
CSIRT DESCRIPTION

RFC 2350

EXE-SOC Security Operations Centre

Formal public description of EXE-SOC in accordance with RFC 2350, Expectations for Computer Security Incident Response.

ISSUE DATE

30/09/2026

VERSION

1.0

PROJECT ID

101128063

STATUS

Approved



Funded by
the European Union

Funded by the European Union. Views and opinions expressed are however those of the author(s) only and do not necessarily reflect those of the European Union. The European Union cannot be held responsible for them.

DOCUMENT INFORMATION

INFORMATION	
Project name	EXE Security Operations Centre
Project ID	101128063
Issue date	30/09/2026
File name	RFC2350 - EXE-SOC CSIRT Description.pdf
Document version	1.0
WP / Task	WP5 / Task 5.2 – RFC2350 publication
Document status	Approved

DOCUMENT APPROVALS

APPROVING AUTHORITY	NAME AND ROLE	DATE
Steering Committee	Richard Hrabovský, chairman of the Steering Committee	30/09/2026

EXE-SOC CSIRT Description according to RFC 2350

This document provides a formal public description of EXE-SOC in accordance with RFC 2350, Expectations for Computer Security Incident Response. It defines the team contact information, constituency, authority, incident-handling policies, services and incident-reporting arrangements.

1. Document Information

FIELD	INFORMATION
1.1 Date of Last Update	Version 1.0, 30 September 2026.
1.2 Distribution List for Notifications	No dedicated public distribution list is used. Changes will be reflected in the current version published on the EXE-SOC website.
1.3 Location of this Document	The current version is intended for publication at https://exesoc.sk . Users should verify that they are consulting the latest published version.
1.4 Authenticating this Document	The document may be authenticated by the EXE-SOC team PGP key specified in section 2.8.

2. Contact Information

FIELD	INFORMATION
2.1 Name of the Team	EXE-SOC Security Operations Centre Short name: EXE-SOC
2.2 Address	EXE-SOC exe, a.s. GBC V, Galvaniho 19 821 04 Bratislava Slovakia
2.3 Time Zone	Europe/Bratislava – CET/CEST
2.4 Telephone Number	Main phone: +421 917 930 945 Emergency phone: +421 917 930 945
2.5 Facsimile Number	Not used.
2.6 Other Telecommunication	Microsoft Teams and other agreed secure collaboration channels may be used with customers and partners.

2.7 Electronic Mail Address	Public team email: soc@exe.sk Restricted team email: incidents@exe.sk Reaction test email: incidents@exe.sk Security notification emails: incidents@exe.sk ; soc@exe.sk ; soc@exe.cz ; exesoc@exe.cz ; exesoc@exe.sk
2.8 Public Keys and Encryption Information	EXE-SOC uses a team PGP key for main communication. Primary fingerprint: D5C7 CB33 D034 C0F7 728E 8592 17BD 0EE9 DE61 6EDD User ID: Exe SOC < soc@exesoc.sk >
2.9 Team Members	A complete list of team members is not publicly disclosed. Authorised personnel identify themselves when required for incident handling or coordination.
2.10 Other Information	Public website: https://exesoc.sk FTP: not used Mailing list: not used Usenet: not used
2.11 Points of Customer Contact	Regular business hours: Monday–Friday, 08:00–17:00 CET/CEST. Outside business hours: on-call support and incident escalation are available through emergency contact channels.

2.12 Team Representatives

FIELD	INFORMATION
Representative 1	Miroslav Dilský Team representative miroslav.dilsky@exe.sk +421 917 930 945
Representative 2	Miroslav Pikus Team representative miroslav.pikus@accura.io +421 903 786 603

2.13 Team Registration Details

FIELD	INFORMATION
Host organisation	exe, a.s.
Country	Slovakia

Additional country	Czech Republic
Established on	31 January 2026
Team type	Commercial Security Operations Centre (SOC)
MISP organisation	N/A

3. Charter

3.1 Mission Statement

EXE-SOC is a Security Operations Centre operated by exe, a.s. The team provides security monitoring, threat detection, incident-handling support and cybersecurity advisory services to organisations under contractual agreements with exe, a.s. EXE-SOC uses modern security technologies, automation and AI-assisted analytical capabilities to support security operations and incident investigation.

3.2 Constituency

Formal constituency: EXE-SOC provides security monitoring, threat detection, incident-handling support and cybersecurity advisory services to organisations under contractual agreements with exe, a.s.

Informal constituency: EXE-SOC cooperates with selected cybersecurity partners and communities on knowledge sharing and cybersecurity-related topics.

Location of constituency members: Slovakia, Czech Republic and the European Union.

3.3 Constituency Network

FIELD	INFORMATION
Domain names	exesoc.sk *.exesoc.sk exe.sk *.exe.sk exe.cz *.exe.cz
AS Numbers	N/A
Security notification IP range	84.16.33.161/28
Security notification AS Numbers	N/A

3.4 Sponsoring Organisation / Affiliation

EXE-SOC is operated and sponsored by exe, a.s., Slovakia. EXE-SOC was established within Project 101128063 under the Digital Europe Programme and continues as an operational capability of exe, a.s.

3.5 Authority

EXE-SOC operates under the authority and governance of exe, a.s. For customer environments, EXE-SOC authority is limited to permissions, responsibilities, service boundaries and escalation arrangements defined in the applicable contract and customer-specific operating documentation. Direct changes to customer systems are performed only where explicitly authorised.

4. Policies

4.1 Types of Incidents and Level of Support

EXE-SOC supports security events and incidents affecting its formal constituency and falling within the agreed service scope. These may include:

- phishing and business-email compromise;
- malware and ransomware;
- identity, authentication and privilege misuse;
- suspicious endpoint, server, cloud or network activity;
- unauthorised access and account compromise;
- data-movement and potential data-loss events;
- denial-of-service and availability-related events;
- insider-threat indicators; and
- other incidents covered by customer-specific monitoring and response procedures.

The level and priority of support depend on severity, potential impact, available evidence, service scope and contractual arrangements. EXE-SOC may involve specialised experts or cooperate with external teams and authorities where required.

4.2 Co-operation, Interaction and Disclosure of Information

EXE-SOC cooperates with customers, internal support teams, peer CSIRT/SOC teams, technology providers, cybersecurity communities and competent authorities as appropriate. Information is shared on a need-to-know and least-disclosure basis, considering contractual obligations, confidentiality, personal-data protection, applicable law, information classification and incident sensitivity. EXE-SOC respects applicable Traffic Light Protocol markings.

4.3 Communication and Authentication

Email is the primary communication method. Telephone and agreed collaboration channels may be used for coordination. PGP/GnuPG should be used for sensitive information exchanged with external parties. Where necessary, identities or instructions may be verified through a second communication channel or known customer and peer-team contacts.

5. Services

EXE-SOC provides services in accordance with its service catalogue, operational framework and customer-specific agreements. Detailed service levels are defined separately for each customer.

5.1 Incident Response

EXE-SOC supports incident response through monitoring, triage, investigation, coordination, communication, reporting and recommendations. The precise response authority depends on the internal mandate or customer agreement.

5.1.1 Incident Triage

- receive or detect a security event or incident report;
- verify relevance and available evidence;
- classify severity and potential impact;
- enrich the case with available identity, endpoint, server, cloud, network and threat-intelligence context;
- identify ownership and escalation paths; and
- document the initial assessment and next action.

5.1.2 Incident Coordination

- coordinate analysis across EXE-SOC roles and specialist teams;
- notify authorised customer or internal contacts;
- facilitate cooperation with peer teams, providers or authorities;
- maintain communication, ownership and audit trail;
- provide response and mitigation recommendations; and
- escalate according to severity and customer procedures.

5.1.3 Incident Resolution

- support containment, eradication and recovery planning within EXE-SOC authority;
- record actions, evidence, findings and decisions;
- confirm closure criteria with the responsible owner;
- prepare operational or management reporting; and
- capture lessons learned and follow-up actions.

5.2 Proactive Activities

- security monitoring and detection engineering;
- centralised log management and telemetry onboarding;
- development and tuning of detections and alert thresholds;
- threat-intelligence and indicator-of-compromise handling;
- security reporting and recommendations;
- customer readiness and telemetry-gap assessment;
- support for SOC design, implementation, operation or migration;
- cybersecurity consulting, awareness and knowledge transfer;
- testing of processes, playbooks and automation; and
- continuous improvement based on operational findings, tests, audits and reviews.

Specialised services such as vulnerability assessment, penetration testing, advanced threat hunting or malware analysis are provided only where formally introduced, appropriately resourced and included in the relevant agreement.

6. Incident Reporting Form

Incidents should be reported to **incidents@exe.sk**. Reports should include, where available and appropriate:

- reporter name, organisation and reliable contact details;
- affected organisation, service, system, account, asset, IP address or domain;
- date and time of detection, including time zone;
- description of the event or incident;
- known or suspected impact and current status;
- relevant indicators, logs, screenshots, message headers or other evidence;
- actions already taken;
- other organisations already contacted;
- handling restrictions, confidentiality requirements and TLP marking; and
- the assistance requested from EXE-SOC.

Reporters should not send passwords, private keys or unnecessary personal data. Sensitive attachments should be encrypted using the EXE-SOC public key. If email is unavailable or inappropriate, the emergency telephone number may be used.

7. Disclaimers

EXE-SOC takes reasonable care in preparing analyses, notifications, recommendations and public information. Cybersecurity information may be incomplete, time-sensitive or dependent on the telemetry and context available at the time of analysis. EXE-SOC does not warrant that its information will identify or prevent every threat or incident.

Services are provided within the applicable mandate, agreement, service scope, available evidence and legal or regulatory constraints. Customers and recipients remain responsible for business decisions, system ownership and actions outside EXE-SOC authority. Contractual liability is governed by the applicable agreement; this public description does not create additional contractual obligations.

A. Appendix – Document Control

FIELD	INFORMATION
Document owner	EXE-SOC / exe, a.s.
Publication location	https://exesoc.sk
Review frequency	At least annually and after material changes to contacts, constituency, authority, services or policies.
Public contact	soc@exe.sk
Incident contact	incidents@exe.sk
Related TI process	Trusted Introducer Listing application