yoroi.company

Via Santo Stefano 11
40125 Bologna
T 051 0301005
T 02 86882231

Capitale sociale € 50.000 i.v.
Iscr. Reg. Imp, C.F. e P.IVA
03407741200
R.E.A. BO 516975

# 1. Document Information

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

## 1.1. Date of Last Update

Version 1.0 2018/03/26

## 1.2. Distribution List for Notifications

There is no distribution list for public notifications.

## 1.3. Locations where this Document May Be Found

The current version of this document can be found at https://www.yoroi.company/downloads/rfc-2350-yoroi-csdc.pdf .
The digital signature of this document can be found at https://www.yoroi.company/downloads/rfc-2350-yoroi-csdc.sig .

## 1.4 Authenticating this Document

This document has been signed with the PGP key of YOROI-CSDC. See section 2.8 for more details

## 1.5 Document Identification

Title: "RFC 2350 YOROI-CSDC"

Version: 1.0

Document Date: March 2018

Expiration: This document is valid until superseded by a later version

# 2. Contact Information

## 2.1. Name of the Team

YOROI Cyber Security Defence Center Team

Short name : YOROI-CSDC

## 2.2. Address

Yoroi Srl

Piazza Sanguinetti 106

47521 Cesena, FC

## 2.3. Time Zone

Time-zone: CET/CEST

## 2.4 Telephone Number

+39 051 0301005

## 2.5 Facsimile Number

None.

## 2.6 Electronic Mail Address

The mailboxes <cert AT yoroi.company> and <csdc AT yoroi.company> are monitored by the YOROI-CSDC team.

## 2.7 Other Telecommunication

The constituency of the YOROI-CSDC shall communicate with the YOROI Computer Emergency Response Team via the CSDC portal at https://users.yoroi.company/.

## 2.8 Public Keys and Encryption Information

PGP is used for functional exchanges between YOROI-CSDC and its Partners (reports, alerts, intelligence etc).

ID: 0xDAFAA596

Fingerprint: 3833 D721 BD45 7A80 AA48 C94E A6E4 65FE DAFA A596

## 2.9 Team Members

YOROI-CSDC is a CERT for the private sector, communes and non-governmental entities. YOROI-CSDC is operated by Yoroi Srl, a privately-held cyber-security firm. The team is made up of Cyber Security Analyst, Threat Analysts and Incident Responders.

## 2.10 Other Information

## 2.11 Points of Customer Contact

The preferred, unstructured, method to contact YOROI-CSDC team is to send an e-mail to the address <cert AT yoroi.company> or <csdc AT yoroi.company> which are monitored by a duty officer during hours of operation.

Structured Incidents reporting, support and service requests from the constituency of the YOROI-CSDC should be communicated via CSDC portal at https://users.yoroi.company/.

Urgent cases can be reported by phone on +39 051 0301005

# 3. Charter

## 3.1 Mission Statement

YOROI-CSDC's mission is to defend its constituency and support them to protect themselves against national and intentional cyber-attacks that would hamper the integrity of their IT assets and harm the interests of their Organizations. The scope of YOROI-CSDC's activities covers prevention, detection, response and recovery.  YOROI-CSDC operates according to the following key values:

- Highest standards of ethical integrity
- High degree of service orientation and operational readiness
- Effective responsiveness in case of incidents and emergencies and maximum commitment to resolve the issues
- Building on, and complementing the existing capabilities in the constituents
- Facilitating the exchange of good practices between constituents and with peers
- Fostering a culture of openness within a protected environment, operating on a need to know basis

## 3.4 Constituency

The constituency of YOROI-CSDC is composed by all the organization having defined relationship, partnerships or business contracts with Yoroi Srl.

## 3.5 Sponsorship and/or Affiliation

The YOROI-CSDC is an authorized user of the CERT mark and is part of the european CERT/CSIRT community “Trusted Introducer”.


## 3.6 Authority

The YOROI-CSDC is not authoritative. YOROI-CSDC achieve its functions through the services delivered to its constituency, the collaboration with authoritative CERTs, peers, Information Security community, Law Enforcement, Service Providers and Vendors.

# 4. Policies

## 4.1 Types of Incidents and Level of Support

YOROI-CSDC may address and/or may support the handling of all types of computer security incidents which occur, or threaten to occur in its constituency according to contracts, agreements and mandates defined with constituency members.

YOROI-CSDC is committed to keeping its constituency informed about relevant vulnerabilities, emerging threats and trends, and, where possible, it will inform its community of such criticalities before they are actively exploited by threat actors.

## 4.2 Cooperation, Interaction and Disclosure of Information

YOROI-CSDC highly regards the importance of operational cooperation and information-sharing between Computer Emergency Response Teams, and also with other organisations which may contribute towards or make use of their services.

YOROI-CSDC treats all submitted information as TLP:AMBER per default, and will only forward it to concerned parties in order to resolve specific incidents when consent is implicit or expressly given.

YOROI-CSDC shall exchanges all necessary information with other CSIRTs as well as with affected parties' administrators. Neither personal nor overhead data are exchanged unless explicitly authorized.

## 4.3 Communication and Authentication

YOROI-CSDC protects sensitive information in accordance with relevant regulations and policies within the EU.

For regular communication not containing sensitive information YOROI-CSDC may use conventional methods like unencrypted email sent through secured email infrastructures. End-to-end secured communications are handled via PGP-encrypted emails or other agreed means, depending on the sensitivity level and context.

Constituency can securely communicate incidents and related data, support requests or issues to the YOROI-CSDC team via the CSDC portal at https://users.yoroi.company.

# 5. Services

## 5.1 Proactive Services

YOROI-CSDC provides information (e.g. on threat landscape, published vulnerabilities, new attack tools or artefacts, security/protection measures, etc.) needed to protect systems and networks. YOROI-CSDC aims at:

- raise security awareness in its constituency
- publish announcements concerning security threats relevant for its constituency
- observe current trends in technology
- distribute knowledge to the constituency and support cyber security awareness.
- provide and promote information exchange within peers and constituency.
- leverage threat intelligence collected and produced by threat analysts and malware researchers of the YOROI-CSDC to reduce exposure of its constituency.

## 5.2 Incident Response

YOROI-CSDC provides assistance and support to the management of the cyber security incident impacting its constituency offering reactive services such as incident triage, incident coordination, artifact analysis and incident resolution.

### 5.2.1 Incident Triage

Determining whether an incident is authentic, assessing and prioritizing the incident.

### 5.2.2 Incident Coordination

Determine the involved organizations, facilitate contact to other parties which can help resolve the incident, facilitating

contact with other sites which may be involved, facilitating contact with appropriate law enforcement officials, if necessary.

Support for press announcement and/or communication to users. Ensuring adequate threat info-sharing for proactive measures.

### 5.2.2 Incident Resolution

Determining the initial cause of the incident (e.g. vulnerability exploited or attack-vector), advise local security teams on appropriate actions, follow up on the progress of the concerned local security teams. Helping to secure the system involved in the security incident and collect evidence of the incident.

## 6. Incident Reporting Forms

A standard incident reporting form is available to the constituency at https://users.yoroi.company/.

## 7. Disclaimers

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