
# Recruitment of CERT staff

*Handbook, Document for teachers*

September 2014

European Union Agency for Network and Information Security www.enisa.europa.eu

## 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



## Copyright Notice

# Table of Contents

# 1 Introduction

## Goal

To raise the ability of CERT managers to optimally recruit staff for their CERT teams.

## Target audience

CERT managers who are responsible for recruiting staff.

## Course Duration

6 hours, 20 minutes

## Frequency

It is recommended that the exercise be performed once by CERT managers whose tasks cover the recruitment of the staff and thereafter every three years.

## Structure of this document

| | Task | Duration |
|---|---|---|
| | Introduction to the exercise | 20 min |
| | Task 1: Writing job advertisements for recruiting CERT | 90 min |
| | Task 2: Analysing and choosing candidates to be interviewed | 90 min |
| | Task 3: Interviewing chosen candidates | 120 min |
| | Task 4: Final selection of the best candidates | 30 min |
| | Summary of the exercise | 30 min |

# 2 General Description

The purpose of the exercise is to improve the ability of CERT managers to optimally recruit staff for their CERT teams. Students will learn:

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

In particular, the exercise is intended to deliver a collection of tips on how to recognize and understand a candidate's attitude towards many aspects (technical, ethical and organizational) of network security.

The trainer should be an experienced CERT manager who has conducted many interviews with candidates and managers, or who has managed an incident response team in the past.

# 3 EXERCISE COURSE

The course of this exercise is as follows. All discussions should be moderated by the trainer.

## 3.1 Introduction to the exercise

To begin with, ask students what kind of staff they have in their CERT teams and what different roles need to be fulfilled within their teams. Next, describe the typical organizational structures of a CERT team (independent business model, organization embedded model, campus model, etc) [1] and the typical services that a CERT provides (incident handling, alerts and warnings, vulnerability handling) [2]. Also explain that, despite the differences between several CERT models, the team's staff should include the following members:

- General manager, who manages a CERT team,
- Technical staff, ie, staff to operate CERT services, and
- Researchers, ie, staff to undertake research.

Additionally, some consultants can assist the general manager in his work; these would include a legal specialist who deals with legal issues and preserves evidence in the event of a lawsuit.

The number of people to be hired depends on the scale of the CERT services which will be provided and its financial resources but, roughly speaking, the operational technical team should consist of one technical manager plus two technicians and the research team of one research manager plus two researchers.

The CERT team leader should have a background in security and experience in the work involved in resilience crisis management in the field. Staff of an operational technical team should be security specialists who can deliver the specialized CERT services for handling and responding to IT incidents. Researchers should have a good background in network security, experience in security projects and publications in the field of network security.

## 3.2 Keys to the exercise

### 3.2.1 Task 1 Writing job advertisements for recruiting CERT staff

At the beginning, tell students that determining the key competencies required of the future staff for their team will have a significant influence on the effectiveness of each service provided by the team; it will also motivate the work-place in a way that enables everybody to exchange ideas, work together and improve their skills. All this will affect the team's success in the future. Recruiting the right staff requires careful identification of features that are important for a team as a whole, but it also requires taking note of the individual skills of candidates.

**Step 1:** Ask students to prepare job advertisements (blank templates are included in the students' exercise book). This step should take at most 45 minutes.

- Task of groups 1-2 (technicians) is to write a job offer for a technical position. The main tasks of an employee holding this position will include:
    - Handling and responding to network security incidents
    - Operating the CERT early warning and alerting system for a CERT constituency
    - Writing security advisories
    - Writing news about security threats

  - Preparing CERT reports
  - Carrying out security audits
- Task of groups 3-4 (researchers) is to write a job offer for a research position. The main tasks of an employee holding this position will include:
  - Participation in projects related to the security network
  - Carrying out research on new methods for the detection and analysis of malicious software
  - Development of the concept of IT projects to pursue new solutions
  - Cooperation with software engineers in the implementation of proposed solutions
  - Testing developed applications
  - Writing technical documentation
  - Development of IT security polices

**Step 2:** Each group presents its job advertisement proposal to the others. (It may be displayed so everybody can see it.) This step should take at most 30 minutes

Job advertisements for the technician position may include the following main requirements:

- Good knowledge of issues related to security on the Internet
- Good knowledge of mechanisms of TCP / IP and most common network services
- Good knowledge of Windows operating systems
- Very good knowledge of Linux (administration will be an advantage)
- Knowledge of programming languages: Perl, PHP
- Good knowledge of at least one foreign language
- Responsibility
- The ability to work in a team
- The ability to transfer knowledge
- High personal culture (diplomacy)
- Communicative

Additional advantages could be:

- Two years administration experience
- Membership of IT security organizations

Job advertisements for the researcher position may include the following main requirements:

- Higher education or related level of education (MSc)
- Very good knowledge of network security issues, in particular the risks involved in network monitoring and the analysis of malicious software
- Experience with new technologies (more than one) such as honeypots, client honeypots, systems IDS / IPS / WAF, the sandbox, darknets, and early warning systems
- Very good knowledge of TCP / IP
- Good knowledge of Linux
- Practical knowledge of C / C or Java, and scripting languages
- Practical knowledge of relational databases
- Ability to think analytically
- Ability to work both in a group and on his or her own
- Knowledge of at least one foreign language
- Good writing skills

Additional advantages will be:

- Experience in research projects in the field of IT security
- Experience in project management

The CERT team can offer:

- Participation in innovative international projects in cooperation with world-renowned IT companies and institutions
- Ability to pursue their own research interests
- Access to information about the latest events relating to the propagation of threats in networks
- Participation in international working groups and conferences
- IT security training

In general, according to ENISA, the technical qualifications of CERT technical staff should include:

- Broad knowledge of Internet technology and protocols
- Knowledge of Linux and Unix systems (depending on the equipment of the constituency)
- Knowledge of Windows systems (depending on the equipment of the constituency)
- Knowledge of network infrastructure equipment (router, switches, DNS, proxy, mail, etc)
- Knowledge of Internet applications (SMTP, HTTP(s), FTP, telnet, SSH, etc)
- Knowledge of security threats (DDoS, phishing, defacing, sniffing, etc)
- Knowledge of risk assessment and the practical implementation of security measures

The personal abilities of CERT technical staff should include:

- Flexibility, creativity and a good team spirit
- Strong analytical skills
- Ability to explain difficult technical matters in simple words
- A good feeling for confidentiality and working in a procedural manner
- Good organizational skills
- Ability to handle stress well
- Strong communication and writing skills
- Open mindedness and a willingness to learn

There are also additional competencies that could be considered:

- Willing to work 24x7 or on call duty (depending on the service model)
- Maximum travelling distance (in case of emergency, availability in the office; maximum travelling time)
- Level of education
- Experience in working in the field of IT security

Required CERT staff qualities are also described in references (see 3 and 5).

**Step 3**: This phase could be summed up as a discussion of the skills that have the highest priority for each position. Ask students to make their own lists of the highest priorities for the competencies of an ideal candidate for a particular position. Write all the ideas on the whiteboard. Afterwards, if any items considered to be important were missed by students, add them to the list.

It should be stressed here that both technical knowledge and the skills connected to the personality of a candidate are very important. Skills such as communication abilities, language fluency, personal habits, friendliness, and optimism are essential for contacts and teamwork.

Also, motivation, the ability to hard work under pressure, resistance to stress, as well as attitude to ethical issues, have high priority in this kind of work.

### 3.2.2 Task 2 Analysing and choosing candidates to be interviewed

Students from groups of the same profile form one group, so from now on there is one technicians and one researchers group.

**Step 1**: Distribute a collection of 6 CVs (having selected them earlier from a 12 CV collection included in the Virtual Image in /usr/share/trainer/03_RCS/adds/ directory) to each group. It is assumed that all candidates have passed computer literacy tests at the level required to be a member of a CERT team. Students from each group analyse all the CVs and try to match them with the prepared job offers. In parallel, students write short opinions about all the candidates (strong and weak points, pros and cons in several aspects). At the end of this step, each group decides which two candidates should be interviewed. This step should take about 45 min.

**Step 2**: Each group presents its opinions about the candidates and justifies their choice (for each CV). Ask questions, comment on the students' opinions and try to show aspects potentially missed by the students.

### 3.2.3 Task 3 Interviewing chosen candidates

This phase is devoted to interviews. Each interview should not exceed 15 minutes.

**Step 1:** First, let the students become familiar with the code of conduct (CoC) in the TF CERT ([7], included in the exercise package). Afterwards, based on the CoC as well as on the prepared job advertisement and the CVs of the chosen candidates, the groups propose up to 20 interview questions (5 general, 5 technical, 10 others) that they would like to ask particular candidates of their choice.

**Step 2:** Each group presents their interview questions to the others and explains which of them are most important. Propose a few questions (including some in respect of CoC - if missed by students) and let the students decide which of them they consider important. At this stage, do not comment on their choice.

**Step 3:** Each group decides on a set of about 10 questions to be put to a chosen candidate. During the presentation, ask each group to assess the validity of some the questions.

**Step 4:** Ask for volunteers from each group to play the roles of the chosen candidates. (Notice that the number of candidates chosen to be interviewed may very between two and four.) If there are no volunteers, you need to choose them. Students from technicians will play the role of candidates for the research position and, analogically, students from researchers will play the role of candidates for the technical position. Volunteers receive copies of the CVs and have 15 minutes for preparation. At the same time, the rest of a group has a break. For volunteers' information only: advise them to give answers which cannot be unambiguously interpreted easily. Suggest to them that they pretend to have different personal abilities than they actually have.

**Step 5:** After a break, the students start interviewing the selected candidates. Every group joins all the interview sessions. If it happens that both groups have chosen the same candidate (ie, same CV), this candidate is interviewed by both groups in one interview, responding to the questions of the technicians and the researchers. After each interview the group discusses the candidate's answers and shares its opinions. Summarize them and encourage students to ask additional questions – if needed.

Interview questions I. Large collections of general job interview questions are available at [6]. Examples of some general questions regarding work history, experience, expectations from the new job and company, interests, the future, etc, that should be asked of candidates may include:

| | Question |
|---|---|
| | 1. Please introduce yourself. |
| | 2. What were your expectations for the job and to what extent were they met? |
| | 3. What were your responsibilities? |
| | 4. What major challenges and problems did you face? How did you handle them? Which was the most or least rewarding? |
| | 5. What was your biggest accomplishment or failure in this position? |
| | 6. Questions about his or her supervisors and co-workers. Who was your best boss and who was the worst? |
| | 7. Why are you leaving your job? |
| | 8. How do you handle stress and pressure? |
| | 9. What motivates you? |
| | 10. Do you prefer to work independently or in a team? Give some examples of teamwork. |
| | 11. If you know your boss is 100% wrong about something, how would you handle it? |
| | 12. What interests you about this job? |
| | 13. What do you know about this company? |
| | 14. Why do you want to work here? |
| | 15. Is there anything I haven't told you about the job or company that you would like to know? |
| | 16. What are your goals for the next five years or ten years? |
| | 17. Tell us about your hobby. (Speak about it in a foreign language.) |

**Facultative Questions:**

| | Question |
|---|---|
| | 1. What are your salary expectations? |
| | 2. What have you been doing since your last job? |
| | 3. Why were you fired? (if applicable) |
| | 4. Do you take work home with you? |
| | 5. Are you willing to travel? |

**Interview questions II**. More specific questions regarding technical qualifications and personal abilities may include:

**Technical issues**

| | Question |
|---|---|
| | 1. How does Snort work? What is the working principle of network intrusion detection systems? |
| | 2. What is the difference between low- and high-interaction honeypots? What honeypots do you know? |
| | 3. What is the difference between TCP and UDP protocols? Name a few services that use TCP and UDP. |
| | 4. What examples of network worms do you know? What are the methods for their propagation? |
| | 5. How should information about new vulnerabilities or warnings of new threats be published? |
| | 6. What are the most common motivations behind black-hat hacking? |
| | 7. Why would anyone want to infect a home-user computer? |
| | 8. What is phishing? What techniques can be used to phish? |
| | 9. What is a botnet? How can you take it down? |
| | 10. What are countermeasures against DDoS attacks? |

Ethical/general issues

| | Question |
|---|---|
| | 1. What would you do if you discovered a publicly-unknown software vulnerability? |
| | 2. What do you think about 'ethical hacking'? Have you ever done it? |
| | 3. What do you understand by the concept of ethics in the security industry? |
| | 4. What national or international security organizations do you know? |
| | 5. What is the biggest threat and/or the most popular type of incident on the network handled by CERTs nowadays (according to the statistics from the annual CERT report)? |

Moreover, a collection of interview questions should include a few questions referring to the candidates' CVs.

### 3.2.4 Task 4 Final selection of the best candidates

After all the interviews, ask the students to prepare their own opinions about all the candidates and to make their selections (with justifications). Then, ask them to vote for the candidates.

After all the presentations, begin a discussion with the following questions:

- Which candidate's answers convinced them to choose that candidate (if any was selected)? Do the other students have similar feelings about this?
- Which candidate's answers convinced them to reject that candidate (if any was rejected)? Do the others have similar feelings about this?

## 4 Summary of the exercise

As a summary of this exercise, you can ask students the following:

- What they think are the most useful abilities for becoming part of a CERT team?
- How do they imagine an ideal candidate (technical qualifications, personal abilities and other competencies) for different roles within a CERT team?
- On the other hand, what do they consider problematic about some recruited staff in their daily work?

Also, you can ask students where would be the best place to publish their job offers. Moreover, where and how they would seek candidates? You can also ask for other possibilities for recruiting.

Encourage students to exchange their opinions, to ask questions, and to give their feedback about the exercise.

Moreover, you can mention also that a candidate who has just graduated from university can be considered for a position as a junior IT specialist researcher. This candidate should have, however, some past experience in Internet security activities such as script kiddies, research groups and writing security news, etc.

## 5 EVALUATION METRICS

Evaluate the offers and the prepared interview questions, as well as the reasons for choosing or rejecting the candidates.

- Did the students consider the appropriate skills for each position in their job offers (technical, personal, ethical)?
- Did the students propose adequate questions for conducting the interviews?

Were the students' opinions about candidates and selections adequately and sufficiently justified?

## References

1. CERT organizational structure, http://www.enisa.europa.eu/activities/cert/support/guide2

2. CERT services. http://www.cert.org/csirts/services.html, (2008)

3. CERT/CC. Staffing Your Computer Security Incident Response Team – What Basic Skills Are Needed? http://www.cert.org/csirts/csirt-staffing.html

4. ENISA: CERT team roles and staffing. http://www.enisa.europa.eu/activities/cert/support/guide2/internal-management/team-roles

5. Handbook for Computer Security Incident Response Teams (CERTs), CERT/CC document. http://www.cert.org/archive/pdf/csirt-handbook.pdf [Staff issues, p.166-171]

6. Large collections of various interview questions.http://jobsearch.about.com/od/interviewquestionsanswers/a/interviewquest.htm http://www.jobinterviewquestions.org/

7. The European CERT Network. Code of Conduct. http://www.ecsirt.net/service/coc.html


**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