



Recruitment of CERT staff

Toolset, Document for students

September 2014





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.

Acknowledgements

Contributors to this report

We would like to thank all our ENISA colleagues who contributed with their input to this report and supervised its completion, especially Lauri Palkmets, Cosmin Ciobanu, Andreas Sfakianakis, Romain Bourgue, and Yonas Leguesse. We would also like to thank the team of Don Stikvoort and Michael Potter from S-CURE, The Netherlands, Mirosław Maj and Tomasz Chlebowski from ComCERT, Poland, and Mirko Wollenberg from PRESECURE Consulting, Germany, who produced the second version of this documents as consultants.

Agreements or Acknowledgements

ENISA wants to thank all institutions and persons who contributed to this document. A special 'Thank You' goes to the following contributors: Anna Felkner, Tomasz Grudzicki, Przemysław Jaroszewski, Piotr Kijewski, Mirosław Maj, Marcin Mielniczek, Elżbieta Nowicka, Cezary Rzewuski, Krzysztof Silicki, Rafał Tarłowski from NASK/CERT Polska, who produced the first version of this document as consultants and the countless people who reviewed this document.

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 the authors and editors, 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

© European Union Agency for Network and Information Security (ENISA), 2013

Reproduction is authorised provided the source is acknowledged.



Table of Contents

1	What Will You Learn	1
2	Exercise Task	1
2.1	Task 1 Writing job advertisements for recruiting CERT staff	1
2.2	Task 2 Analyzing and choosing candidates to be interviewed	1
2.3	Task 3 Interviews with chosen candidates	1
2.4	Task 4 Final selection of the best candidates	1
3	Appendix A	2
4	Appendix B	4



1 What Will You Learn

The purpose of this exercise is to improve your ability to optimally recruit staff for the CERT team. You will learn:

- What kind of professional experience and/or qualifications, as well as personal abilities, are essential to fulfil the main roles and responsibilities of a CERT;
- What kinds of questions should be asked during a job interview; and
- How to choose the most suitable candidates for the CERT team.

2 Exercise Task

2.1 Task 1 Writing job advertisements for recruiting CERT staff

You will be either a member of the 'Technicians' or 'Researchers' group. The task of your group is to complete a job advertisement template for positions in either the 'Incident Handling Service' or the 'Security Project Development Team' respectively (see appendix A). Be prepared to present your job advertisement proposal to others.

2.2 Task 2 Analyzing and choosing candidates to be interviewed

Each group will receive a collection of 6 CVs. Analyze all the CVs and try to match them with the prepared job offers. Write short opinions about all the candidates (strong and weak points, pros and cons in several aspects). Be prepared to present your opinions about all candidates and justify your choice.

2.3 Task 3 Interviews with chosen candidates

Read the 'code of conduct' developed by TF CERT. Using the CoC, your prepared job advertisement and the CVs of the chosen candidates, propose up to 20 interview questions (5 general, 5 technical, 10 others) that you would like to ask the candidates of your choice. (Use the blank template in appendix B.)

Be prepared to present your questions to others and explain which of them you find the most useful. The trainer will also propose a few questions and let you decide which of them you consider important. Decide on a set of 10 questions to be asked of a chosen candidate. After a 15 minute break, volunteers from each group will play the roles of the chosen candidates and the others will start to interview them. Every group joins all the interview sessions. After each interview, the groups individually discuss the candidates' answers and share opinions.

2.4 Task 4 Final selection of the best candidates

After all the interviews, prepare your own opinion about all the candidates and make your selection (with justifications). Then vote for the candidates.



3 Appendix A

Job Advertisement for IT Security Specialist (Incident Handling Service)

Main tasks:

- Handling network security incidents
- Operating the CERT early warning and alerting system for a CERT constituency
- Writing security advisories
- Writing security news
- Preparing CERT reports

Essential requirements (technical qualifications, knowledge and personal skills)

-
-
-
-
-
-
-
-
-
-
-
-
-
-
-
-
-
-
-
-

Additional assets

-
-
-

We offer

-
-
-
-
-



Job Advertisement for IT Specialist (Security Projects Development Team)

Main tasks:

- Participation in projects related to the security network
- Carrying out research on new methods for the detection and analysis of malicious software
- Development of concepts for IT projects to pursue new solutions
- Cooperation with software engineers in the implementation of the proposed solutions
- Testing developed applications
- Writing technical documentation
- Development of IT security policies

Essential requirements (technical qualifications, knowledge and personal skills)

-
-
-
-
-
-
-
-
-
-
-
-
-
-
-

Additional assets

-
-
-

We offer

-
-
-
-
-

4 Appendix B

Job Interview Questions Form

Candidate 1 Candidate 2

I. General issues:

- 1.
- 2.
- 3.
- 4.
- 5.

II. Technical knowledge and qualifications:

- 1.
- 2.
- 3.
- 4.
- 5.

III. Personal skills:

- 1.
- 2.
- 3.
- 4.
- 5.

IV. Facultative questions:

- 1.
- 2.
- 3.
- 4.
- 5.

**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