CSIRT Description for **REDTEAM.PL CERT**

1. About this document

This document contains a description of REDTEAM.PL CERT according to RFC 2350. It provides basic information about the CERT, the ways it can be contacted, describes its responsibilities and the services offered.

1.1 Date of Last Update

This is version 1.1, published on 23 October 2020.

1.2 Distribution List for Notifications

This profile is kept up-to-date on the location specified in 1.3.
Notifications of updates are submitted to *Trusted Introducer*.

1.3 Locations where this Document May Be Found

The current version of this CSIRT description document is available at REDTEAM.PL website at: https://redteam.pl/rfc2350.pdf

Signature for this document is available at:
https://redteam.pl/rfc2350.pdf.sig

Please make sure you are using the latest version.

1.4 Authenticating this Document

This document has been signed with PGP key and its authenticity can be verified using REDTEAM.PL CERT key as published in 2.8.

2. Contact Information

2.1 Name of the Team

Full name: REDTEAM.PL CERT
Short name: REDTEAM.PL

2.2 Address

RED TEAM Sp. z o.o. Sp.k.
Chmielna 2/31
00-020 Warsaw
Poland

2.3 Time Zone

Europe/Warsaw
Central European Summer Time (CEST) – UTC +2

Central European Time (CET) – UTC +1

2.4 Telephone Number

Unavailable as initial contact method.

2.5 Facsimile Number

Fax is not available.

2.6 Other Telecommunication

None available.

2.7 Electronic Mail Address

cert@redteam.pl

2.8 Public Keys and Other Encryption Information

```
User ID:      REDTEAM.PL CERT <cert@redteam.pl>
Fingerprint:  4DD0 B30C 4205 89AB 456F 7EC9 6425 548F 73FF 61DE
```

This key can be retrieved from directory servers or directly from REDTEAM.PL website: https://redteam.pl/pgp/cert-redteam-pl.asc

2.9 Team Members

No information is provided about the REDTEAM.PL CERT team members in public.

2.10 Other Information

General information about REDTEAM.PL cyber security services can be found at: https://redteam.pl

Information about REDTEAM.PL CERT and SOC services can be found at: https://soc.redteam.pl

2.11 Points of Customer Contact

The preferred method for contacting REDTEAM.PL CERT is e-mail cert@redteam.pl

3. Charter

3.1 Mission Statement

REDTEAM.PL is a private company providing professional cyber security services, which includes i.a. digital forensics, incident response (DFIR) and IT Expert Witness opinions.

REDTEAM.PL CERT delivers CSIRT and SOC services to private and government organisations.

REDTEAM.PL in accordance to Polish law can cooperate with law enforcement agencies and the judiciary as an IT Expert Witness. Therefore can secure digital evidence, perform analyzes and opinions for criminal proceedings in the case of cyber crime.

REDTEAM.PL provides non-profit information such as APT attacks analysis and security research which is intended to help CSIRTs in fighting cyber crime. This kind of information is publicly available on our techblog at: https://blog.redteam.pl

3.2 Constituency

Our constituency consists of the organisation who signed an agreement to use our incident response services.

3.3 Sponsorship and/or Affiliation

REDTEAM.PL is a private, self-funding entity.

REDTEAM.PL CERT is affiliated within the *Trusted Introducer*, details can be found at: https://www.trusted-introducer.org/directory/teams/redteampl.html

3.4 Authority

REDTEAM.PL CERT handles and coordinates incidents on behalf of its customers and is bound by contractual terms. REDTEAM.PL however is regularly expected to make recommendations during the incident handling process where parties affected are not REDTEAM.PL's customers.

4. Policies

4.1 Types of Incidents and Level of Support

All incidents are considered normal priority unless they are labeled otherwise.

4.2 Co-operation, Interaction and Disclosure of Information

ALL incoming information is handled confidentially by REDTEAM.PL CERT, regardless of its priority.

REDTEAM.PL CERT respects EthicsfIRST[1] and supports the Information Sharing Traffic Light Protocol[2] (ISTLP, TLP) – information that comes in with the tags WHITE, GREEN, AMBER or RED will be handled appropriately.

[1] https://ethicsfirst.org
[2] https://www.trusted-introducer.org/ISTLPv11.pdf

4.3 Communication and Authentication

Usage of PGP in all cases where sensitive information is involved is highly recommended.
REDTEAM.PL CERT PGP key is provided in 2.8.

5. Services

REDTEAM.PL offers a wide range of cyber security services.
Detailed descriptions are available on REDTEAM.PL websites:
https://redteam.pl
https://soc.redteam.pl

5.1 Incident Response

REDTEAM.PL CERT offers incident response and digital forensics services which includes but are not limited to securing evidence and forensics analysis after security incidents.

5.2 Proactive Activities

REDTEAM.PL CERT provides various CSIRT and SOC services such as threat hunting and threat intelligence.

6. Incident Reporting Forms

There are no specific forms developed for reporting incidents to REDTEAM.PL CERT.
Incidents should be reported to the e-mail address provided in 2.7.

7. Disclaimers

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