GLOBAL SECURITY OPERATIONS CENTER (GSOC)

RFC 2350 Team Documentation

Date	December 14th 2023
Sensitivity	CLEAR
Contact	Yannick Callewaert
E-mail	soc@exclusive-networks.com
Version	0.3

Table of Contents

1 Information about this Document

1.1 About this document

This document contains all formal descriptions related to the Exclusive Networks Global SOC (EXN-GSOC), based on RFC 2350.

1.2 Document Version History

Version	Date	Authors	Notes
0.1	20th of July 2022	Andy De Petter	Initial Draft
0.2	1st of December 2023	Yannick Callewaert	Update
0.3	14th of December	Yannick Callewaert	Update

1.3 Distribution List for Notifications

The Exclusive Networks Global SOC can be reached through a shared mailbox at soc@exclusive-networks.com.

2 Contact

2.1 Team Name

EXN-GSOC – Exclusive Networks Global SOC

2.2 Post Address

Yannick Callewaert
A. Stockletlaan 202
B-2570 Duffel
Belgium

2.3 Time zone

The Global SOC operates primarily in GMT+1 (Central European Time, Europe/Brussels)

2.4 Telephone Number

+32 496 728977

2.5 E-mail

soc@exclusive-networks.com

2.6 Public keys and encryption

General contact e-mail address: soc@exclusive-networks.com
Key ID: **0x33AF1CF9**
Fingerprint: **BC5D 229E 1CA4 4066 BB45 94B1 0233 16E0 33AF 1CF9**

2.7 Team members

- Yannick Callewaert (Primary Representative)
  ycallewaert@exclusive-networks.com (regular)
  yannick@theforce.exclusive-networks.com (PGP secured)
  Key ID: **0x030CBCE1**
  Fingerprint: **DD7B BF1D 1CCF CCD5 A7D0 4D22 BE82 2ABC 030C BCE1**

- Pieter-Jan Blaton
  pblaton@exclusive-networks.com (regular)
  pblaton@theforce.exclusive-networks.com (PGP secured)
  Key ID: **0x9BF7C44E**
  Fingerprint: **78D0 AAAD B2BD 7F4F 477C 4EBB FD2F 94D0 9BF7 C44E**

- Martika Rashidi
  mrashidi@exclusive-networks.com (regular)
  martika@theforce.exclusive-networks.com (PGP secured)
  Key ID: **0x942D0893**
  Fingerprint: **5E6B 65EA 76E2 A8BC A1E7 7207 84D3 7FE8 942D 0893**

2.8 Other information

Not available.

2.9 Point of contact

The default way to contact the EXN-SOC is through e-mail at soc@exclusive-networks.com. For telephone contact, the primary team representative can be contacted directly on mobile. The Global SOC works during extended business hours: 07am – 7pm.

3 Charter

3.1 Mission Statement

The GSOC is the central security incident monitoring and response team of Exclusive Networks Group. Its mission is to monitor the corporate infrastructure – both centrally as distributed - for security incidents and breaches and to respond efficiently to such incidents when they occur.

3.2 Constituency

The constituency of the EXN-GSOC is Exclusive Networks as a Commercial Organization: all employees, contractors within the Exclusive Networks Group worldwide.
The constituency is geographically spread, as Exclusive Networks has offices in 45+ countries.
The Exclusive Networks Global GSOC is intervening for all cyber security incidents (including vulnerabilities) that occur on managed infrastructure (workstations, IT and network infrastructure).
The GSOC does not offer services to customers of Exclusive Networks or of its subsidiaries.

3.3 Sponsorship and/or Affiliation

With an explicit mandate endorsed by the CISO/CTO, the GSOC has full authority to implement corrective controls in order to immediately mitigate the impact of a security incident.

3.4 Authority

The Exclusive Networks Global GSOC is intervening for all cyber security incidents ,including vulnerabilities, which occur on managed infrastructure (workstations, IT and network infrastructure).

4 Policies

4.1 Types of incident and level of support

All incidents are classified based on severity and category. For Exclusive Networks employees we refer to the internal SharePoint page.
In case you need to report an issue or an incident as a business partner, please contact your Exclusive Networks representative through the known communication channels.
If you are a CSIRT or SOC you can contact us through email and we will respond within 3 business days. (see 2.9 Point of contact)

4.2 Cooperation, interaction and disclosure of information

The Exclusive Networks Group SOC is a member of the Belgian Cyber Security Coalition. There is also a variety of industry partners with whom we are sharing Threat Intelligence (eg through MISP).
Communications are tagged with a unique identifier to refer to the incident number, as recorded within the EXN-GSOC's incident management system.
Communication with constituency is primarily via e-mail.

4.2.1 RED – personal for named recipients only

In the context of a meeting, for example, red information is limited to those present at the meeting. In most circumstances, red information will be passed verbally or in person.

4.2.2 AMBER – limited distribution

Limited disclosure, recipients can only spread this on a need-to-know basis within their *organisation* and its *clients*.
Information in this category can be circulated widely within a particular community. However, the information may not be published or posted publicly on the Internet, nor released outside of the community.

4.2.3 AMBER + STRICT– limited distribution

Limited disclosure, restricted to participants' organization.

4.2.4 GREEN – peers and partners, non-public

GREEN may be shared with peers and partner organizations within their sector or community, but not via publicly accessible channels.

4.2.5 CLEAR – unlimited

CLEAR may be distributed without restriction, subject to copyright controls.

4.3 Communication and authentication

It is mandatory to transmit all communication higher than “GREEN” through secure (encrypted) channels.

5 Services

5.1 Reactive Services

- Alerts & warnings
- Incident handling
- Vulnerability handling
- Incident response
- Artefact handling
- Digital forensics

5.2 Proactive Services

- Announcements
- Tech watch
- Tools development
- Intrusion detection
- Threat intelligence

5.3 Security Quality Management Services

- Security awareness
- Training
- Red team

5.4 Incident reporting forms

Not available (e-mail only).