Recruitment of CSIRT Staff

Toolset, Document for Students

1.0

DECEMBER 2016

www.enisa.europa.eu European Union Agency For Network And Information Security

About ENISA

The European Union Agency for Network and Information Security (ENISA) is a centre of network and information security expertise for the EU, its member states, the private sector and Europe's citizens. ENISA works with these groups to develop advice and recommendations on good practice in information security. It assists EU member states in implementing relevant EU legislation and works to improve the resilience of Europe's critical information infrastructure and networks. ENISA seeks to enhance existing expertise in EU member states by supporting the development of cross-border communities committed to improving network and information security throughout the EU. More information about ENISA and its work can be found at www.enisa.europa.eu.

Contact

For contacting the authors please use cert-relations@enisa.europa.eu.
For media enquires about this paper, please use press@enisa.europa.eu.

Legal notice

Notice must be taken that this publication represents the views and interpretations of ENISA, unless stated otherwise. This publication should not be construed to be a legal action of ENISA or the ENISA bodies unless adopted pursuant to the Regulation (EU) No 526/2013. This publication does not necessarily represent state-of the-art and ENISA may update it from time to time.

Third-party sources are quoted as appropriate. ENISA is not responsible for the content of the external sources including external websites referenced in this publication.

This publication is intended for information purposes only. It must be accessible free of charge. Neither ENISA nor any person acting on its behalf is responsible for the use that might be made of the information contained in this publication.

Copyright Notice

Table of Contents

1 What Will You Learn

This training sets out to provide an indication of what an organisation might consider during the recruitment of staff for CSIRT teams. The contents are mere suggestions and the responsibility for the interview process shall lie with the recruiting agency. ENISA accepts no responsibility for any issues arising during the interview process.

2 Exercise course

2.1 Introduction

Your trainer will discuss with you what kind of staff you have in your CSIRT teams and what the different roles are. Different types of CSIRTs will be regarded, based on scope (global, regional, sectoral, national, organisation internal, product) and on constituency (government, research&education, national collaboration, financial, medical, law enforcement, etc.) – and the typical service areas and services that a CSIRT provides (incident management, analysis, information assurance, situational awareness, etc.).

The discussion will then focus on 3 typical CSIRT roles, that are apparent in a majority of teams, and that will be used for the basis of this exercise:

- Medior[1] specialist & incident handler
- Senior specialist & incident handler
- General manager, who manages a CSIRT team

The number of people to be hired depends on a combination of 3 factors:

1. Incident load (which depends on the size of the constituency, the constituency's network's exposure to the global Internet, and the attractiveness of the constituency for miscreants)
2. Scale and scope of the CSIRT services to be provided
3. Available financial resources

A team with 3 incident handlers is generally seen as the absolute minimum however. Ideally, a team has, apart from the general manager, at least one senior specialist who can also act as technical manager, plus at least 3 medior specialists to do incident handling and related research issues. Bigger teams can make separate teams for e.g. alerts & warnings, incident handling and research.

2.2 Keys to the exercise

2.2.1 Task 1: Assembling job profiles for your CSIRT

2.2.1.1 Prepare job profiles in groups.

The teacher will divide the class into groups. Each group will prepare the job profile for a specific role, as in the roles discussed in the introduction. You can use the template below, and the 3 different categories (functional requirements, competencies and tasks) suggested there, but this is not obligatory. Important is to realise that CSIRT work is not just about technical skills, but also about various other skills. The trainer will discuss this.

[1] The word "medior" is a fairly new occurrence and not commonly seen everywhere yet. It is meant as a level indicator of experience and is situated inbetween junior and senior.

<table>
<tr><th colspan="3"><b>Profile role :</b> Medior specialist & incident handler</th></tr>
<tr><td><b>Functional requirements</b></td><td><b>Competencies</b></td><td><b>Tasks</b></td></tr>
<tr><td></td><td></td><td></td></tr>
<tr><td></td><td></td><td></td></tr>
<tr><td></td><td></td><td></td></tr>
<tr><td></td><td></td><td></td></tr>
<tr><td></td><td></td><td></td></tr>
<tr><td></td><td></td><td></td></tr>
<tr><td></td><td></td><td></td></tr>
<tr><td></td><td></td><td></td></tr>
<tr><td></td><td></td><td></td></tr>
<tr><td></td><td></td><td></td></tr>
<tr><td></td><td></td><td></td></tr>
<tr><td></td><td></td><td></td></tr>
<tr><td></td><td></td><td></td></tr>
<tr><td></td><td></td><td></td></tr>
<tr><td colspan="3"><b>Other important aspects :</b></td></tr>
</table>

Profile role : Senior specialist & incident handler		
Functional requirements	**Competencies**	**Tasks**
Other important aspects :		

<table>
<tr><th colspan="3"><b>Profile role :</b> General manager</th></tr>
<tr><th>Functional requirements</th><th>Competencies</th><th>Tasks</th></tr>
<tr><td></td><td></td><td></td></tr>
<tr><td></td><td></td><td></td></tr>
<tr><td></td><td></td><td></td></tr>
<tr><td></td><td></td><td></td></tr>
<tr><td></td><td></td><td></td></tr>
<tr><td></td><td></td><td></td></tr>
<tr><td></td><td></td><td></td></tr>
<tr><td></td><td></td><td></td></tr>
<tr><td></td><td></td><td></td></tr>
<tr><td></td><td></td><td></td></tr>
<tr><td></td><td></td><td></td></tr>
<tr><td></td><td></td><td></td></tr>
<tr><td></td><td></td><td></td></tr>
<tr><td></td><td></td><td></td></tr>
<tr><td colspan="3"><b>Other important aspects :</b></td></tr>
</table>

2.2.1.2 Present job profiles plenary & discuss

Each group will present their job profiles to the plenary, followed by discussion.

2.2.2 Task 2: Writing job advertisements (60 min)

2.2.2.1 Write job advertisements for the job profiles

You work in groups again, this time to write job advertisements for the profiles established in the previous part of this training.

2.2.2.2 Present job advertisements plenary & discuss (30 minutes)

Each group will present their job advertisements to the plenary, followed by discussion.

2.2.3 Task 3: Analysing and choosing candidates to be interviewed

2.2.3.1 Study CVs, make SWOT analysis and select candidates for interviews

You work in a new group, one group per job profile, so normally 3 groups. Your group will study 6 CVs of candidates for that specific job. Part of the group will compare those CVs against the job advertisements (and corresponding job profiles) established earlier in this training – while the other part of the group will write short opinions about all 6 candidates based on SWOT analysis: strength, weaknesses, opportunities, threats (SWOT template suggestion provided below: copy this onto a blank sheet of paper). At the end of this step, your group decides which two candidates should be interviewed.

<table>
<tr><td colspan="4"><b>SWOT analysis</b>
<b>Profile role :</b> General manager   <b>Candidate :</b></td></tr>
<tr><td><b>Strengths</b></td><td><b>Weaknesses</b></td><td><b>Opportunities</b></td><td><b>Threats</b></td></tr>
<tr><td></td><td></td><td></td><td></td></tr>
</table>

2.2.3.2 Present results plenary & discuss

Each group will present their opinions about the candidates to the plenary and justify their choice (for each CV).

2.2.4 Task 4: Interviewing chosen candidates

2.2.4.1 Build questions for interviews

You will familiarise yourself with the CSIRT Code of Practice (CCoP) that the European CSIRT community TF-CSIRT recommends as good practice for CSIRTs. Then, based on the CCoP as well as on the prepared job advertisements and the CVs of the chosen candidates, your group (the same as in the last exercise) will propose up to 20 interview questions (5 general, 5 technical, 5 communication/presentation, 5 others including ethics) that you would like to ask particular candidates of your choice. You can use the following template.

General questions	Rating/notes
1.	
2.	
3.	
4.	
5.	
Technical questions	
1.	
2.	
3.	
4.	
5.	
Communication/presentation questions	
1.	
2.	
3.	
4.	
5.	
Other questions	
1.	
2.	
3.	
4.	
5.	

2.2.4.2 Present questions plenary & discuss

Each group will present their interview questions to the plenary and will explain which of those they consider the 5-10 most important ones.

2.2.4.3 Prepare roleplay for interviews

Your group will now design a role model to use in the job interviews that will take place soon – what interviewer will focus on what areas. The developed questions are meant as starting points.

2.2.4.4 Establish volunteer interviewees

Volunteers will be asked to play the roles of the chosen candidates. In general this will be limited to 3-4 candidates, due to time constraints.

2.2.4.5 Do interviews

Next, as a group you start interviewing the selected 3-4 candidates. After the interview your group discusses the candidate's answers and shares their opinions. During all this, all other groups are present and listen in silence.

2.2.5 Task 5: Final Selection & Summary

2.2.5.1 Select best candidates

Each student individually prepares their personal opinion about all the candidates, makes their selection, and considers their reasos for that selection. Then there will be a vote for the candidates.

2.2.5.2 Discuss selection plenary

The trainer will discuss the results of the selection with you, and your reasoning behind it.

3 Conclusions

The trainer will discuss process and outcomes with you and provide further hints.

ENISA

European Union Agency for Network
and Information Security
Science and Technology Park of Crete (ITE)
Vassilika Vouton, 700 13, Heraklion, Greece

Athens Office

1 Vass. Sofias & Meg. Alexandrou
Marousi 151 24, Athens, Greece

PO Box 1309, 710 01 Heraklion, Greece
Tel: +30 28 14 40 9710
info@enisa.europa.eu
www.enisa.europa.eu