1. Job profile table

Profile role :		
Functional requirements	**Competencies**	**Tasks**
Other important aspects :		

2. Medior specialist & incident handler : example of real-life profile

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

3. Senior specialist & incident handler : example of real-life profile

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

4. General manager : example of real-life profile

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

5. SWOT analysis table

SWOT analysis **Profile role : …… Candidate :**			
Strengths	**Weaknesses**	**Opportunities**	**Threats**

6. Interview question collection

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?	

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