RFC2350

CERT Orange Cyberdefense

Confidentiality: Public

TLP:WHITE

Version: 2.2

Date: September 1st, 2023

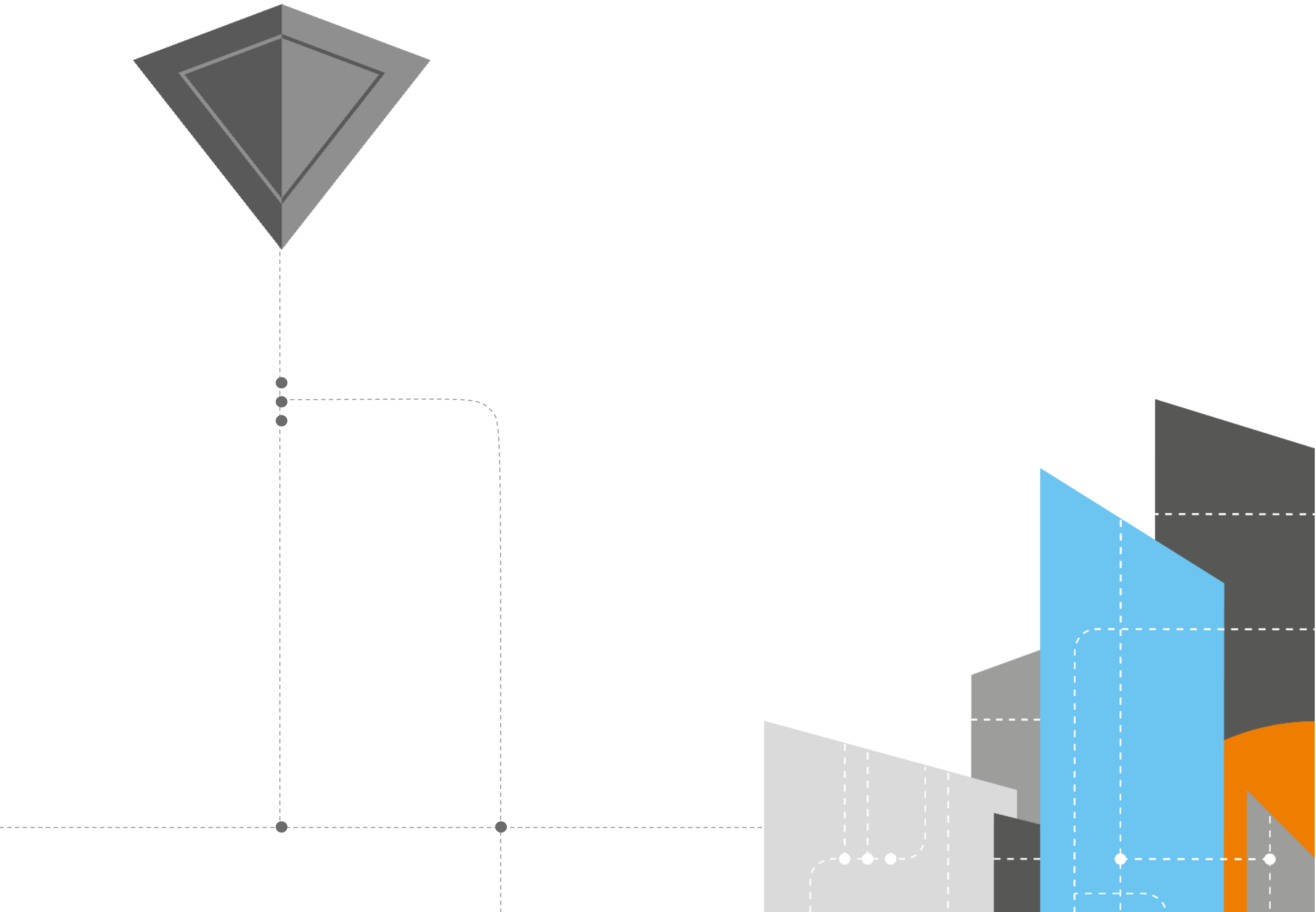

Table of Contents

1 Document Information

This document contains a description of CERT Orange Cyberdefense as implemented by RFC 2350. It provides basic information about our team, its channels of communication, its roles and responsibilities.

1.1 Date of Last Update

August 30th, 2023

1.2 Distribution List for Notifications

No distribution list exists for updates to this document.

1.3 Locations where this Document May Be Found

This document can be found here:

https://orangecyberdefense.com/global/rfc2350/

2 Contact Information

2.1 Name of the Team

CERT Orange Cyberdefense

2.2 Address

CERT Orange Cyberdefense
54, place de l'Ellipse
CS 80094
92983 PARIS LA DEFENSE CEDEX

2.3 Time Zone

Central European Time (UTC+1)

2.4 Telephone Number

+33.810336060 (24/7)

2.5 Facsimile Number

None available

2.6 Other Telecommunication

None

2.7 Electronic Mail Address

cert-contact.ocd[at]orange.com

2.8 Public Keys and Encryption Information

User ID: CERT Orange Cyberdefense <cert-contact.ocd[at]orange.com>

Key ID:	0xBD54B276
Key type:	RSA
Key size:	4096
Expires:	Never
Fingerprint:	8D98 949B 5292 5FA9 B5A4 E75E A77B 7788 BD54 B276

The key and its signatures can be found at the usual large public key servers.

2.9 Team Members

The team consists of IT security experts, able to respond to incidents through their skills in various domains, such as forensics, reverse engineering, threat intelligence, vulnerability research, fraud detection, network analysis, etc.

2.10 Other Information

Information about our supporting host is available at https://orangecyberdefense.com/

2.11 Points of Customer Contact

The preferred communication channel is email, encrypted or not according to your privacy needs, through the email address mentioned in 2.7.

You may also reach us by phone (see 2.4) if need be.

3 Charter

3.1 Mission Statement

CERT Orange Cyberdefense is the department dedicated to Incident Response, Technological Security Monitoring and Cybercrime Prevention within Orange Cyberdefense (a subsidiary of Orange Group)

Located in Europe, Asia and North America, CERT Orange Cyberdefense offers a unique combination of technologies and talents for minimizing Internet-related risks, to all kind of organizations.

3.2 Constituency

Our constituency includes all our clients' organizations.

3.3 Sponsorship and/or Affiliation

CERT Orange Cyberdefense belongs to Orange Cyberdefense (OCD), a fully-owned subsidiary of Orange Group.

3.4 Authority

CERT Orange Cyberdefense operates under the authority of the chief of the Orange Cyberdefense Global Operations unit.

4 Policies

4.1 Types of Incidents and Level of Support

CERT Orange Cyberdefense is able to respond to any kind of IT security incident shared with us. Our team will do everything that is needed to investigate advice, contain, remediate and monitor incidents and advise impacted entities. The level of support provided to our clients depends on their needs and may vary depending on the emergency of the situation and the associated SLAs agreed together.

4.2 Co-operation, Interaction and Disclosure of Information

How is incoming information classified?

All incoming information is classified by default as "internal". If a specific agreement exists, information is handled in accordance with this agreement and classified as "restricted" or "confidential".

What considerations are adopted for the disclosure of information?

"Restricted" or "Confidential" information can only be publicly disclosed with agreement of the involved parties, or on the basis of need to know.

We abide and respect the Information Sharing Traffic Light Protocol (FIRST.org v1) whenever used.

4.3 Communication and Authentication

The clearances for access to "restricted" or "confidential" information are defined either in a specific agreement or by a manager accredited within the team. Information classified as "internal", "restricted" or "confidential" cannot be disclose without authorization from a CERT Orange Cyberdefense manager.

5 Services

5.1 Incident Response

We offer a wide range of reactive services, including:

- Alerts and warnings
- Incident handling
- Incident analysis
- Incident response on site
- Crisis management
- Incident coordination
- Vulnerability handling
- Vulnerability analysis
- Vulnerability response
- Vulnerability coordination
- Forensic analysis
- Active Directory Remediation

More specifically, we can for example conduct threat hunting, malware or post-mortem compromise analysis missions.

5.2 Incident Triage

Following the assessment by Customer's security or exploitation teams of dubious or unusual behavior (unexplained ingress or egress network traffic, outside of working hours authentications, etc.), or after detection of malicious behaviors on Customer’s information system by Customer's teams or a third party, CERT Orange Cyberdefense mobilizes its incident response team to restore trust in the information system.

A first pass triage taking into account the seriousness of the impacted assets, a quick assessment of the threat agent based on internal experience and threat intelligence information, and business context, allows our CSIRT to assign resources and define a first security stance to be followed by our investigators and client internal teams in the following response activities.

5.3 Incident Coordination

The incident response service’s goal is to identify the incident perimeter, the threat agent's means of control on the information system, and advising and setting up means of surveillance and confinement allowing leading remediation operations in the best possible conditions.

In that way, the incident response service includes:

- A quick treatment after the incident’s detection,
- Preliminary assessment of impacted perimeter in collaboration with Customer's personnel,
- Collection of technical evidence,
- Perimeter first pass analysis to validate its relevance,
- Proposition of provisional and/or corrective measures,
- In-depth analysis of the incident to identify the incident causes and the impact extent

These actions are materialized by the following deliverables:

- A preliminary analysis report returned 5 working days at the latest after the evidence collection, including:
- The first findings,
- The urgent confinement actions,
- The project’s next milestones.
- A forensic investigation report, including:
- A detailed chronology of the incident’s events
- The compromise indicators linked with the incident
- The intelligence elements linked with the threat agents
- An action plan to restore the nominal situation and avoid an incident reproduction
- A managerial report mentioning the key assessments to bring a context to the risks associated with the incident and action plan,
- The evidence collected, and analysis work products.

Preliminary restitution

A preliminary restitution is delivered during the intervention. It aims at giving an immediate visibility on the conclusions of the ongoing investigation. It will be materialized five working days at the latest after acquiring evidence elements by a preliminary analysis report. It aims at giving an immediate visibility on the investigation status and the first observations.

Project follow-up

During the whole intervention phase, and for cases where it would last over a week, a project follow-up will be led by Orange Cyberdefense’s teams for the client in the form of a weekly report sent to a contact identified at the project initiation. This weekly report includes an investigation activities progress report, a possible reminder of alerts sent during the week, a consumed charges follow-up, and the activities scheduled for the following week.

5.4 Incident Resolution

Our CSIRT team relies on a methodical approach, tried and tested during numerous incident expertise missions. This method is based on defining a restricted perimeter (the one impacted by the incident), and then progressively extending the perimeter according to the information collected and the analysis led by the experts. This cycle is repeated until reaching an exhaustive knowledge of the incident.

The conclusion phase consists in:

- Securing data linked with the intervention, depending on the type of data and your choices (restoration, destruction or storage)
- Giving a feedback in order to strengthen Customer's internal knowledge and identifying areas of progress ;
- Providing you with a forensic investigation report.

5.5 Proactive Activities

We provide numerous proactive services, such as:

- Announcements
- Technology watch
- Security audits/assessments
- Adoption of security tools
- Development of security tools
- Intrusion detection services
- Security awareness raising

We also do have security quality management activities, including:

- Risk analysis
- Disaster recovery
- Security consulting
- Awareness building
- Education/training
- Product evaluation

6 Incident Reporting Forms

No form is available to report incidents to us. But you may contact Orange Cyberdefense through the form available here:

https://orangecyberdefense.com/global/contact/

7 Disclaimers

While every precaution will be taken in the preparation of information, notifications and alerts, CERT Orange Cyberdefense assumes no responsibility for errors or omissions, or for damages resulting from the use of the information it provides