RFC 2350 Description

Atos Czech Republic SOC-CERT team (Eviden SOC-CERT (CZ))

Document version: 1.0 | Date: 2026-07-07

1. Document Information

This document describes the Atos Czech Republic SOC-CERT team ("the Team") according to RFC 2350.

1.1 Date of Last Update

Version 1.0 — 2026-07-07

1.2 Distribution List for Notifications

None. Questions regarding updates of this document should be addressed to the Team's e-mail address (see 2.7).

1.3 Locations where this Document May Be Found

The current version of this document is available from the Team upon request via e-mail (see 2.7).

1.4 Authenticating This Document

This document is published as a PDF signed with a qualified electronic signature. The plain-text version signed with the Team's PGP key (see section 2.8) is available on request.

2. Contact Information

2.1 Name of the Team

Official name: Atos Czech Republic SOC-CERT team Short name: Eviden SOC-CERT (CZ)

2.2 Address

Eviden Czech Republic s.r.o. SOC-CERT team Doudlebska 1699/5 140 00 Praha 4 Czech Republic

2.3 Time Zone

Europe/Prague (CET, UTC+1; CEST, UTC+2 during daylight saving time)

2.4 Telephone Number

+420 604 290 196

2.5 Facsimile Number

None.

2.6 Other Telecommunication

None.

2.7 Electronic Mail Address

dl-cz-soc@atos.net

This address is used both for general contact and for incident reports.

2.8 Public Keys and Encryption Information

The Team uses the following PGP key:

```
Type:   RSA/4096    Expires: 2030-07-13
Fpr:    9388 B128 6232 087B D9BA 72C6 E449 74FD 3957 A219
Sub:    RSA/4096  Usage: Encrypt  Expires: 2030-07-13
UID:    Atos CZ SOC <dl-cz-soc@atos.net>
```

The key is available in the Trusted Introducer directory entry of the Team.

2.9 Team Members

Team Leader: Adam Kapala

Team Representatives (Trusted Introducer):

• Petr N■mec

• Adam Kapala

The full list of team members is not publicly disclosed.

2.10 Other Information

General information about the Team can be found in the Trusted Introducer directory: https://www.trusted-introducer.org/directory/

2.11 Points of Customer Contact

The preferred method for contacting the Team is via e-mail at dl-cz-soc@atos.net. Incident reports containing sensitive information should be encrypted using the Team's PGP key (see 2.8).

The Team operates during regular business hours only: Monday to Friday, 09:00–17:00 (Europe/Prague).

3. Charter

3.1 Mission Statement

The mission of the Atos Czech Republic SOC-CERT team is to support the security of the information and communication infrastructure of Eviden Czech Republic s.r.o. by preventing, detecting, and responding to information security incidents, and by coordinating their resolution within its constituency.

3.2 Constituency

The constituency of the Team is Eviden Czech Republic s.r.o., including its internal information and communication infrastructure:

• Domains: *.atos.net

Constituency type: Commercial Organisation.

3.3 Sponsorship and/or Affiliation

The Team is an organisational unit of Eviden Czech Republic s.r.o., a member of the Atos Group (the legal entity name Eviden Czech Republic s.r.o. remains in effect until its planned change to Atos Czech Republic s.r.o.).

3.4 Authority

The Team operates under the authority and mandate of the Security Director of Eviden Czech Republic s.r.o., Tomáš Hlavsa. Within its constituency, the Team is authorised to coordinate the handling of information security incidents and to issue related recommendations.

4. Policies

4.1 Types of Incidents and Level of Support

The Team addresses all types of information security incidents which occur, or threaten to occur, within its constituency.

The level of support depends on the type and severity of the incident, the size of the affected user community, and the Team's resources at the time. Incidents are prioritised according to their severity and potential impact.

4.2 Co-operation, Interaction, and Disclosure of Information

The Team cooperates with other CSIRT/SOC teams and relevant authorities as needed. All information received in connection with an incident is treated as confidential and is shared with third parties only on a need-to-know basis and in accordance with applicable legal and regulatory requirements, including the GDPR.

The Team supports the use of the Traffic Light Protocol (TLP); information received with TLP markings is handled accordingly.

4.3 Communication and Authentication

For ordinary communication, unencrypted e-mail and telephone are considered sufficient. For sensitive information, PGP-encrypted e-mail is the preferred method (see 2.8). Where appropriate, the identity of communication partners is verified using the Trusted Introducer directory or other trusted channels.

5. Services

5.1 Incident Response

The Team provides the following reactive services to its constituency:

• Receipt and triage of incident reports

• Incident analysis and coordination of incident resolution

• Support of incident recovery

5.2 Proactive Activities

The Team provides the following proactive services:

• Security monitoring of the constituency's infrastructure

• Issuing of security advisories and warnings to the constituency

• Consultancy and support in the area of system hardening

6. Incident Reporting Forms

No specific incident reporting form is used. Incidents should be reported via e-mail to dl-cz-soc@atos.net, including, where possible, a description of the incident, affected systems, timestamps, and relevant logs. Sensitive reports should be encrypted (see 2.8).

7. Disclaimers

While every precaution is taken in the preparation of information, notifications, and alerts, the Atos Czech Republic SOC-CERT team assumes no responsibility for errors or omissions, or for damages resulting from the use of the information contained within.

Tomas Hlavsa

Digitally signed by Tomas Hlavsa
Date: 2026.08.12 11:40:24 +02'00'