ENHANCING SECURITY OPERATION CENTRES (SOCS)

CALL FOR APPLICATIONS TO SELECT MEMBERS OF AN ENISA AD HOC WORKING GROUP ON SOCS.

1. INTRODUCTION

The proliferation of emerging technologies into our daily life and the accelerated pace with which companies, governments and institutions digitalise their core functionalities are creating opportunities for economic prosperity. The road to prosperity, however, comes with a compromise, as the threat landscape is ever-increasing, creating opportunities for cyber criminals to cause unprecedented harm. Cornerstone to the protection of digital infrastructure for nations and organisations and the mitigation of the impact from cyberattacks are the Security Operation Centres (SOCs) and the Computer Security Incident Response Teams (CSIRTs), whose importance is established in the NIS Directive (Directive (EU) 2016/1148 on security of network and information systems)[1].

Typically, a SOC comprises a team of experts who are responsible for the management of cybersecurity incidents. The services offered by SOCs have expanded over the last years to adapt to the fast pacing technological evolutions and to novel cyberattacks. SOCs commonly offer:

- Information security incidents analysis,
- Monitoring and detection,
- Event analysis,
- Vulnerability analysis,

[1] https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=uriserv:OJ.L_.2016.194.01.0001.01.ENG&toc=OJ:L:2016:194:TOC

- Awareness building.

There is an abundance of literature examining the services that SOCs offer, describing tools to enhance SOCs' capabilities and reasoning about areas for improvement. There is scarce literature, however, providing a consolidating framework of all the services and processes that SOCs could establish, an analysis of the gaps in current practice and a roadmap on how to effectively achieve such services.

ENISA has been actively publishing reports and guidelines for SOCs since 2006. ENISA's seminal work provided a step-by-step guide on how to set up a SOC[2], which was updated recently[3]. Other reports focused on communicating good practice in incident management[4], baseline capabilities[5] and maturity profiles[6] which were later packed in a self-assessment tool for national CSIRTs. Finally, ENISA has been active in creating and delivering training material[7] and tailored exercises in order to enhance the skills of the SOC analysts.

Building on successful past work, ENISA, in collaboration with the Directorate-General for Communications Networks, Content and Technology (DG Connect), seeks to capture current practices in CSIRTS and SOCs, Member States' cybersecurity policies and investment plans relevant to increasing the capacity of SOCs, identify gaps based on maturity models for SOCs that establish best practice (i.e., FIRST framework[8]) and highlight pathways for research and innovation that will increase the maturity of current stakeholders in the field. This is the area the ad hoc Group will be working in.

2. SCOPE OF THE AD-HOC WORKING GROUP

The scope of this ad-hoc working group is to assist ENISA in capturing current practices across the EU regarding typical SOCs capabilities, i.e. capabilities to identify, protect against, detect, respond to and recover from cyber threats affecting a particular organisation. This will include in particular to assess and analyse:

- Relevant capabilities in existing CSIRTS and SOCs, based on widely accepted maturity models for SOCs and the level of cybersecurity threats that EU organisation currently face;
- Member States' policies and investment plans to increase SOCs capabilities; and
- Gaps and shortcomings in SOCs capabilities, based on the referred widely-accepted maturity models for SOCs and level of cybersecurity threat.

Based on the above assessment and analysis, provide recommendations to improve SOCs capabilities. Such improvements may include:

- Fostering collaboration between CSIRTs and SOC stakeholders;
- Providing training and educational modules;
- Designing exercises and "Capture the flag"-type events;
- Creating novel tools and infrastructure for all services that SOCs offer; and
- Other activities.

[2] https://www.enisa.europa.eu/publications/csirt-setting-up-guide
[3] https://www.enisa.europa.eu/publications/how-to-set-up-csirt-and-soc
[4] https://www.enisa.europa.eu/publications/good-practice-guide-for-incident-management
[5] https://www.enisa.europa.eu/publications/national-governmental-certs-enisas-recommendations-on-baseline-capabilities
[6] https://www.enisa.europa.eu/topics/csirts-in-europe/csirt-capabilities/csirt-maturity
[7] https://www.enisa.europa.eu/topics/trainings-for-cybersecurity-specialists/
[8] https://www.first.org/standards/frameworks/csirts/csirt_services_framework_v2.1

To carry out this work, relevant stakeholders and experts in the field will be interviewed, including:

- Members of the Cooperation Group and the CSIRT Network under the NIS Directive and of the Cyber Crisis Liaison Organisation Network (CyCLONe);
- Other relevant authorities in the Member States;
- Employees and managers for national CSIRTs, sectorial SOCs, SOCs, stakeholders utilising SOCs' services;
- Providers of SOCs services; and
- Partners of EU projects relevant to SOCs, notably projects funded by the Horizon 2020 and Connecting Europe Facility programmes.

The key tasks of this working group include, but are not limited to:

- Advising ENISA on capturing current practices in SOCs;
- Identify relevant actions and plans from Member States relevant to SOCs;
- Advice on identifying gaps and synergies, including advice on specific cases and application scenarios in the field that highlight SOCs' needs;
- Advising ENISA on relevant stakeholders for interviews;
- Engage with willing Member States, stimulate alignments/ cooperation amongst them with the ultimate goal of supporting that cooperation, including with national and EU funding;
- Assisting ENISA in conducting interviews and in providing recommendations; and
- Generally advising ENISA in carrying out its tasks in relation to enhancing the capabilities of SOCs.

The preliminary estimate of the duration of the ad hoc working group is for up to one (1) calendar year from the kick-off date that will be set by ENISA. Extension of the mandate of this ad hoc working group is highly possible, provided that the scope of the work is not completed in one (1) year.

3. BACKGROUND OF THE AD HOC WORKING GROUP

As stipulated in Regulation (EU) 2019/881[9], Art. 20, the Executive Director of the EU Agency for Cybersecurity may set up ad hoc working groups composed of experts, including experts from the Member States' competent authorities, where necessary and within ENISA's objectives and tasks. Ad hoc working groups provide ENISA with specific advice and expertise. Prior to setting up an ad hoc working group, the Executive Director of ENISA shall inform the agency's Management Board[10].

The members of the ad hoc working groups are selected according to the highest standards of expertise, aiming to ensure appropriate balance according to the specific issues in question, between the public administrations of the Member States, the Union institutions, bodies, offices and agencies, and the private sector, including industry, users, and academic experts in network and information security[11].

[9] Article 20(4) of Regulation (EU) 2019/881.
[10] Article 20(4) of Regulation (EU) 2019/881.
[11] Recital 59 of Regulation (EU) 2019/881.

The recent EU Cybersecurity Strategy has highlighted the need to coordinate EU activities and with national endeavours, especially creating synergies for co-founding projects that will enhance the maturity of SOCs. Therefore, a gap analysis and recommendations for such projects are key to effectively allocating budget resources.

Along these lines, ENISA seeks to interact with a broad range of stakeholders for the purpose of collecting input on a number of relevant aspects including but not limited to: protection of critical infrastructure (especially with the assistance of SOCs); knowledge of threat landscape for critical sectors (as described in NIS and for telecommunications); SOCs' perception of the threat landscape for critical infrastructure; orchestration & automation tools for SOCs; threat intelligence sharing; training and education for SOCs; exercises and capture-the-flag-type competitions for SOCs; awareness raising; academic research related to SOCs; stakeholders utilising SOCs services; relevant EU policies; and related technological fields.

The membership to these groups is foreseen to pursue broad, interdisciplinary representation across stakeholders' communities.

4. APPOINTMENT OF MEMBERS

The members of the ad hoc working group shall be appointed by the Executive Director of ENISA from a list of suitable applicants duly selected in line with this call.

The appointment will be done for a period equal to the duration of the working group.

The selection of members is based on a personal capacity or for the purpose of representing particular interests that generally serve a public goal and they have a clear demonstrable skillset in such areas as protection of critical infrastructure; knowledge of threat landscape for critical sectors (as described in NIS and for telecommunications); orchestration & automation tools for SOCs; threat intelligence sharing; training and education for SOCs; exercises and capture-the-flag-type competitions for SOCs; awareness raising; academic research related to SOCs; and stakeholders utilising SOCs services related technological fields.

The members of this ad hoc working group may be reimbursed for their expenses to participate in the meetings according to the ENISA Reimbursement Rules.

Besides members of the ad hoc working group, ENISA is likely to establish a reserve list, in accordance with the same conditions that apply to members, who shall be called to replace any members indisposed due to reasons stated below.

Members who are no longer willing or no longer capable to contribute effectively to the group's deliberations, who in the opinion of ENISA do not comply with the conditions set out in Article 339 of the Treaty on the functioning of the European Union or who resign, shall no longer be invited to participate in any meetings of the Group and may be replaced for the remaining duration of the ad hoc working group.

Organisations and public entities, such as EU bodies, offices or agencies and international organisations, may be granted an observer status; organisations and public entities appointed as observers shall nominate their representatives. Observers and their representatives may be permitted by the Chair to take part in the discussions of the group and provide expertise. Their representatives generally cover their own expenses.

ENISA staff will be designated as Chair and Secretariat of the ad hoc working group.

ENISA will propose to the ad hoc working group a set of draft rules of procedure to be adopted as appropriate.

The membership of an ad hoc working group is generally limited to fifteen (15) members. Additionally, representatives of the various organisations and bodies, mentioned above can join meetings as observers.

In principle, the ad hoc working group shall convene in ENISA premises or as otherwise decided on a proposal of the Chair. The bulk of the work can be carried out remotely; conference calls or video conferencing are permitted and encouraged; support and planning will be provided by ENISA as appropriate.

5. TRANSPARENCY

The members of the ad hoc working group shall make a confidentiality and an absence of conflict of interest statement. Observers, invited experts etc. have no such obligation. Ad hoc working groups are subject to the conditions of Regulation (EC) No1049/2001[12].

6. PERSONAL DATA PROCESSING

Personal data shall be collected, processed and published in accordance with Regulation (EU) 2018/1725[13]. For further information, please refer to the data protection notice that is available as a separate document with the call.

7. REIMBURSEMENT OF MEMBERS

Members of an ad hoc working group may be reimbursed for their travel and subsistence expenses. If a member is from a location other than the location required for the provision of services or place of meeting, the following expenses are then eligible:

1. Travel expenses (economy class flight or 1st class train – whichever is more cost effective) from the European country/city in which the contractor is officially registered to another European city.
2. A “per diem” applicable to the country in which the meeting will take place. This allowance is set by the European Commission (download the latest rates from website (http://ec.europa.eu/comm/europeaid/perdiem/index_en.htm) and it covers all daily living expenses including hotel, meals, local travel etc.
3. No other claims for living or transportation costs will be accepted.

Members may select to refrain from being reimbursed on the basis of personal or professional considerations; in this case they remain eligible to apply.

[12] Regulation (EC) No 1049/2001 of the European Parliament and of the Council of 30 May 2001 regarding public access to European Parliament, Council and Commission documents. Exceptions are intended to protect public security, military affairs, international relations, financial, monetary or economic policy, privacy and integrity of the individual, commercial interests, court proceedings and legal advice, inspections/investigations/audits and the institution's decision-making process.
[13] Regulation (EU) 2018/1725 of the European Parliament and of the Council of 23 October 2018 on the protection of natural persons with regard to the processing of personal data by the Union institutions, bodies, offices and agencies and on the free movement of such data, and repealing Regulation (EC) No 45/2001 and Decision No 1247/2002/EC.

Observers are neither remunerated nor reimbursed, except in duly justified cases, to be determined by the Executive Director of ENISA.

8. APPLICATION PROCEDURE

Individuals interested are invited to submit their application to ENISA via the dedicated section on the ENISA web site. Applications must be completed in one of the official languages of the European Union. However, applications in English would facilitate the evaluation procedure. If another language is used, it would be helpful to include a summary of the CV and/or the application in English. An application will be deemed admissible only if it is submitted by the deadline.

8.1 DEADLINE FOR APPLICATION

The duly completed applications must be submitted by 18:00 (CET time) on the 25th of July 2021. The date and time of submission will be established on the website upon submission of an application.

9. SELECTION CRITERIA

ENISA will take the following criteria into account when assessing applications:

- Relevant competence (e.g. technical, legal, organisational or a combination thereof) and experience in the area **of setting up SOCs** and/or in other areas of relevance for the purpose of providing advice **on enhancing SOCs, such as the knowledge of the ICT market and its threats, developments as regards the cyber threat landscape, knowledge and experience in research for SOCs, and other related cybersecurity facets.**
- Ability to deliver technical advice at the tactical level, including those of scientific or technical nature, on issues relevant to **enhancing SOCs**, including in the above-mentioned areas of relevance for this purpose.
- Good knowledge of English allowing active participation in the discussions.

10. SELECTION PROCEDURE

The selection procedure shall consist of an assessment of the applications performed by ENISA as appropriate against the selection criteria mentioned above in this Call, followed by the establishment of a list of the most suitable applicants and concluded by the appointment of the members of the ad hoc working group by the Executive Director of ENISA.