Recruitment of CSIRT Staff

Handbook, Document for Trainers

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 Objective and description

Main Objective	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.	
Targeted Audience	The training is aimed at CSIRT managers who are responsible for recruiting staff.	
Total duration	1 day (8 hours without breaks)	
Time Schedule	**Introduction to the training**	0.50 hours
	Task 1: Assembling job profiles for your CSIRT	1.50 hours
	Task 2: Writing job advertisements	1.00 hours
	Task 3: Analysing and choosing candidates to be interviewed	1.50 hours
	Task 4: Interviewing chosen candidates	2.50 hours
	Task 5: Final Selection	0.50 hours
	Conclusions	0.50 hours
Frequency	It is recommended that this training be performed once by CSIRT managers whose tasks include the recruitment of the staff, and every three years thereafter.	

This training sets out to optimise the ability of CSIRT managers to recruit the right staff for their CSIRT teams. Students will learn:

- What staff roles are essential for a CSIRT
- What kinds of professional experience and/or qualifications, as well as personal abilities, are essential to fulfil these roles
- How to write job profiles for these roles
- How to write job advertisements based on the job profiles
- How to analyse job applications and shortlist the best candidates
- How to interview candidates

- How to choose the best candidates to join the team

The trainer needs to be aware of the following:

- The trainer should preferably have significant experience as a CSIRT manager (or equivalent) who has selected candidates for one or more CSIRTs.
- This training has several (sub-)tasks where timing depends on class size. The starting point for the timings given is a class of twenty students, five groups of four students when they split up for Task 1. Based on the size of your class, you can adapt the task timings and omit some elements to fit your schedule.
- All group discussions should be moderated by the trainer.

2 Exercise course

2.1 Introduction to the training (30 minutes)

To begin, discuss with the students what kind of staff they have in their CSIRT teams and what the different roles are. Next, shortly describe types of CSIRTs based on scope (global, regional, sectoral, national, organisation internal, product) and on constituency (government, research & education, national collaboration, financial, medical, law enforcement, etc.) [1] and the typical service areas and services that a CSIRT provides (incident management, analysis, information assurance, situational awareness, etc.) [2].

Also explain that, despite the differences between several CSIRT models, the team's staff should include the following members:

- Medior[1] specialist & incident handler (explain that junior specialists usually have no place in a CSIRT, unless it is a very big team that offers a career and education path internally)
- Senior specialist & incident handler
- General manager, who manages a CSIRT team
- Other staff (researchers, press spokesperson, legal expert, admin, etc.)

The number of people to be hired depends on a combination of three 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

However, a team with three incident handlers is seen as the absolute minimum. Ideally, a team has, apart from the general manager, at least one senior specialist who can also act as technical manager, plus at least three 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.

The general manager should have a background in security and experience in the work involved in resilience crisis management in the field.

The senior and medior specialists should be network/computer security specialists who can deliver specialised CSIRT services for handling and responding to IT incidents, and do related research.

[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.

2.2 Keys to the exercise

2.2.1 Task 1: Assembling job profiles for your CSIRT (90 minutes)

Explain to the students that determining the 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 workplace 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, and these are best laid down in job profiles. Make sure to stress, however, that any team, especially a CSIRT, is not the sum of the collected job profiles, but can be much more. This also depends on (a) unique individual skills that escape job profiling and (b) team spirit and motivation.

2.2.1.1 Prepare job profiles in groups. (45 minutes)

Divide the class into groups of three or four students. Ask the students to prepare job profiles (blank templates are included in the students' exercise book). Assign the following job profiles to the groups, depending on the number of groups available:

- One or more groups write a profile for the medior specialist & incident handler;
- One or more groups write a profile for the senior specialist & incident handler;
- Only one group should write a profile for the general manager. Preferably, fill this group with students who have more management experience;
- *Only in special cases, depending on the setting/audience of the training: assign groups to specific other profiles like for a dedicated researcher or a communications (PR) expert. The trainer will need his/her experience and improvisation skills in that case, as in this training, no profiles or job advertisements are available as examples for those functions.*

Stress that the students should not only think about and write down technical skills, but also consider soft skills (communication, team play, etc.), ethics and training/education requirements.

Below, we offer an example for each of the three job profiles. These examples are (with variations) in use with several European teams:

2.2.1.1.1 Medior specialist & incident handler

Functional requirements:

- Technical education on academic level (bachelor or master) or comparable
- A minimum of 5 years working experience in an IT function (e.g. system management or security)
- Experience gained by working inside a CSIRT/CERT or SOC is a plus
- Good skills of communication and explanation, on both user and technical level. Experience gained by giving relevant training/course work is a plus
- Good working knowledge of the Internet and computer networks, and related cyber security aspects, at least on a technical level
- Knowledge of threats and risks in regard cyber security, and possible counter measures.
- Knowledge of Internet protocols, Windows and UNIX/LINUX environments. Knowledge of mobile operating systems is a plus
- Good knowledge regarding the security aspects of at least a number of IT environments
- Experience in system and network management

- Knowledge of DNS, TCP/IP, network infrastructure components, applications, services, protocols, virtualisation and malware
- Knowledge of process oriented IT management (e.g. ITIL), programming languages and methodologies are a plus
- Excellent command of the team’s primary language and very good command of English, both in speaking and talking
- Good communicator and presenter
- Can write clear and well-organised written communications
- Strong sense of responsibility
- Sensitivity for the organisational, functional and managerial dynamic of the organisation
- Discreet and knows how to keep secrets

Competences:

- Situational awareness
- Communicative
- Very good analytical skills
- Client oriented
- Good convincer
- Collaborative
- Good planner
- Innovative
- Good integrity
- Resilient in stressful situations
- Flexible

Tasks

- Incident handling and coordination when on duty
- Collaborate with colleagues nationally and internationally on incident handling
- Information research and analysis leading to workable solutions
- Giving advice on preventive and mitigating security measures (technical)
- Communication with the constituency
- Writing security advisories and alerts
- Assist with security investigations or audits

2.2.1.1.2 Senior specialist & incident handler

Functional requirements:

- Technical education on academic level (bachelor or master) or comparable
- A minimum of 10 years working experience in an IT function, with at least 5 years in a security function
- Experience gained by working inside a CSIRT/CERT or SOC is a plus
- Excellent skills of communication and explanation, not only on user and technical level but also on management level. Experience gained by giving relevant trainings/courses is a plus.
- Recognition of sensitive situations and the ability to modify behaviour accordingly
- Leadership qualities and strong result focus

- Relevant security certifications like CISSP, CISA, CISM, CEH, relevant SANS, CERT/CC and other trainings – or similar or better experience
- Experience with standards, methods and techniques in the area of cyber security

Competences:

- Strong situational awareness
- Pro-actively communicative
- Sensitive to management challenges and issues
- Excellent analytical skills
- Client oriented
- Skilled in convincing others to take action
- Collaborative and inspiring
- Excellent organiser
- Innovative
- Strong Integrity
- Capable of handling stressful, sometimes complex situations
- Highly flexible

Tasks

- Incident handling and coordination when on duty
- Coordinating the handling of complex/sensitive incidents
- Collaborate with colleagues nationally and internationally on incident handling
- Information research and analysis leading to workable solutions (also on own initiative)
- Giving advice on preventive and mitigating security measures (technical, but also security awareness and organisational measures)
- Giving advice on communication to various stakeholders
- Writing security advisories and alerts, preparing reports
- Carry out security investigations or audits

2.2.1.1.3 General Manager

Functional requirements:

- Education on academic level (bachelor or master) or comparable – a technical orientation is a plus
- A minimum of fifteen years working experience, of which at least ten years in or close to IT, and at least five years in a management function
- Experience gained by working with or inside a CSIRT/CERT or SOC is a plus
- Excellent communication skills on both a management level and also with staff members
- Relevant certifications in communication/presentation abilities are a plus
- Very strong recognition of sensitive situations and the ability to steer the organisation accordingly
- Strong, inspiring leadership qualities and result-oriented

Competences:

- Strong organisational and human awareness
- Pro-actively communicative, consistently working towards lessons learnt
- Highly sensitive to management and human challenges

- Excellent decision making skills
- Oriented towards the mission of the team
- Ability to see and maintain the bigger picture
- Excellent convincer
- Collaborative and inspiring
- Excellent organiser and reliable leader
- Strong sense of integrity
- Strongly resilient in stressful, sometimes highly complex situations with communication on various organisational levels
- Highly adaptive

Tasks

- Create a working place for the team where every man and woman wants to give their best to contribute and feels safe and respected
- Tactical and strategic management
- Coordinating crises with “all hands on deck”
- Collaborate with colleagues nationally and internationally on how to improve the effectiveness of incident handling
- Communicate with (and report to) various stakeholders, like important clients and higher management
- Responsible for hiring new staff

2.2.1.2 Present job profiles plenary & discuss (45 minutes)

Each group should present their job profiles to the class. It may be displayed so everybody can see it.

*NOTE: this sub-task is also an exercise in communication & presentation. If the trainer is equipped to do so, it is certainly advisable to give the students some basic, **constructive** feedback on their way of presenting. [refer to ENISA trainer best practices guide]*

Next is a discussion of the skills that have the highest priority for each position. Ask students to list their top five priorities for the competencies of an ideal candidate for a particular position. Gather and order this on a whiteboard or flip-chart. If students missed any important items, add them to the list in discussion with them.

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.

2.2.2 Task 2: Writing job advertisements (60 min)

Explain to the students how important it is to translate the job profiles to readable, understandable, engaging and inspiring job advertisements: after all, you are looking for the best candidates, not for average ones. See it this way: if you want mediocre candidates, then just list the requirements in a job advertisements. If you want the best and most inspired candidates, then consider it an honour that they will work for your team and write the job advertisement from that perspective, making sure that you motivate and inspire such potential candidates to *desire* to work for your team. Engage their passion!

2.2.2.1 Write job advertisements for the job profiles (30 minutes)

Use the same groups as in 4.2. Make sure that job advertisements are written for all profiles established in 4.2 – but make sure that each group does *not* work on the profile they made previously, but on one of the other profiles. Again, motivate the students to think out of the box and be creative: after all they want to find the best candidates, and inspiring colleagues.

NOTE: this sub-task is also an exercise in (quick) writing skills, which is important for most CSIRT members, as it is required both for writing e-mails to especially constituents, as well as for the writing of alerts & warnings.

2.2.2.2 Present job advertisements plenary & discuss (30 minutes)

Each group should present their job advertisements to the class. They may be displayed so everybody can see them.

*NOTE: this sub-task is also an exercise in communication & presentation, essential skills for most if not all CSIRT members. If the trainer feels equipped to do so, it is certainly advisable to give the students some basic, **constructive** feedback on their way of presenting. (See e.g. [10])*

Next is a discussion of the job advertisements to see how to make them even better.

2.2.3 Task 3: Analysing and choosing candidates to be interviewed (90 minutes)

Explain to the students how important the analysis and choice of interviewees is, but that it is more than just counting how many skills and how many years match what's in the job profile. Make sure that there is sufficient focus on soft skills and not only technical ones. Also teach students to look for the unexpected and the unwritten, thus pre-teaching part of the next task. It also needs to be made clear that this process can *not* be left only to HR and/or management - CSIRT team members must be involved. To leave pre-selection to an HR staff member or, even worse, an external recruiter, surrenders your chance to get the best people for the job, colleagues that the students want to have, to make the CSIRT not only very effective, but also an inspiring environment to work in.

2.2.3.1 Study CVs, make SWOT analysis and select candidates for interviews (45 minutes)

In this sub-task form new groups, one per job profile. The maximum group size should not exceed five students, or some people will be left behind in the discussions. In case of a large class, assign more than one group to each profile.

Distribute a collection of six CVs (having selected them earlier from a collection of ten) to each group. It is assumed that all candidates have passed computer literacy tests at the level required to be a member of a CSIRT team. Students from each group analyse all the CVs and try to match them with the prepared job advertisements (and corresponding profiles). In parallel, students write short opinions about all the candidates based on SWOT analysis: strength, weaknesses, opportunities, threats (a SWOT template will be provided). At the end of this step, each group will decide which two candidates they want to interview.

Make sure to stress that choosing only TWO candidates for an interview is because of the format of this training and the time available. In real life, select as many candidates for interviews as you think *or feel* need to be interviewed, as you want to know more. Dare to include *feeling* indeed, as sometimes the potentially best candidate is not obvious from an only rational assessment of the CVs – sometimes you need to give candidates the chance for an interview simply based on *gut feeling*. One of the authors of this training has that way hired some of the very best people, who are now among the most respected individuals in the CSIRT community.

2.2.3.2 Present results plenary & discuss (45 minutes)

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. If really necessary, add to the selection (but preferably stick with the students' choice, for motivational reasons).

NOTE: this sub-task is also an exercise in communication & presentation, essential skills for most if not all CSIRT members. If the trainer feels equipped to do so, it is certainly advisable to give the students some basic, ***constructive*** *feedback on their way of presenting. (See e.g. [10])*

2.2.4 Task 4: Interviewing chosen candidates (150 minutes)

This phase is devoted to interviews. Each interview should not exceed fifteen minutes. Groups are the same as in the previous task.

2.2.4.1 Build questions for interviews (30 minutes)

First, let the students become familiar with the CSIRT Code of Practice (CCoP) that the European CSIRT community TF-CSIRT recommends as good practice for CSIRTs [5]. Afterwards, based on the CCoP as well as on the prepared job advertisements and the CVs of the chosen candidates, the groups propose up to twenty interview questions (five general, five technical, five communication/presentation, five others including ethics) that they would like to ask particular candidates of their choice.

2.2.4.2 Present questions plenary & discuss (30 minutes)

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

For the trainer's benefit, below you find a number of questions – of course the real number of questions is infinite: it cannot be stressed enough that interviewing is not a strictly defined process, and that even when you start from standard questions, the replies of the interviewee will often inspire non-prepared questions on the spot. Also, there must always be questions that are CV dependent! And finally, not all of the questions below will apply to **all** of the three profiles that we are using in this training – e.g. the general manager really does not need to an expert on honeypots!

This question collection is part of the rtf document that you are expected to make available to your students at the end of the training.

General questions	Rating/notes
1. Please introduce yourself.	
2. What were your expectations for your current/previous job and to what extent were they met?	
3. What were your responsibilities in your current/previous job?	

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. Who was your best boss and who was the worst? Explain why.	
7. Why do you want to leave your job? (Or, if applicable) What have you been doing since your last job? (Or, if applicable) Why were you fired?	
8. How do you handle stress and pressure?	
9. What motivates you? What makes you tick?	
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 do you handle it?	
12. Tell us about your most passionate hobby or pastime. (Discuss using a language other than your primary language if possible. E.g. a German-speaking team could discuss in English.)	
13. What interests you about our job?	
14. What do you know about our company/organisation/team?	
15. Why do you want to work here?	
16. What are your salary expectations?	
17. Is there anything I haven't told you about the job or company that you would like to know?	
18. What are your goals for the next five or ten years?	
19. Do you take work home with you?	
20. Are you willing to travel?	

Technical questions	Rating/notes
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. Suppose you connect a brand new computer for the first time to the Internet, and you type www.coca-cola.com in your favourite browser – explain the process of what happens in the background when that name is somehow converted into IP numbers? (Asking about how DNS works)	

5. What examples of network worms do you know? What are the methods for their propagation?	
6. How should information about new vulnerabilities or warnings of new threats be published?	
7. What are the most common motivations behind black hat hacking?	
8. Why would anyone want to infect a home computer?	
9. What is phishing? What techniques can be used to phish?	
10. What is a botnet? How can you take it down?	
11.Can you describe different types of DDoS attacks?	
12. What are countermeasures against DDoS attacks?	
13. What can you tell us about APTs?	
14. What do you think is the importance of the certificate system, with certificate authorities, etc.?	
15. Do you know of any problems with the certificate system in recent years, or vulnerabilities?	
16. What is the biggest threat and/or the most popular type of incident on the network handled by CSIRTs nowadays? (After reply) How do you know?	

Questions on soft skills, ethics and various	Rating/notes
1. What do you think about “ethical hacking”? Have you ever done it?	
2. What do you understand by the concept of ethics in the security industry? (Make it more specific to CSIRTs if they have experience there already)	
3. Think of yourselves working in our CSIRT and you need to talk with people who are not at all technically savvy, like end users or managers – how do you go about this, in order to get the results you want?	
4. Think of yourselves working in our CSIRT and you need to talk with our upper management. They don’t have a clue what we are doing, but they are responsible for our whole organisation and are used to making important decisions in a short amount of time. How do you go about this, in order to get the results you want?	
5. And suppose we ask you to talk with the press, as no one else is available to do it. Your supervisor is too busy with the major incident at hand and the PR spokesman is on holiday – how do you prepare, what do you do, and what do you **not do**?	

6. There is a branch of science where there is a pre-supposition that says “the meaning of communication is the response you get”. What do you think about that? Do you agree or disagree and why so?	
7. What would you do if you discovered a publicly-unknown software vulnerability?	
8. What national or international security organisations do you know? Do you know any CSIRT groups or conferences?	

2.2.4.3 Prepare roleplay for interviews (10 minutes)

Instead of rigidly deciding on a subset of questions to ask, make the groups design a role model - what interviewer will focus on what areas. The questions are starting points, not set in stone.

NOTE: a sub goal is to install free association for interviewers, rather than blindly following a pre-programmed list of questions. The rationale is that you want to select the best people - and you will not get the best people of you follow a rigid process of selection.

2.2.4.4 Establish volunteer interviewees (20 minutes)

Ask for volunteers from each group to play the roles of the chosen candidates. Note that the number of candidates chosen to be interviewed is planned to be four, or three if time requires. If there are no volunteers, you need to choose them. Seek to enhance learning: e.g. the students who worked on the senior expert position, will play the role of candidates for the medior expert, and vice versa. Volunteers receive copies of the CVs and get 15 minutes to prepare. At the same time, the rest of a group has a break. For volunteers’ information only: advise them to give answers that have ambiguity, are not too direct – this will happen in real life too. Also encourage them to pretend to have different personal abilities than they actually have – they play a role based on a CV, inspire them to go inside that role and play it!

2.2.4.5 Do interviews (60 minutes)

After the 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 (i.e. same CV), this candidate is interviewed by both groups in one interview. After each interview, the group should discuss the candidate’s answers and share their opinions. Summarize them and encourage students to ask additional questions if needed.

As the trainer, we advise that you point out at least the following aspects, which are really important when leading job interviews – preferably add your own experience and insights as well:

- Free association. What you want for people in CSIRTs is to have a strong capacity of “free association” – which also implies being able to think out of the box: thinking beyond the naked facts that are visible at a certain moment in time, by making a manifold of associations and thereby intuitively finding possible options to test, that are possibly rationally not quite clear yet. Steve Jobs once said “Intuition is a very powerful thing, more powerful than intellect, in my opinion.” Albert Einstein was even more explicit: “The only real valuable thing is intuition”. The way to find out about free association in a job interview, where time is limited, is to think of situations in real life (no need for them to be CSIRT-related as such work scenarios may take more time to paint in detail) where the interviewee is confronted with having to find a way or ways forward based on insufficient input and with challenges that can well be out of the ordinary. Such situations can even be bizarre (outside people’s normal experience), as those tend to be more challenging. The replies do not have to be “right” (and there often is no “right” answer) – what you are looking for in the replies is indeed free association, and the kind of curiosity and creativity that are so essential to the CSIRT business. If on the other hand you get replies like “well I can’t do anything because I don’t know enough” this should start to ring some alarm bells.

- Flexibility. Another quality essential in CSIRT work is to be able to follow the set process and rules (saves time, increases reliability) **but** at the same time to deviate from them when it is needed and be flexible. This is because in CSIRT work we often get confronted with standard situations, where the set process works fine. And then sometimes, we get cases which are subtly different, maybe very different or completely new. At that moment, flexibility is essential. Think of such cases, and they may also be outside CSIRT business, and test the interviewees’ willingness to go for the process **and also** deviate from it when necessary. If, on the other hand, you get a reply like “I always follow the process, that’s what the process is for”, you might not have the best possible candidate for the job.
- Use all information in the CV. To find questions for the above capacities of free association and flexibility, what often works is to look in the CV for specific work they have done or volunteer jobs that serve as basis for “intriguing questions”. Just as an example, if during their time at university they served as bar(wo)man in their student’s club, you can imagine they will have been confronted with some challenging situations, especially when students would have had too much to drink. Ask what they did, how did they solve the situation. Do their replies show creativity and flexibility?
- Surprise questions. This works especially well when you have more interviewers. Have one of the interviewers volunteer to do at least 1, maybe 2 surprise questions – questions which need to be surprising or bizarre enough to at least temporarily throw the interviewee off balance, into confusion. Confusion is the greatest state of learning. See and hear how they recover and react. This will give you at least some idea of the interviewees reaction to stress challenges, and again, of their creativity.
- Sense of humour. Last, but certainly not least: get some clues about the sense of humour of the interviewee. CSIRT work is teamwork, and especially in stressful, challenging situations, a proper sense of humour is a major asset.

2.2.5 Task 5: Final Selection & Summary (30 minutes)

This task combines the final selection of candidates with a discussion of the topic of this training.

2.2.5.1 Select best candidates (5 minutes)

After all the interviews, ask the students to prepare their personal opinions about all the candidates and to make their selections, and to consider their reasons for that selection. Then, ask them to vote for the candidates.

Note: The vote for the candidates itself is not interesting - it's about process and motivation. This will need to surface in the class discussion that is next.

2.2.5.2 Discuss selection with all students (25 minutes)

Write down the results of the selection on whiteboard or flip chart and then discuss it with the following questions:

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

3 Conclusions

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

- What they think are the most useful abilities for being part of a CSIRT team?
- How do they imagine an ideal candidate (technical and communication qualifications, personal abilities and other competencies) for different roles within a CSIRT 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 would they 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.

You can also mention that a candidate who has just graduated from university can be considered for a position in bigger teams as a junior researcher. This candidate should have, however, some past experience in Internet security activities such as capture the flag, research activity (or script kiddy…), etcetera.

4 Evaluation Metrics

Evaluate the profiles, advertisements 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, communication, personal, ethical)?
- Did the students propose adequate questions for conducting the interviews?

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

5 References

[1] Improved CSIRT Typology. Whereas older typologies for CSIRTs were one-dimensional and rather confusing, this new typology takes the approach of using 2 axes: one for scope (global, regional, sectoral, national, organisation internal, product) and one for constituency (government, research & education, national collaboration, financial, medical, law enforcement, etc.):

[2] FIRST CSIRT Services Framework. The traditional CERT/CC services list (https://www.cert.org/incident-management/services.cfm) is still widely in use, but FIRST decided it was time for a more substantial standard work on this essential topic. Between 2014 and 2016 they have been doing wide consultations in the CSIRT community to reach consensus on this new CSIRT services model: https://www.first.org/_assets/global/first-csirt-services-education-framework-first-final-draft.pdf

[3] CSIRT Maturity Kit. This collection of CSIRT best practices has a chapter on human aspects which covers: Code of Conduct, Personal Resilience, Skillset description and Training: https://check.ncsc.nl/static/CSIRT_MK_guide.pdf [chapter 3]

[4] SIM3: Security Incident Management Maturity Model. Currently (November 2016) the only CSIRT maturity model widely in use. The European CSIRT community TF-CSIRT bases their Certification scheme on this model since 2009. SIM3 has several categories of CSIRT parameters that can be measured – one of these is the H(uman) category, that is of interest here: https://www.trusted-introducer.org/SIM3-Reference-Model.pdf

[5] CCoP - CSIRT Code of Practice. This Code of Practice is for CSIRTs and their members in general. It was originally written in 2005 and adopted by the European CSIRT community TF-CSIRT as a best practice. The CCoP was updated and improved in 2016: https://www.trusted-introducer.org/CCoP_approved.pdf

[6] What Skills Are Needed When Staffing Your CSIRT? Universities and schools hardly train CSIRT professionals (yet). The CSIRT work is not mainstream. For most CSIRTs it is hard to very hard to find good professionals. Teams need to be well aware of what kind of people they are looking for and what kind of skills they need to have. The following write-up by CERT/CC of the skills required is an excellent one: https://www.cert.org/incident-management/csirt-development/csirt-staffing.cfm

[7] CERT organizational structure. ENISA offers an overview on CSIRT organisational structures in this document – as a team's staffing needs depend on the kind of organisation that they want to be, this is a worthwhile read: https://www.enisa.europa.eu/publications/csirt-setting-up-guide [chapter 6]

[8] Handbook for Computer Security Incident Response Teams. This pioneering work of 1998, updated in 2005, is still much referenced as it's the only CSIRT handbook that treats the majority of CSIRT relevant aspects in one book rather than specific aspects in depth: http://www.cert.org/archive/pdf/csirt-handbook.pdf [Staff issues, p.166-171]

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

[10]ENISA Good Practice Guide on Training Methodologies. The subtitle "How to become an effective and inspirational trainer" is sufficient explanation: https://www.enisa.europa.eu/publications/good-practice-guide-on-training-methodologies/at_download/fullReport

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