TEHTRIS CERT – RFC 2350

1 Document information ........................................................................................................ 2
  1.1 Date of Last Update ........................................................................................................ 2
  1.2 Distribution List for Notifications .............................................................................. 2
  1.3 Locations where this Document May Be Found .......................................................... 2
  1.4 Authenticating this Document ..................................................................................... 2

2 Contact Information .............................................................................................................. 3
  2.1 Name of the Team .......................................................................................................... 3
  2.2 Address .......................................................................................................................... 3
  2.3 Timezone ....................................................................................................................... 3
  2.4 Telephone Number ....................................................................................................... 3
  2.5 Facsimile Number ......................................................................................................... 3
  2.6 Other means for communication .................................................................................. 3
  2.7 Electronic Mail Address .................................................................................................. 4
  2.8 Public Keys and Other Encryption Information .......................................................... 4
  2.9 Team Members ............................................................................................................. 4
  2.10 Other Information ......................................................................................................... 4
  2.11 Points of Customer Contact ........................................................................................ 4

3 Charter .................................................................................................................................. 5
  3.1 Mission Statement .......................................................................................................... 5
  3.2 Constituency ................................................................................................................... 5
  3.3 Sponsorship and/or Affiliation ...................................................................................... 5
  3.4 Authority ......................................................................................................................... 5

4 Policies .................................................................................................................................. 6
  4.1 Type of Incidents and Level of Support ......................................................................... 6
  4.2 Co-operation, Interaction and Disclosure of Information ............................................... 6
  4.3 Communication and Authentication ............................................................................. 6

5 Services ................................................................................................................................. 7
  5.1 Pre-emptive Security Measures ..................................................................................... 7
  5.2 Incident Response ........................................................................................................... 7
  5.3 Proactive Activities ........................................................................................................... 8

6 Incident Reporting Forms .................................................................................................... 9

7 Disclaimer .............................................................................................................................. 10
1 Document information

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

1.1 Date of Last Update

Version 1.4 2020/02/16 update 2020

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 CERT description may be found at https://tehtris.com/en/services/cert/

1.4 Authenticating this Document

This document has been signed with the PGP key of TEHTRIS CERT. The signature of this document is available at https://tehtris.com/en/services/cert/
2 Contact Information

2.1 Name of the Team
TEHTRIS CERT

2.2 Address
TEHTRIS CERT
13-15 rue Taitbout
75009, PARIS
FRANCE

2.3 Timezone
CET (From October to March, UTC+1)
CEST (From March to October, UTC+2)

2.4 Telephone Number
Phone: +33 (0) 9-72-50-80-33 [inputs are filtered, but all messages are monitored]

2.5 Facsimile Number
Fax: +33 (0) 1-72-71-25-99

2.6 Other means for communication
Twitter: @tehtris
2.7 Electronic Mail Address

cert (at) tehtris (dot) com
This is a mail alias that relays mail to the human(s) on duty for the TEHTRIS CERT.

2.8 Public Keys and Other Encryption Information

TEHTRIS CERT is using the following PGP key for its email exchanges with cert (at) tehtris (dot) com address:
- ID: 19C7 677A AB9A 85E6
- Fingerprint: A1F2 9BA1 2811 4E68 043C 07C5 19C7 677A AB9A 85E6

2.9 Team Members

Winston DELBEY is the current TEHTRIS CERT leader.

Other members of this CERT team are some TEHTRIS security experts and consultants.

2.10 Other Information

None

2.11 Points of Customer Contact

The preferred method to contact TEHTRIS CERT is to send e-mail to the cert (at) tehtris (dot) com address.

This mailbox is monitored actively during hours of operations.

Standard hours of operations:
  7h00 - 22h00 from Monday to Friday
  8h00 - 20h00 on Weekends

The mailbox is monitored 365 days / 365.
3 Charter

3.1 Mission Statement
The missions of TEHTRIS CERT are
i) to assist our customers and our partners community in implementing proactive measures to reduce the risks of computer security incidents
ii) to assist our customers and our partners community in responding to such incidents when they occur
iii) to contribute to worldwide community by sharing valuable information such as cyber threat intelligence, and by helping at fighting against cyber threats through multiple means

3.2 Constituency
TEHTRIS CERT constituency is composed of all the customers and partners of the TEHTRIS solutions, such as the global TEHTRIS XDR Platform, who subscribed a related Service Level Agreement support contract.

3.3 Sponsorship and/or Affiliation
TEHTRIS CERT is part of TEHTRIS Company. TEHTRIS CERT maintains relationships with various CERT/CSIRT teams throughout the world, on all continents, on an as-needed basis.

3.4 Authority
TEHTRIS CERT aims at handling incident response for customers and partners perimeters. Thus, TEHTRIS CERT has an advisory role with local security teams and has no specific authority to require any specific action. The recommendations, provided by TEHTRIS CERT to its customers and partners, will be implemented under the direction of the related stakeholders.
4 Policies

4.1 Type of Incidents and Level of Support

TEHTRIS CERT is generally contacted by its customers or partners to handle any type of incidents occurring on its own perimeter. Depending on the type of security incident, TEHTRIS CERT will gradually roll out its services, which includes incident response and digital forensics.

4.2 Co-operation, Interaction and Disclosure of Information

TEHTRIS CERT operates under the restrictions imposed by French laws.

All information exchanged with customers or partners during an incident (and after its resolution) will be handled confidentially in secure environments using encryption if necessary.

TEHTRIS CERT will cooperate with other Organizations in the Field of Computer Security, which may help to deliver its services, especially for incident resolution. In any such exchange, TEHTRIS CERT will protect the privacy of its customers through anonymization of technical data that may be exchanged. Customers will be informed of such exchanges.

If customers or partners object the default TEHTRIS CERT behavior, it should be specified in initial contractual agreement or explicitly asked in the communication with TEHTRIS CERT. Requiring specific behavior may lower the quality of assistance TEHTRIS CERT may provide, depending on the content of the related contracts and SLA subscribed.

4.3 Communication and Authentication

For normal communication without any sensitive information, unencrypted e-mail may be used but TEHTRIS CERT strongly encourages customers and partners to use encrypted email (through OpenPGP) to exchange data with TEHTRIS CERT.
5 Services

5.1 Pre-emptive Security Measures

As the TEHTRIS CERT services are mainly delivered to TEHTRIS customers and partners, TEHTRIS CERT will implement or provide information to TEHTRIS XDR Platform developers, any technical security measures that may help to detect or block security threats, including emerging ones, especially for honeypots, EDR, EPP, NIDS, SIEM, SOAR, CTI, etc.

5.2 Incident Response

TEHTRIS CERT is usually mandated, by its customers and partners, to be responsible for the coordination of security incidents somehow involving customers and partners perimeters. The technical resolution of incident might be operationally left to some local administrators working with TEHTRIS customers and partners, linked to TEHTRIS CERT support, depending on the situation.

Without being exhaustive, following aspects are covered by TEHTRIS CERT:

- 5.2.1 Incident Triage
  - Investigating whether indeed an incident occurred
  - Determining the extent of the incident.

- 5.2.2 Incident Coordination
  - Determining the initial cause of the incident (vulnerability exploited).
  - Facilitating contact with other sites, that may be involved.
  - Facilitating contact with appropriate law enforcement officials, if necessary.
  - Making reports to other CERT/CSIRT teams.
  - Composing announcements to users, if applicable.
5.2.3 Incident Resolution

- Providing action plan to remove the vulnerability and supporting local administrators to perform the action plan.
- Providing action plan and support to help securing the system from the effects of the incident.
- Evaluating whether certain actions are likely to reap results in proportion to their cost and risk.
- Providing action plan and support to collect any evidence after the fact in order to be used in criminal prosecution or any disciplinary action.

5.3 Proactive Activities

TEHTRIS CERT performs the following proactive activities:
- Technology watch
- Intrusion detection
- Development of security tools
- Information about major security threats or vulnerabilities to its customers
- Training on security topics
6 Incident Reporting Forms

No public form is proposed on our web site, to report incidents to TEHTRIS CERT, but you can directly use the email contact with proper information when needed. TEHTRIS XDR Platform subscribers can use internal tools through the TEHTRIS XDR Unified Console, in order to share events and needed information.

In case of emergency or crisis, please provide to TEHTRIS CERT at least the following information:

- Contact details and organizational information: name of person and organization name and address, email address, telephone number;
- IP address(es), FQDN(s), and any other relevant technical element with associated observation;
- Scanning results (if any) and/or any extract from the log showing the problem;
7 Disclaimer

While every precautionary measures will be taken in the preparation of information, notifications and alerts, TEHTRIS CERT assumes no responsibility for errors or omissions, or for direct and indirect damages resulting from the use of the information contained within.