The Hague **Security Delta**

Wanted Security Professionals

An Analysis of Job Advertisements

HSD
The Hague Security Delta

Executive Summary

Access to talent is a crucial prerequisite for the creation of innovative security solutions and the growth of the security sector. A rising number of security courses, studies and security related vacancies demonstrate that the security domain is a fast-growing and interesting field with a need for sufficient qualified personnel. The Hague Security Delta (HSD) Office commissioned a study of recent job vacancies in the security domain to find out which qualifications employers seek and for which type of jobs.

The study has found that a significant amount of vacancy descriptions include confusing and sometimes unrealistic requirements. This may discourage candidates to apply for these jobs. One way employers could improve this situation and help solving the Human Capital problem would be by consistently using an agreed framework for career paths. The framework should include a cross-reference to the Dutch educational system and to professional certificates. Furthermore, an editorial check before publishing a job advert helps to prevent unclear and conflicting requirements.

Wanted Security Professionals

Job titles vary far and wide. The analysis, based on vacancies collected through publicly accessible recruitment websites, found 91 unique job titles amongst 127 job openings.

Some of these individual titles can be grouped into categories such as consultant, officer, engineer or security guard. However, this does not mean that jobs with similar titles describe similar tasks and requirements. For instance, within the cybersecurity subdomain, the job titles with the word ‘architect’ showed that the employers were in fact looking for a pen-tester, an auditor, a consultant or a solution engineer.

Candidates searching for jobs may find the plethora of titles confusing and misleading. They also might overlook suitable vacancies because some employers use creative job titles. In several cases the job title did not match the description of the role at all and there are a few examples where the job advertisement aimed to recruit candidates for several different jobs in one go. The potential effect is that employers and candidates miss out on each other.

The top 5 most in demand security professionals are (based on content of the job description)

1. Consultant Information Security
2. Security Guard
3. Information security officer
4. Cybersecurity specialist/engineer
5. Environment, Health and Safety (EHS) officer

Within cybersecurity, career paths are unclear, as there is hardly any distinction in tasks and required competences amongst roles in different competence areas and at different seniority levels. Employers search for cybersecurity generalists that master many different competences at the same time. The complexity of these descriptions may discourage candidates from other relevant professions to apply for a role in cybersecurity. Roles in safety & security are more structured. But although there are similarities between these jobs and cybersecurity jobs, the pathways between them are not indicated.

Required Education

Regarding the required education, there is a big difference between cybersecurity jobs and other safety & security jobs. Jobs in cybersecurity require, in 78% of the cases, a higher education degree (HBO and WO in Dutch). Employers ask for a wide variety of degrees, varying from information sciences or computing, to management & business and law studies. In contrast, 76% of the safety & security jobs require a vocational level education in security or environmental management (in Dutch: MBO or VMBO) or do not state any requirements at all.

Amongst the cybersecurity jobs, employers tend to state that the candidate should have either a degree from a university of applied sciences (HBO) or university level education (WO) background. This is remarkable, as higher vocational education institutes and universities provide different types of education. This suggests that employers do not acknowledge this difference. Further confusion arises when employers use the terms Bachelor or Master. Employers do not specifically ask for any of these, instead they just state: 'Bachelor or Master' while there is at least one year of additional education between them.

Within cybersecurity, 56% of the employers ask for professional certificates (the research found 46 unique desired certificates). This is where employers demonstrate insufficient knowledge of the professional development and career paths of cybersecurity professionals. In fact, this group asks for 'one or more of the following lists of certificates:….'. This is then followed by a list, showing certificates that support different career paths.

Moreover, some employers ask for certificates that do not exist. These could be typing errors but in two analysed cases the candidate needed to be 'ISO 27001 certified'. This is not possible as ISO 27001 is a certification for organisations, not for individuals. Furthermore, many professional certificates require proof of several years of working experience (usually five years). A significant amount of employers (19%) required less than five years of experience while at the same time asking for at least one of those certificates.

Certificates in the other safety & security jobs also seem to be diverse although they are only required in 10% of the jobs. A small number of employers ask for 'relevant safety & security certificates'.

Required Competences

Security professionals generally require similar character traits in both cybersecurity and the other safety & security jobs. Good communication skills, being able to work in a team as well as independently, and the ability to cope with stress are examples of traits that they all need. There are a few variations that stand out. In cybersecurity the ability to take initiative is highly valued and not often mentioned within the other safety & security jobs. In this domain there is a demand for a neat and professional appearance, which is rarely mentioned in cybersecurity jobs.

Communication skills in Dutch are required for 40% of all jobs. Additionally, for cybersecurity, 42% of employers ask specifically for a good command of the English language.

Safety & security job vacancies generally do not state many specific technical skills. The most frequently asked are knowledge of MS-office and affinity with computers. A few employers require knowledge of First Aid, ISO 14000, VCA certification requirements and management systems for EHS (KAM in Dutch) or ISO 9001.

On the other hand, the total list of competences mentioned in cybersecurity job vacancies counts no less than 85 different areas of technical knowledge. A large amount of the technical competences is related to working with products from different vendors.

Other Requirements

In the safety & security jobs it is common to perform some sort of background check or screening of the candidate (60% of all job openings). This can be a very confusing requirement for the potential candidates, as we found that there are 13 different names given to background checks and none of these employers explain what these checks entail. One employer explains that they will check out the candidate's social media profiles. For cybersecurity roles, background checks are less common (18%).

Some requirements may create a barrier for candidates to apply for the job. In the safety & security domain, the appearance of the candidate is of importance. This is shown by that fact that 20% of the employers require a neatly groomed person (in one case specifically without visible piercings, tattoos, or unconventional hairstyle). Two employers even ask for a photo of the candidate. Additionally, some employers state that they seek 'mentally healthy people'. Finally, there is one employer that specifically writes about the male technician that they will hire.

A driving licence is needed for 38% of the jobs in security. On top of that, in 18% of the cases the candidate needs to own a means of transportation without further explanation to which extend they need this for the execution of their work related tasks.

Working outside office hours or in shifts is generally more frequent in the broader security domain jobs (42% of all job listings) than in cybersecurity (10%), however, when selecting those jobs in cybersecurity with the key words: SOC, threat, and incident, it rises to 100%.

Recommendations

Employers and candidates could benefit from a consistent framework or model for career paths in security. The plethora of job titles and roles is confusing and not beneficial for both parties. Within the cybersecurity domain, some frameworks have been published by NIST, CyberSeek, and the Dutch Platform for Information Security (PvIB). However, there appear to be more cybersecurity-related roles than those frameworks accommodate. There is more clarity in the roles, tasks, and required education for safety & security jobs and a part of these are agreed upon through collective labour agreements (CAO in Dutch).

In some cases, finding the right candidates may benefit from mapping cross-overs between cybersecurity and safety. For example, roles such as information security officer and EHS officer require similar competences and working with comparable management systems. Working towards an agreed model for career paths in security and connecting these to competences, education and professional certificates is advisable. Additionally, agreeing on the use of a security-jargon dictionary may relieve the incorrect use and confusing diversity of terms.

Recruiters might also be able to help posting better job descriptions. A check on writing style, unclear requirements and unrealistic demands prevents the demotivation to apply within certain target groups.

The findings in this analysis for cybersecurity functions show that this area is still in its infancy from a human resources perspective. To improve the attraction and flow of talent, better constructed function profiles that are more logically related to each other and to existing education and certifications are needed. New security challenges will require current functions to be changed or new ones to be created. Developing talent to move from diminishing traditional roles into future careers requires effort from educators, employers, public institutions and talents themselves.

Table of Contents

1. Introduction

The Dutch security cluster 'The Hague Security Delta' (HSD) is a network of businesses, governments and knowledge institutions that work together on innovative security solutions and knowledge development. HSD Office, together with partners, addresses Human Capital issues that HSD partners are facing in the field of safety and security. Access to talent is a crucial prerequisite for the creation of innovative security solutions and the growth of the security sector.

To improve the availability of specialists in cybersecurity HSD Partners and the HSD Office launched a Human Capital Agenda for Cyber Security[1]. HSD partners are working together on projects for this purpose.

One of the challenges identified in the Human Capital Agenda is the gap in knowledge about the extent of the Human Capital problem. To optimise actions and projects, HSD analyses its online platform for education and job vacancies www.securitytalent.nl, collaborates with relevant stakeholders and researches trends in education and the job market[2]. However, there are still questions related to required skills and competences, function descriptions and career paths.

This report is the result of a study of job advertisements on public recruitment websites in the Netherlands. The study focused on the question what skills employers are looking for and for what roles. Furthermore, the study aimed to gain more insight in the relationship between writing style and motivation of candidates to apply.

1 https://www.thehaguesecuritydelta.com/media/com_hsd/report/109/document/20161208-HCA-Cyber-Security-DEF.pdf
2 https://securitytalent.nl/news/research-cbs-shift-in-employment-in-the-security-domain1

2. Research Method

For this study, job advertisements from public recruitment websites were analysed by using a method for content analysis. Content coding is a method that is frequently used to study job vacancies with the aim to discover employers' requirements[3],[4].

The texts were evaluated with an adopted version of the Critical Discourse Analysis method described by Wall, Stahl & Salam[5]. They describe the following steps: 1) identifying the problem, 2) specifying the literature, 3) developing codes for validity claims, 4) analysing content and coding, 5) reading and interpreting, 6) explaining the findings, and 7) engaging in critical reflexivity.

These steps were carried out as follows:

The identified problem is evidently the growing need for security professionals and with this study we hope to contribute to means to solve the shortage of skilled staff.

The job advertisements were retrieved from publicly available recruitment sites, with key words; IT security, cyber security, information security, security, safety and forensics.

The texts were searched for words and sentences related to job titles, competences and required education. The vacancies were coded manually, without software for content analysis. Furthermore, the writing style of a job advertisement can influence whether or not people will apply. Therefore, the texts were also tested for violations of validity claims such as:

- Understandability (the text is clear and understandable). An incomprehensible text with undefined concepts and jargon leads to confusion and insecurity of candidates to apply.
- Sincerity (the text is honest and rigorous). If the text is inconsistent, connotative with hyperboles, metaphors and jargon, the candidate may apply for a different job than advertised. This makes the employer look unreliable.
- Realistic (the requirement are realistic and probable). Unrealistic and irrational requirements lead to a mismatch between job description and candidates.
- Motivation (the text is inviting and stimulating). Writing style can promote stereotypes, ideologies and gender-coding. This includes unconscious bias: some words and the format of job advertisements may discourage women and minorities to apply.

The findings were discussed in a meeting with training & education partners and employer representatives at the HSD[6].

[3] Messum, D., Wilkes, L., Peters, K., & Jackson, D. (2016). Content analysis of vacancy advertisements for employability skills: Challenges and opportunities for informing curriculum development. *Journal of Teaching and Learning for Graduate Employability, 6* (1), 72-86.
[4] Ahsan, K., Ho, M., & Khan, S. (2013). Recruiting project managers: A comparative analysis of competencies and recruitment signals from job advertisements. Project Management Journal, 44(5), 36–54.
5 https://www.dora.dmu.ac.uk/xmlui/bitstream/handle/2086/11180/2015_Critical_Discourse_Analysis_Review_Methodology_CAIS%20(1).pdf?sequence=1&isAllowed=y
6 https://www.thehaguesecuritydelta.com/news/newsitem/1098-kick-off-future-jobs-and-talent-pool-in- safety-security

3. Findings

3.1 Job titles

Job titles vary far and wide. The analysis, based on job vacancies collected through publicly accessible recruitment websites, found 91 unique job titles amongst 127 job openings. Some of these individual titles can be grouped into categories such as consultant, officer, engineer or security guard. However, this does not mean that jobs with similar titles describe similar tasks and requirements. For instance, within the cybersecurity subdomain, the job titles with the word 'architect' showed that the employers were in fact looking for a pen-tester, an auditor, a consultant or a solution engineer.

Candidates searching for jobs may find the plethora of titles confusing and misleading. They also might overlook suitable vacancies because some employers use creative job titles. In several cases the job title did not match the description of the role at all and there are a few examples where the job advertisement aimed to recruit candidates for multiple jobs in one go. The potential effect is that employers and candidates miss out on each other.

After reorganizing the individual job titles (appendix 1), the following top 5 of most in demand security professionals appears:

1. Consultant Information Security (35% of all vacancies)
2. Security Guard (29%)
3. Information security officer (29%)
4. Environment, Health and Safety (EHS) officer (12%)
5. Cybersecurity SOC specialist (9%) and Cybersecurity engineer (9%)

Roles in safety & security are more structured. But although there are similarities between these jobs and cybersecurity jobs, the pathways between them are not indicated. Within cybersecurity, career paths are unclear, as there is hardly any distinction in tasks and required competences amongst roles in different competence areas and at different seniority levels. Employers search for cybersecurity generalists that master many different competences at the same time. The complexity of these descriptions may discourage candidates from other relevant professions to apply for a role in cybersecurity.

Based on job titles alone, it not possible to fit all of the job openings into career pathway frameworks for cybersecurity such as those presented by NIST[7], CyberSeek[8], or Platform voor Informatiebeveiliging[9]. This is partly due to the mismatch between the job title and description of the actual job, and partly because there appear to be more cybersecurity roles than those frameworks accommodate.

In contrast to the cybersecurity jobs, advertisements for safety & security jobs show more clarity in the roles, tasks, and required education. This may be because a part of these roles are agreed upon through collective labour agreements (CAO in Dutch)[10].

7 https://www.nist.gov/itl/applied-cybersecurity/nice/resources/nice-cybersecurity-workforce-framework
8 https://www.cyberseek.org
9 https://www.pvib.nl/actueel/nieuws/whitepaper-beroepsprofielen-informatiebeveiliging
10 https://www.fnv.nl/sector-en-cao/alle-sectoren/beveiliging/caos-beveiliging/

3.2 Education

Regarding the required education, there is a big difference between cybersecurity jobs and other safety & security jobs. Jobs in cybersecurity require, in 78% of the cases, a higher education degree (HBO and WO in Dutch). Employers ask for a wide variety of degrees, varying from information sciences or computing, to management & business and law studies. In contrast, 76% of the safety & security jobs require a vocational level education in security or environmental management (in Dutch: MBO or VMBO) or do not state any requirements at all.

Amongst the cybersecurity jobs, employers tend to state that the candidate should have either a degree from a university of applied science (HBO) or university level education (WO) background. This is remarkable, as these are different types of education. This suggests that employers do not acknowledge this difference. Further confusion arises when employers use the (for the Dutch education relatively new) terms Bachelor or Master. Employers do not specifically ask for any of these, instead they just state: 'Bachelor or Master' while there is at least one year additional education between them.

Within cybersecurity, 56% of the employers ask for professional certificates (the analysis found 46 unique desired certificates). This is where employers demonstrate insufficient knowledge of the professional development and career paths of cybersecurity professionals. In fact, this group asks for 'one or more of the following lists of certificates:....'. This is then followed by a list, showing certificates that support different career paths.

Moreover, some employers ask for certificates that do not exist. These could be typing errors but in two analysed cases the candidate needed to be 'ISO 27001 certified'. This is not possible as ISO 27001 is a certification for organisations, not for individuals. Furthermore, many professional certificates require proof of several years of working experience (usually five years). A significant amount of employers (19%) required less than five years of experience while at the same time asking for at least one of those certificates. Certificates in the Security & Safety domain also seem to be diverse although they are only required in 10% of the jobs. A few employers ask for 'relevant safety & security certificates'. A full list of required education and certificates is included in appendices 2,3, and 4.

3.3 Required skills and competences

Security professionals generally require similar character traits in both cybersecurity and the other safety & security jobs. Good communication skills, being able to work in a team as well as independently, and the ability to cope with stress are examples of traits that they all need. There are a few variations that stand out. In cybersecurity the ability to take initiative is highly valued and not often mentioned within the other safety & security jobs. In this domain there is a demand for a neat and professional appearance, which is rarely mentioned in cybersecurity jobs.

Communication skills in Dutch are required for 40% of all jobs. Additionally, for cybersecurity, 42% of employers ask specifically for a good command of the English language.

Safety & security jobs generally do not require a lot of specific technical skills. The most frequently asked are knowledge of MS-office and affinity with computers. A few employers require knowledge of First Aid, ISO 14000, VCA certification requirements and management systems for EHS (KAM in Dutch) or ISO 9001. On the other hand, the total list of competences mentioned in cybersecurity jobvacancies counts no less than 85 different areas of technical knowledge. A large amount of the technical competences is related to working with products from different vendors.

3.4 Other requirements

In the safety & security jobs it is common to perform some sort of background check or screening of the candidate (60% of all job openings). This can be a very confusing requirement for the potential candidates, as we found that there are 13 different names given to background checks and none of these employers explain what these checks entail. One employer explains that they will check out the candidate's social media profiles. For cybersecurity roles, background checks are less common (18%).

Some requirements may create a barrier for candidates to apply for the job. In the safety & security domain, the appearance of the candidate is of importance. This is shown by that fact that 20% of the employers require a neatly groomed person (in one case specifically without visible piercings, tattoos, or unconventional hairstyle). Two employers even ask for a photo of the candidate. Additionally, some employers state that they seek 'mentally healthy people'. Finally, there is one employer that specifically writes about the *male* technician that they will hire.

A driving licence is needed for 38% of the jobs in security. On top of that, in 18% of the cases the candidate needs to own a means of transportation without further explanation about to which extend they need this for the execution of their work related tasks.

Working outside office hours or in shifts is generally more frequent in the broader security domain jobs (42% of all job listings) than in cybersecurity (10%), however, when selecting those jobs in cybersecurity with the key words: SOC, threat, and incident, it rises to 100%.

3.5 Writing style

The writing style of a job advertisement can influence whether or not people will apply. This is important in the security domain, where there is a shortage of specialists in cybersecurity.

3.5.1 Understandability

A large part of job vacancies use abbreviations, jargon, passive tense (suggesting evasion of responsibility) , and unspecific concepts or verbs such as:

- you will be coordinating
- you will be taking care of
- you will be contributing to
- knowledge of security concepts
- knowledge of security products
- you will be confronting security challenges
- we may perform pre-employment screening
- you will create innovative concepts
- delivering of support with the execution
- acting as a manager
- striving to a solution
- enabling people to understand
- testing of the audits
- creating a good story for the board of directors

These examples of indirect or vague meanings and passive tense is confusing and leaves the text open for interpretation.

3.5.2 Sincerity & Reality

Multiple times the job title was not coherent with the job titles used in the text. This form of inconsistency puts the candidate on the wrong foot and make the employer look unreliable. Paragraph 3.2 describes most of the unrealistic requirements that employers state when they ask for combinations of professional certificates as well as the expected experience in years. Another example of a breach of the reality claim is one job description that contains no less than 46 different tasks for, even more surprisingly, a part-time job: 0,7 fte.

In a few cases, the employers combine several job vacancies into one advertisement. This leads to confusing and incorrect job titles, with the result that some candidates skip reading the advertisement at all because they do not expect the second (or third) job further along the text.

3.5.3 Motivation

Security is traditionally a male dominated area and words and the format of job advertisements may discourage women to apply. The majority of the job vacancies in security unconsciously use male stereotype language. This happens more often in cybersecurity job descriptions than in safety & security vacancies. It is most evident in the requirements for soft skills or character traits. In cybersecurity, attractive candidates have traits that are associated with male stereotypes such as pro-active, influencer, leader, competitive, prevalence or forcing.

It is rare for employers to indicate their salary budget as a motivator to apply. Most state that the salary is competitive (for cybersecurity roles) or compliant with the CAO (for safety & security jobs). There is generally more emphasis on the perks that come with the job such as permanent education, laptops, smartphones, sustainable offices, good coffee, brainfood and fruit, personal trainers and massages.

Many employers seem to be blurring the line between work and private life. They highlight their social events, dinners, after-work drinking habits, parties and weekend trips. This may be useful for employers to attract certain personalities, but it seems an superfluous luxury to select candidates on these types of sociabilities in a market where there is a shortage of experts.

Many candidates are attracted to the security profession because of the cool-factor of the work and the contribution to society. Unfortunately, some employers fail to appeal to this motivation. In cybersecurity, jobs aim to keep external auditors at length or to satisfy the board of directors. These descriptions use words like being in control, enabling the business, and proof of compliance. For example, one description of the role of an EHS-officer has as goal to sanction people for non-conformances. This suggests that security is a hostile environment. On a positive note, some employers do express the meaning of working in security and refer that we are all have a part in keeping our society safe and secure.

4. Conclusion

There is large need for security professionals but employers, especially in cybersecurity, seem to struggle to define what kind of professionals they need. Unlike safety & security professions, there is no agreement on function titles, required education and career paths in cybersecurity. This leads to a confusing and unrealistic set of requirements in job vacancies and task descriptions for cybersecurity professionals, which in turn may be discouraging for applicants or attract applicants that do not fit.

Employers searching for safety & security staff write more straightforward job vacancies, but use confusing terminology for pre-employment screening procedures. Furthermore, their emphasis on physical attributes or barriers to acceptance (screening and transportation) may discourage suitable applicants. In some cases one can question whether they meet discrimination and privacy guidelines.

Finally, the writing style of job advertisements is often unconsciously biased. This demotivates certain groups from applying.

5. Recommendations

Employers and candidates could benefit from a consistent framework for security as a whole, completed with an overview of possible career paths in security. The plethora of job titles and roles is confusing and not beneficial for both parties. Within the cybersecurity domain, some frameworks have been published but there appear to be more cybersecurity roles than those frameworks accommodate. There is more clarity in the roles, tasks, and required education for safety and security jobs as a large part of these are agreed upon through collective labour agreements.

In some cases, finding the right candidates may benefit from mapping cross-overs between cybersecurity and safety. For example, roles such as information security officer and EHS officer require similar competences and working with comparable management systems. Aiming for a collective outline of competences, education and professional certificates is advisable to support carreers and attract new talent. Additionally, agreeing on the use of a security-jargon dictionary may relieve the incorrect use and confusing diversity of terms.

Recruitment sites might also be able to help employers to post better job descriptions. For instance, background checking of candidates is a common requirement, but it is presented with a confusingly long list of different names. It may help if recruitment sites create a field with a closed list of possible options for background checks with reference to an explanation of the process. Furthermore, a content editor could conduct a final check on writing style, possible illegal requirements and unrealistic demands. Finally, hiring managers should also review job descriptions for masculine terms and balancing these with feminine words such as collaborative, supportive, trust, or considerate in order to convey a diverse workforce[11]. They could also take the opportunity to emphasise how society benefits from security roles. Working in security has a degree of ‘coolness’ that makes it very attractive to many people, but it is hardly used as a selling point in job advertisements.

The findings in this analysis for cybersecurity functions show that this area is still in its infancy from a human resources perspective. To improve the attraction and flow of talent, better constructed function profiles that are more logically related to each other and to existing education and certifications are needed. New security challenges will require current functions to be changed or new ones to be created. Developing talent to move from diminishing traditional roles into future careers requires effort from educators, employers, public institutions and talents themselves. Harmonization of career paths and education will contribute to a mature and attractive profession and will stimulate candidates to choose a career in security and stay there.

[11] Frankland, J. (2017). IN Security. Why a failure to attract and retain women in cybersecurity is making us all less safe. Great Britain, Rethink Press.

Appendices

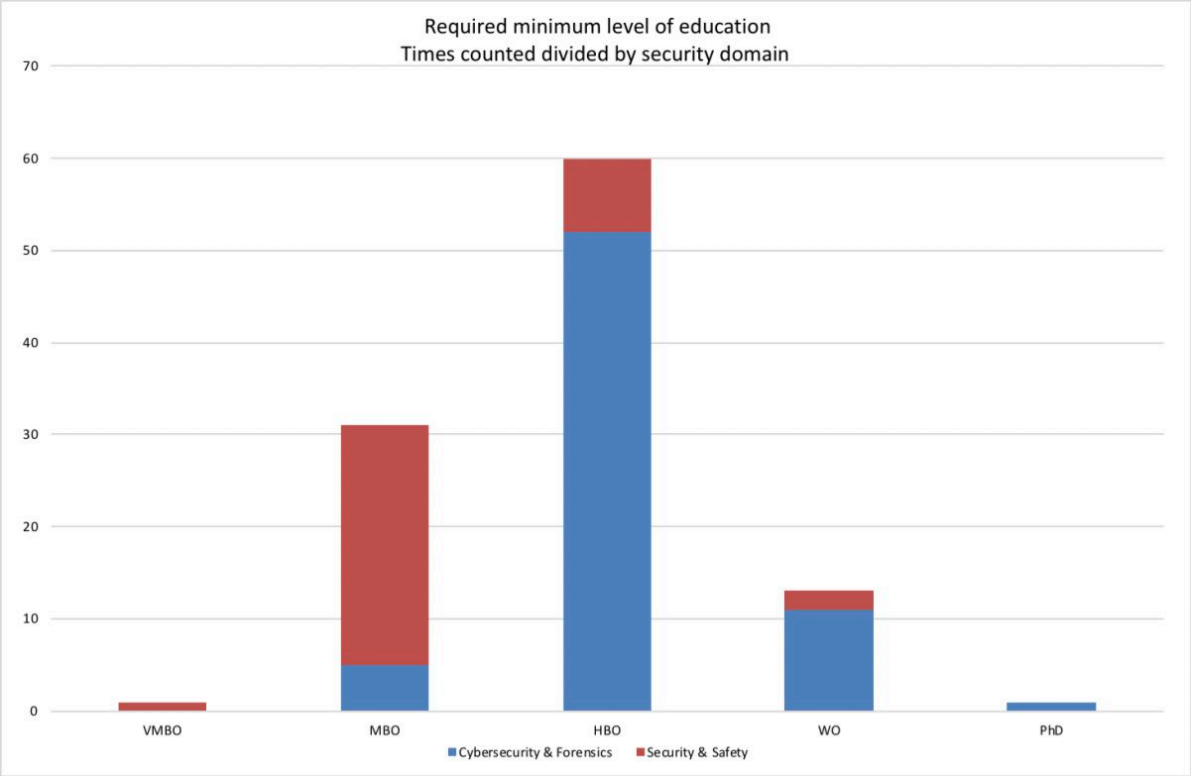
Appendix 1: Security Functions and Job Titles (in Dutch)

Function	Jobtitles
Consultant Cybersecurity	(junior) IT Auditor
	Adviseur informatie & databeveiliging
	Adviseur informatiebeveiliging
	Adviseur informatiebeveiliging & privacy
	Consultant cybersecurity & risk management
	Consultant informatiebeveiliging
	Cybersecurity engineer
	ICT security specialist
	Informatiebeveiliging specialist
	Information security consultant/security architect
	IT risk consultant
	IT security specialist
	Junior Adviseur informatiebeveiliging
	Junior security consultant
	Microsoft security & compliance professional
	Security Architect
	Security consultant
	Security manager/specialist
	Senior consultant cybersecurity
	Senior consultant software security & privacy m/v
	Senior ethical hacker/technical security specialist
Beveiliger	Beveiliger
	Object beveiliger
	Algemeen beveiligingsmedewerker
	Allround beveiliger
	Beveiliger transport
	Camera Observant
	Complexbeveiliger
	Luchthavenbeveiliger
	Nachtwaker Zorg
	Oproepkracht beveiliger en/of verkeersregelaar
	Parttime corporate beveiliger met diploma
	Problem Solver
	Security Officer
	Senior facilitair medewerker security
	Spotter
	Teamleider X-ray
	Zone profit protection manager

Information Security Officer	Adviseur informatiebeveiliging
	Information security manager
	Information security officer
	Information security officer ICT
	IT&C security consultant
	Medior adviseur informatiebeveiliging
	Risk Officer IT
	Security informatieanalist
	Security officer
	Security officer ICT
	Security/privacy officer
	Senior beleidsmedewerker cybersecurity
EHS/KAM officer	Adviseur Veiligheid en Milieu
	Hoofd veiligheid
	KAM coordinator
	KAM manager
	Medewerker quality, environment, safety & health
	Safety and physical security agent
	Senior KAM functionaris (veiligheid)
	Vakspecialist veiligheid
	Veiligheidskundige
Cybersecurity Engineer	2e lijns support engineer
	IT architect cybersecurity
	IT wizard
	Network engineer
	Security engineer/network engieer
	Senior SIEM engineer
	Solutions expert
SOC specialist	Cybersecurity analyst
	Incident response/forensic analyst (optional ransomware responder)
	Security analist SOC (m/v)
	Security specialist SOC
	Security specialist
	Senior security specialist incident response
Onderwijs/onderzoek	(junior) onderzoeker IoT security
	Assistant professor cybersecurity goverance and/or regulations
	Professional cyber resilence & cyber operations
	Projectmanager
	Senior business developer safety & security/digitalisering
Openbare Orde	Agent
	Brandweerofficier
	Controleur openbare ruimte/mountainbiker
	Medior handhaver
	Surveillant
Service/techniek	Beveiligingsmonteur
	Medewerker service en onderhoud
	Onderhouds- en servicemonteurs
	Servicetechnicus Beveiliging

Intelligence	Adviesmedewerker
	Adviseur veiligheid
	Dreigingsinschatter
	Junior politiek-strategisch analist
CISO/Manager	Chief information security officer
	Corporate information security officer
	Manager information security
	Programmaleider infrastructuur- en informatiebeveiliging
	Teamlead IT security
Cybersecurity Tester	Security tester
	Security/pentest expert (applicatiebeveiliging)
Forensisch specialist	Forensic intelligencespecialist
	Forensisch software engineer (master)
	Senior forensich adviseur
Cybersecurity Architect	IT security architect
	Security architect

Appendix 2: Required Education andd Certificates (in Dutch)



Function	Required Education
Consultant Cybersecurity	HBO/WO met sterk ICT component
	Bedrijfskundige HBO/WO opleiding
	HBO/WO
	HBO/WO in richting van IT of soortgelijk
	HBO/WO informatica of bedrijfskundige informatica
	Relevante HBO
	WO werk- en denkniveau
	Bachelor of master opleiding bedrijfsinformatica of security management
	HBO werk- en denkniveau
	HBO/WO IT-opleiding
	HBO/WO opleiding en overeenkomstig werk- en denkniveau
	HBO/WO niveau
	MBO niveau 4
	Bachelor or master in ICT or security management
	HBO/WO bedrijfskunde, informatica (specialisatie in cyber security)
	HBO/WO informatica of vergelijkbaar
	HBO
	Juridische WO
Beveiliger	ABM of MBO beveiliger 2
	MBO 3
	MBO werk- en denkniveau
	MBO
Information Security Officer	HBO werk- en denkniveau
	HBO/WO werk- en denkniveau
	HBO security management of bedrijfskundige informatica
	HBO richting (technische) bedrijfskunde, economie en/of toegepaste techniek
	HBO
	HBO richting ICT
	HBO+/WO werk- en denkniveau
	HBO niveau en een afgeronde opleiding in de richting van informatiebeveiliging of informatica
	HBO met duidelijke IT component
EHS/KAM officer	MBO veiligheidskunde
	MBO veiligheid en milieu, zoals mvk
	MBO/HBO milieukunde
	HBO
	HBO werk- en denkniveau met een afgeronde opleiding
	Ervaring op hbo+ niveau of starter op academisch niveau
Cybersecurity Engineer	WO opleiding
	MBO+/HBO

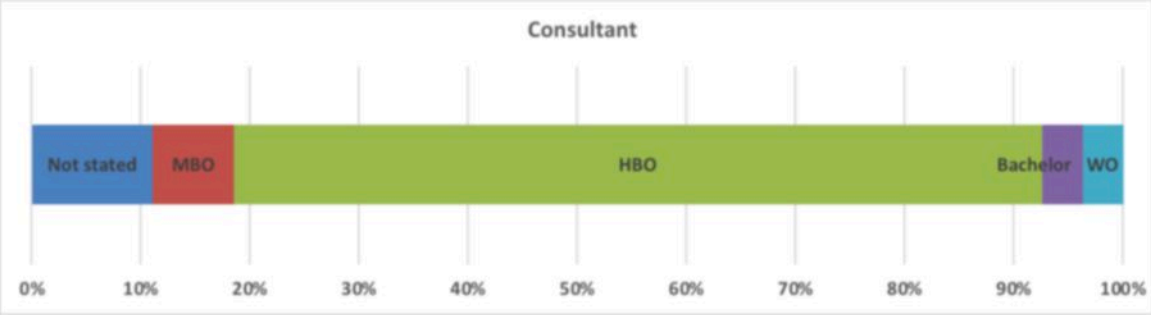
	HBO gericht op netwerkinfrastrucutren of een security focus of MBO met aantoonbaar HBO werk- en denkniveau
	Bachelor of vergelijkbaar
SOC specialist	Relevante HBO opleiding
	HBO diploma of vergelijkbaar op gebied van cybersecurity, informatica of informatiekunde (bijvoorbeeld data science)
	MBO 4 ICT of HBO
	HBO/WO
Onderwijs/onderzoek	PhD in security studies, governance, political science, public administration, sociology or law
	WO
Openbare Orde	Vmbo gl/tl of mbo-3
	MBO handhaving en/of toezicht
	HBO of academische bachelor
	MBO-3
Service/techniek	Technisch MBO-diploma
	MBO electronica
	MBO-3 electrotechniek aangevuld met MBV diploma
	MBV
Intelligence	HBO
	WO contemporaine geschiedenis, internationale betrekkingenof politicologie
CISO/Manager	Relevante WO opleiding
	Opleiding op academisch niveau binnen het vakgebied informatiebeveiliging
	WO werk- en denkniveau
	Master opleiding informatiemanagement of (bedrijfskudige) informatica
	Academisch werk- en denkniveau in een bedrijfskundige of informatie-technische richting
Cybersecurity Tester	HBO/WO denk- en werkniveau
Forensisch specialist	WO technische informatica of software engineering
	HBO -diploma op relevant gebied: forensic science, criminalistiek (straf)recht of natuurwetenschappen
	HBO
Cybersecurity Architect	Bachelor in technical study

Appendix 3: Education and Certificates for Most Demanded Functions

Consultant Information Security

Common competences	Top certifications requested
• Security testing/hacking • Advising technical measures of control • Secure software development • Firewalls • Identity & Access Management	• CISSP • CISA • CEH • CISM • RE • CIPP/e

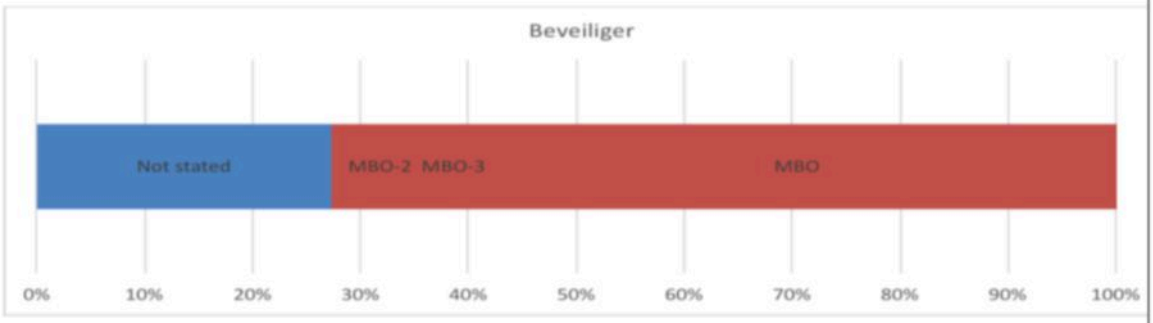
minimum level of education



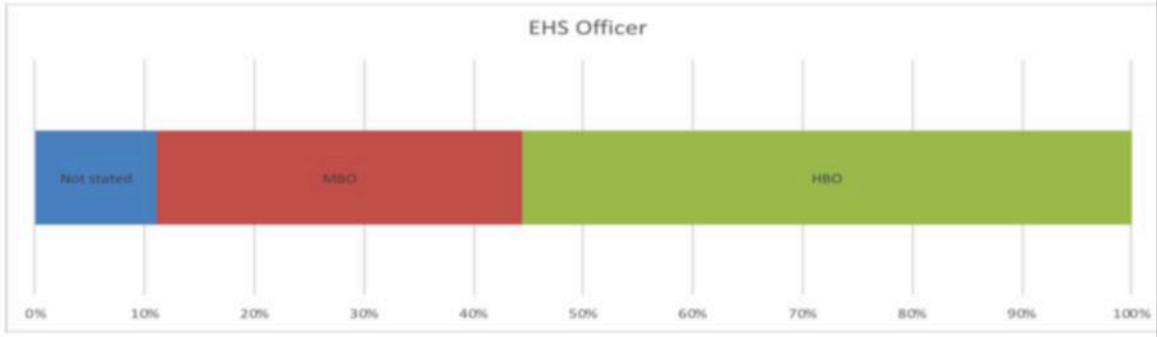
Security guard

Common competences	Top certifications requested
• Affinity with computers • MS Office	• Beveiliger-2 • First aid • ESO

minimum level of education



Information security officer	
Common competences • Advising technical measures of control • Secure software development • Infrastructure • Incident response • Beheer	**Top certifications requested** • CISSP • CISM • CISA • CRISC • CEH
minimum level of education 	

EHS officer	
Common competences • VCA • MS Office • ISO 14001 • EHS/KAM management systems • ISO 9001	**Top certifications requested** • HVK
minimum level of education 	

SOC specialist

Common competences

- Linux
- Unix
- Windows
- Networks
- Incident response

Top certifications requested

- GIAC
- GCIH
- GCIA
- GCFE
- EnCE

minimum level of education

Cybersecurity Engineer

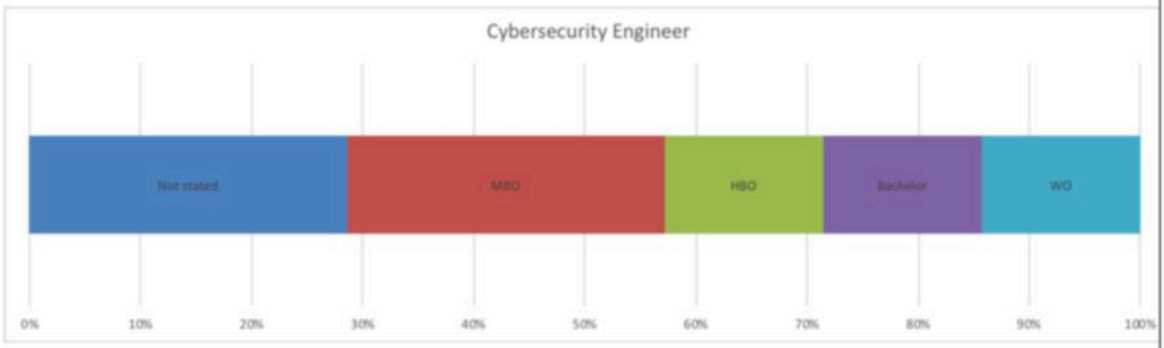
Common competences

- Infrastructure
- Networks
- Firewall
- Switches
- Routers

Top certifications requested

- CISSP
- CISM
- CISA
- CEH
- CCSK
- JNCIP
- ACMP
- ACCP
- CNSE
- CICA
- CTS

minimum level of education



Appendix 4: Professional Certificates (in Dutch)

Cybersecurity (77 vacatures)

Certificate	Total	Consultant	ISO	CISO/ Manager	SOC Specialist	Engineer	Other roles
CISSP	**33**	15	11	3		2	2
CISM	**23**	9	9	3		2	
CISA	**21**	11	6	2		2	
CEH	**15**	9	2		1	2	1
ISO 27001 auditor	**4**	4					
RE	**4**	4					
OSCP	**4**	1			1		2
CRISC	**3**	1	2				
CIPP/e	**3**	3					
CCSK	**3**	1				2	
MCITP	**2**	1				1	
JNCIP	**2**					2	
ACMP	**2**					2	
ACCP	**2**					2	
CNSE	**2**					2	
CICA	**2**					2	
CTS	**2**					2	
GICSP	**1**	1					
ISA CAP	**1**	1					
ISA/IEC 62443	**1**					1	
CDPO	**1**	1					
OCSE	**1**	1					1
ESCA	**1**						1
ECSP	**1**						1
EXIN ISMAS	**1**	1					
S-ISF	**1**	1					
S-ISME	**1**	1					
CCNA	**1**					1	
GCIH	**1**				1		
GCIA	**1**				1		
GREM	**1**				1		
GCFA	**1**				1		
GCFE	**1**				1		
EnCE	**1**				1		
Splunk administrator	**1**					1	
Splunk Architect	**1**					1	
CCSP	**1**	1					
CSSLP	**1**	1					
CSX	**1**	1					
CGEIT	**1**	1					

CCNP	**1**	1					
RHCE	**1**	1					
OSCP	**1**						1
eCPPT	**1**						1
Vmware	**1**					1	
Symantec+Blue Coat	**1**						l

Safety and Security (50 vacatures)

Certificaat	totaal	Beveiliger	KAM	Monteur	Overig
VCA	**5**	2		3	
EHBO/BHV	**5**	5			
MBV	**4**			4	
BOA	**2**				2
HVK	**2**		2		
ESO	**2**	2			
SKO	**1**		1		
Landelijk verkeersregelaars certificaat	**1**	1			
Beveiliging B	**1**	1			
Onderhoudskundige brandmeldinstallaties	**1**				
security certificates	**1**		1		
safety certificates	**1**		1		
law enforment certificates	**1**		1		
RTGB	**1**				1
beheerder brandmeldinstallatie	**1**	1			
Basistraining prijktijkopleiders in de beveiliging	**1**	1			
ISPS	**1**	1			
NEN 3140	**1**			1	
NEN 1010 training	**1**			1	
liftcertificaat	**1**			1	

Colophon

Wanted Security Professionals, An Analysis of Job Advertisements

Author

Nicole van Deursen

Commissioned by

Mark Ruijsendaal
Rik Schiffelers

The Hague Security Delta
Wilhelmina van Pruisenweg 104
2595 AN The Hague
info@thehaguesecuritydelta.com
www.thehaguesecuritydelta.com

@HSD_NL

The Hague Security Delta
Wilhelmina van Pruisenweg 104
2595 AN Den Haag
070 204 51 80

info@thehaguesecuritydelta.com
www.thehaguesecuritydelta.com
@HSD_NL