CYBER SECURITY DISTRICT

CYBERSECURITY SALARY GUIDE 2025

CYBERSECURITYDISTRICT.COM

CONTENTS

ABOUT US

Cyber Security District is a recruitment agency with 100% focus on cyber security in The Netherlands. Founded in 2018 by an Ethical Hacker and an IT Recruiter, we have 7 years of experience leading efforts to bridge the cyber security talent gap by connecting organisations with top-tier candidates.

This comprehensive salary guide is the result of extensive research and data collection. Since 2018 we have conducted our annual surveys and we meticulously analysed over 2,500 vacancies and gathered salary data from various cyber security roles across The Netherlands. By leveraging our in-depth industry knowledge and placement data, we provide you an accurate picture of the current cyber security job market.

Contact us

hello@cybersecuritydistrict.com
+31 (0)20 21 01 608

Visit our office

Keizersgracht 209, 1016 DT
Amsterdam, The Netherlands

RECRUITMENT TRENDS 2024

In 2025, the cybersecurity landscape in the Netherlands continues to align with the global surge in awareness and investment in robust cybersecurity measures. The World Economic Forum reports a persistent global shortage of over **4 million** cybersecurity professionals, emphasizing the critical demand for skilled talent.

Dutch organizations, from multinational corporations to SMEs, are doubling down on securing their digital infrastructures to combat the escalating threat of cyberattacks.

In the Netherlands, both permanent and interim hiring models remain vital in the cybersecurity sector, offering flexible solutions to meet diverse organizational needs and address the talent gap effectively.

The choice between permanent and interim hiring depends on factors such as the organisation's budget, project timeline, strategic priorities, and existing workforce.

In recent years, the interim hiring model has gained traction in the Netherlands, particularly in industries with dynamic cybersecurity requirements such as finance, technology, and healthcare. However, permanent roles remain a cornerstone of many organizations' workforce strategies, reflecting a long-term commitment to building and maintaining robust cybersecurity capabilities in-house.

Ultimately, the optimal hiring approach depends on the unique needs and priorities of each organization, and many leverage a combination to effectively meet their cybersecurity objectives.

KEY TRENDS AFFECTING HIRING

In 2025, several key trends are redefining how organizations recruit and retain cybersecurity talent. These trends highlight both the challenges and opportunities in an ever-evolving threat landscape:

Cybersecurity Skills Shortage

The global cybersecurity workforce gap remains critical, with a shortage increase of 8% since last year. In Europe alone, a deficit of 300,000 skilled workers threatens innovation and increases vulnerabilities. Bridging this gap requires collaboration among governments, academia, and private companies to invest in training and align educational curriculums with industry needs.

AI in Cybersecurity

AI continues to revolutionize cybersecurity, enhancing threat detection, response automation, and vulnerability management. However, this shift also demands upskilling existing teams and addressing challenges posed by AI-powered cyberattacks.

As AI reshapes cybersecurity, the need for professionals skilled in AI tools and methods grows. Companies are leveraging internal training and partnerships with educational institutions to address this skills gap.

KEY TRENDS AFFECTING HIRING

Economic Constraints Impact Teams

Economic pressures have forced organizations to optimize resources, leading to tighter budgets and strategic prioritization. Outsourcing, automation, and cost-effective tools are being embraced to ensure robust security without overstretching resources.

Cloud Security Challenges

As cloud adoption accelerates, the need for robust cloud-specific security measures grows. Organizations are investing in tools, training, and frameworks to address risks and ensure compliance.

Geopolitical Tensions

Rising geopolitical conflicts amplify risks, particularly for critical infrastructure. Proactive defense measures, public-private collaborations, and threat intelligence are crucial to mitigating these threats.

The 2025 cybersecurity hiring landscape in the Netherlands is shaped by organizations taking proactive measures to strengthen defenses amidst a persistent skills shortage, economic pressures, and growing reliance on AI and cloud technologies. Geopolitical tensions and supply chain vulnerabilities further complicate the landscape, emphasizing the need for skilled professionals and innovative approaches to safeguard critical systems.

Since 2024, the cyber skills gap has increased by 8%, with two out of three organizations reporting moderate-to-critical skills gaps, including a lack of essential talent and skills to meet their security requirements.

World Economic Forum 2025

SALARIES 2025

APPLICATION DOMAIN

Application Security Specialist

Are responsible for identifying and mitigating security vulnerabilities in software applications. They ensure that software is secure from cyber threats and compliant with security standards.

Relevant certifications

- CSSLP (Certified Secure Software Lifecycle Professional)
- GWAPT (GIAC Web Application Penetration Tester),
- CEH (Certified Ethical Hacker)

Career roadmap

- Years of Experience: 2-5 years
- Previous roles: Software Developer or Security Analyst
- University degrees: Bachelor's in Computer Science, Software Engineering, or Cybersecurity

ENTRY	MID-LEVEL	SENIOR
1-3 years of exp.	4-7 years of exp.	8+ years of exp.
€34,000 - €50,000	€65,000 - €82,000	€80,000 - €115,000

SALARIES 2025

APPLICATION DOMAIN

DevSecOps

Integrate security practices into the DevOps process, ensuring that security is a key component throughout the software development lifecycle. They work to automate security checks and balance security with speed and efficiency.

Relevant certifications

- DevSecOps Foundation
- CSSLP
- CEH

Career roadmap

- Years of Experience: 2-5 years
- Previous roles: DevOps Engineer or Security Engineer
- University degrees: Bachelor's in Computer Science, Software Engineering, or Cybersecurity

ENTRY	MID-LEVEL	SENIOR
1-3 years of exp.	4-7 years of exp.	8+ years of exp.
€55,000 - €75,000	€68,000 - €83,000	€80,000 - €90,000

SALARIES 2025

APPLICATION DOMAIN

Security Software Developer

Create software solutions designed to enhance the security of applications and systems. They develop security tools and applications to protect against cyber threats.

Relevant certifications

- CSSLP
- CEH
- CASE (Certified Application Security Engineer)

Career roadmap

- Years of Experience: 1-3 years
- Previous roles: Software Developer or Application Security Engineer
- University degrees: Bachelor's in Computer Science, Software Engineering, or Cybersecurity

ENTRY	MID-LEVEL	SENIOR
1-3 years of exp.	4-7 years of exp.	8+ years of exp.
€42,000 - €51,000	€65,000 - €77,000	€85,000 - €102,000

SALARIES 2025

INVESTIGATION DOMAIN

Cybersecurity Researcher

Study and analyze various aspects of cybersecurity, including new threats, vulnerabilities, and defense mechanisms. They contribute to the development of new security technologies and protocols.

Relevant certifications

- CSSLP
- CEH
- OSCP

Career roadmap

- Years of Experience: 3-7 years
- Previous roles: Security Analyst and Penetration Tester
- University degrees: Bachelor's or Master's in Computer Science, Cybersecurity, or related fields

ENTRY
0-2 years of exp.

≈ €37,880

MID-LEVEL
2-5 years of exp.

≈ €55,320

EXPERIENCED
5-10 years of exp.

≈ €75,040

SENIOR
10+ years of exp.

€90,540 - €106,740

SALARIES 2025

INVESTIGATION DOMAIN

Incident Analyst

Monitor and analyze an organization's network for security breaches, investigate incidents, and implement measures to prevent future intrusions.

Relevant certifications

- GCIH (GIAC Certified Incident Handler)
- CEH
- CompTIA Security+

Career roadmap

- Years of Experience: 2-5 years
- Previous roles: Security Analyst and Network Security Engineer
- University degrees: Bachelor's in Computer Science, Information Technology, or Cybersecurity

ENTRY	MID-LEVEL	SENIOR
0-2 years of exp.	3-5 years of exp.	6+ years of exp.
€57,750 - €77,000	€77,000 - €115,500	€115,000 - €173,250

SALARIES 2025

INVESTIGATION DOMAIN

Malware Analyst

Study malicious software to understand its behavior, origins, and impact. They develop strategies and tools to detect, analyze, and mitigate malware threats.

Relevant certifications

- GREM (GIAC Reverse Engineering Malware)
- CEH
- GCFA (GIAC Certified Forensic Analyst)

Career roadmap

- Years of Experience: 3-7 years
- Previous roles: Security Analyst and Incident Responder
- University degrees: Bachelor's in Computer Science, Cybersecurity, or related fields

ENTRY	MID-LEVEL	SENIOR
0-2 years of exp.	3-5 years of exp.	6+ years of exp.
€40,000 - €44,872	€56,200 - €91,211	€60,000 - €90,000

SALARIES 2025

ARCHITECTURE DOMAIN

Cybersecurity Architect

Design and build secure network and computer systems, ensuring they can withstand and mitigate cybersecurity threats.

Relevant certifications

- CISSP
- SABSA (Sherwood Applied Business Security Architecture)
- TOGAF (The Open Group Architecture Framework)

Career roadmap

- Years of Experience: 5-10 years
- Previous roles: Security Engineer, Network Engineer, or Systems Architect
- University degrees: Bachelor's in Computer Science, Information Technology, or Cybersecurity

MID-LEVEL
4-7 years of exp.

€94,000 - €113,963

SENIOR
8+ years of exp.

€120,189 - €147,522

SALARIES 2025

ARCHITECTURE DOMAIN

Enterprise Security Architect

Design and implement comprehensive security architectures to protect an organization’s IT infrastructure. They ensure that security solutions align with business objectives and regulatory requirements, providing robust protection against cyber threats.

Relevant certifications

- CISSP
- SABSA
- TOGAF

Career roadmap

- Years of Experience: 7-10 years
- Previous roles: Security Architect, Network Security Engineer, or Security Engineer
- University degrees: Bachelor's in Computer Science, Information Technology, or Cybersecurity; Master's preferred

MID-LEVEL
4-7 years of exp.

€94,000 - €113,963

SENIOR
8+ years of exp.

€120,189 - €147,522

SALARIES 2025

NETWORKING DOMAIN

Network Security Engineer

Focus on protecting an organization’s network infrastructure by implementing firewalls, intrusion detection systems, and other security measures. They ensure the security of data transmission and prevent unauthorized access.

Relevant certifications

- CISSP
- CCNA Security (Cisco Certified Network Associate Security)
- CompTIA Security+

Career roadmap

- Years of Experience: 2-5 years
- Previous roles: Network Administrator or IT Support
- University degrees: Bachelor's in Computer Science, Information Technology, or Cybersecurity

ENTRY	MID-LEVEL	SENIOR
0-2 years of exp.	3-5 years of exp.	6+ years of exp.
€55,260 - €73,680	€58,600 - €86,724	€81,000 - €98,521

SALARIES 2025

OT DOMAIN

OT Security Specialist

Focuses on securing operational technology (OT) environments, including industrial control systems (ICS), SCADA systems, and critical infrastructure. They implement security measures to protect against cyber threats, ensure the integrity of industrial networks, and prevent unauthorized access to critical systems.

Relevant certifications

- GICSP
- CISSP
- CompTIA Security+
- IEC 62443 Certification

Career roadmap

- Years of Experience: 2-5 years
- Previous roles: Network Administrator, IT Support, ICS Engineer, or Security Analyst
- University degrees: Bachelor's in Computer Science, Information Technology, Cybersecurity, or related

ENTRY	MID-LEVEL	SENIOR
0-2 years of exp.	3-5 years of exp.	5+ years of exp.
€61,236 - €87,492	€61,236 - €87,492	€80,000 - €115,000

SALARIES 2025

CLOUD DOMAIN

Cloud Security Architect

Design and implement secure cloud computing environments for organizations. They develop security strategies, policies, and procedures to protect cloud-based systems and data, ensuring compliance with industry standards and regulatory requirements.

Relevant certifications

- CCSP
- CISSP
- AWS Certified Security – Specialty

Career roadmap

- Years of Experience: 7-10 years
- Previous roles: Cloud Security Engineer, Security Architect or Network Security Engineer
- University degrees: Bachelor's in Computer Science, Information Technology, or Cybersecurity; Master's preferred

MID-LEVEL
4-7 years of exp.

€94,000 - €113,963

SENIOR
8+ years of exp.

€120,189 - €147,522

SALARIES 2025

CLOUD DOMAIN

Cloud Security Engineer

Focus on implementing and managing security measures within cloud environments. They work to ensure that cloud infrastructure, applications, and data are secure from cyber threats, implementing best practices and security tools.

Relevant certifications

- CCSP
- AWS Certified Security – Specialty
- CompTIA Cloud+

Career roadmap

- Years of Experience: 3-7 years
- Previous roles: Security Engineer, Systems Engineer, or IT Administrator
- University degrees: Bachelor's in Computer Science, Information Technology, or Cybersecurity

ENTRY	MID-LEVEL	SENIOR
0-2 years of exp.	3-5 years of exp.	6+ years of exp.
€41,700 - €76,500	€59,800 - €85,410	€85,410 - €116,759

SALARIES 2025

GENERALIST DOMAIN

Security Auditor

Evaluate an organization's security policies, procedures, and controls to ensure compliance with regulatory requirements and industry standards. They identify vulnerabilities and recommend improvements to enhance overall security posture.

Relevant certifications

- CISA (Certified Information Systems Auditor)
- CISSP
- CRISC (Certified in Risk and Information Systems Control)

Career roadmap

- Years of Experience: 3-7 years
- Previous roles: IT Auditor or Security Analyst
- University degrees: Bachelor's in Computer Science, Information Technology, or Cybersecurity

ENTRY	MID-LEVEL	SENIOR
0-2 years of exp.	3-5 years of exp.	6+ years of exp.
≈ €42,000	≈ €46,046	€63,100 - €75,000

SALARIES 2025

GENERALIST DOMAIN

Consultant (Technical)

Technical Consultants provide specialized expertise in implementing and optimizing security technologies. They assist organizations in deploying and configuring security solutions, conducting technical assessments, and ensuring systems are secure.

Relevant certifications

- CISSP
- CEH
- CCSP (Certified Cloud Security Professional)

Career roadmap

- Years of Experience: 5-10 years
- Previous roles: Security Engineer or Network Security Engineer
- University degrees: Bachelor's in Computer Science, Information Technology, or Cybersecurity

ENTRY	MID-LEVEL	SENIOR
0-2 years of exp.	3-5 years of exp.	6+ years of exp.
≈ €57,354	€64,347 - €90,713	€90,713 - €97,308

SALARIES 2025

GENERALIST DOMAIN

Consultant (Non-Technical)

Non-Technical Consultants focus on advising organizations on security policies, compliance, risk management, and strategy. They help develop security frameworks and ensure alignment with business objectives and regulatory requirements without delving deeply into the technical aspects.

Relevant certifications

- CISM (Certified Information Security Manager)
- CISSP
- CRISC (Certified in Risk and Information Systems Control)

Career roadmap

- Years of Experience: 2-5 years
- Previous roles: Compliance Officer, Risk Manager or Security Compliance Specialist
- University degrees: Bachelor's in Business Administration, Information Systems; Master's in Business Administration or Information Security preferred

ENTRY	MID-LEVEL	SENIOR
0-2 years of exp.	3-5 years of exp.	6+ years of exp.
≈ €64,350	€75,000 - €90,000	€90,000 - €109,178

SALARIES 2025

OFFENSIVE DOMAIN

Pentester

Penetration Testers simulate cyberattacks on an organization’s systems to identify vulnerabilities and recommend improvements to enhance security.

Relevant certifications

- CEH
- OSCP (Offensive Security Certified Professional)
- GPEN (GIAC Penetration Tester)

Career roadmap

- Years of Experience: 2-5 years
- Previous roles: Security Analyst or Network Security Engineer
- University degrees: Bachelor's in Computer Science, Information Technology, or Cybersecurity

ENTRY	MID-LEVEL	SENIOR
0-2 years of exp.	3-5 years of exp.	6+ years of exp.
≈ €37,800	€52,000 - €61,042	€86,462 - €105,397

SALARIES 2025

OFFENSIVE DOMAIN

Pentester (Team Lead)

Penetration Testers simulate cyberattacks on an organization’s systems to identify vulnerabilities and recommend improvements to enhance security.

Relevant certifications

- CEH
- OSCP (Offensive Security Certified Professional)
- GPEN (GIAC Penetration Tester)

Career roadmap

- Years of Experience: 2-5 years
- Previous roles: Security Analyst or Network Security Engineer
- University degrees: Bachelor's in Computer Science, Information Technology, or Cybersecurity

MID-LEVEL
3-5 years of exp.

€60,000 - €80,000

SENIOR
6+ years of exp.

€80,000 - €116,585

SALARIES 2025

OFFENSIVE DOMAIN

Senior Red Team Expert

Lead advanced simulations of cyberattacks to test an organization's defenses. They design and execute complex scenarios, mentor junior team members, and provide strategic insights to improve security posture.

Relevant certifications

- OSCE
- CEH
- GPEN (GIAC Penetration Tester)

Career roadmap

- Years of Experience: 5-10 years
- Previous roles: Ethical Hacker, Penetration Tester or Security Consultant
- University degrees: Bachelor's or Master's in Computer Science, Cybersecurity, or related fields

SENIOR

6+ years of exp.

€80,000 - €120,000

SALARIES 2025

DEFENSIVE DOMAIN

SOC Analyst

Security Analysts monitor and analyze an organization’s network for security breaches, investigate incidents, and implement security measures to protect against threats.

Relevant certifications

- CEH
- CompTIA Security+
- GCIH (GIAC Certified Incident Handler)

Career roadmap

- Years of Experience: 0-5 years
- Previous roles: IT Support or Network Administrator
- University degrees: Bachelor's in Computer Science, Information Technology, or Cybersecurity

ENTRY LEVEL
0-2 years of exp.

€42,476 - €66,559

JUNIOR
2-4 years of exp.

≈ €53,250

MID-LEVEL
4-6 years of exp.

€53,000 - €65,541

SENIOR
5+ years of exp.

€88,291 - €109,428

SALARIES 2025

DEFENSIVE DOMAIN

Incident Response Specialist

Incident Responders are responsible for addressing and managing the aftermath of a security breach or cyberattack, mitigating the impact and recovering systems.

Relevant certifications

- GCIH
- ECIH (EC-Council Certified Incident Handler)
- CISM

Career roadmap

- Years of Experience: 5-10 years
- Previous roles: Security Analyst, Network Security Engineer or Security Engineer
- University degrees: Bachelor's in Computer Science, Information Technology, or Cybersecurity

JUNIOR	MID-LEVEL	SENIOR
2-4 years of exp.	4-6 years of exp.	6+ years of exp.
€71,914 - €102,212	€102,212 - €126,681	€126,681 - €150,000

SALARIES 2025

DEFENSIVE DOMAIN

Digital Forensics Specialist

Digital Forensics Specialists investigate cybercrimes by collecting, analyzing, and preserving digital evidence to support legal proceedings. They work on cases involving data breaches, fraud, and other cyber incidents, ensuring that evidence is handled according to legal standards.

Relevant certifications

- GCFA
- CCFP
- EnCE (EnCase Certified Examiner)

Career roadmap

- Years of Experience: 3-7 years
- Previous roles: Forensic Analyst or IT Security Analyst
- University degrees: Bachelor's in Computer Science, Information Technology, or Cybersecurity

ENTRY LEVEL
0-1 years of exp.

€40,000 - €55,000

JUNIOR
2-4 years of exp.

€55,000 - €70,000

MID-LEVEL
4-6 years of exp.

€70,000 - €85,000

SENIOR
6+ years of exp.

€85,000 - €100,000

SALARIES 2025

GOVERNANCE, RISK & COMPLIANCE

Privacy Officer

Privacy Officers are responsible for ensuring that an organization’s data handling practices comply with privacy laws and regulations. They develop and implement privacy policies, conduct privacy impact assessments, and oversee data protection strategies.

Relevant certifications

- CIPP (Certified Information Privacy Professional)
- CIPM (Certified Information Privacy Manager)
- CISSP

Career roadmap

- Years of Experience: 5-10 years
- Previous roles: Compliance Officer, Data Protection Officer or Legal Advisor
- University degrees: Bachelor's in Law, Information Systems, or related fields; Master's in Privacy Law or Data Protection preferred

ENTRY	MID-LEVEL	SENIOR
1-3 years of exp.	3-5 years of exp.	5+ years of exp.
≈ €41,275	≈ €57,246	≈ €70,485

SALARIES 2025

GOVERNANCE, RISK & COMPLIANCE

Cybersecurity Risk Manager

Cybersecurity Risk Managers identify, assess, and mitigate risks to an organization’s information systems. They develop risk management strategies, conduct risk assessments, and ensure that security measures align with business objectives.

Relevant certifications

- CRISC (Certified in Risk and Information Systems Control)
- CISSP
- CISM (Certified Information Security Manager)

Career roadmap

- Years of Experience: 5-10 years
- Previous roles: Security Analyst, Risk Analyst or Compliance Specialist
- University degrees: Bachelor's in Computer Science, Information Technology, or Risk Management; Master's preferred

ENTRY	MID-LEVEL	SENIOR
1-3 years of exp.	3-5 years of exp.	6+ years of exp.
≈ €64,953	≈ €92,318	≈ €114,418

SALARIES 2025

GOVERNANCE, RISK & COMPLIANCE

Identity Access Manager

Responsible for overseeing and maintaining an organization's identity and access management (IAM) framework. This includes implementing access controls, managing authentication protocols, ensuring compliance with security policies, and mitigating identity-related risks across IT systems.

Relevant certifications

- CISSP
- CISM
- Azure/AWS Certified Security – Specialty
- Okta Certified Professional

Career roadmap

- Years of Experience: 2-6 years
- Previous roles: Security Engineer, IAM Analyst, IT Security Administrator, Cybersecurity Consultant
- University degrees: Bachelor's in Computer Science, Information Technology, Cybersecurity, or a related

ENTRY	MID-LEVEL	SENIOR
0-2 years of exp.	2-5 years of exp.	5+ years of exp.
€55,000 - €63,000	≈ €66,160	≈ €95,424

SALARIES 2025

GOVERNANCE, RISK & COMPLIANCE

Information Security Officer

The ISO is responsible for developing, implementing, and managing an organization's information security policies, procedures, and systems. They ensure that information assets are adequately protected against potential threats.

Relevant certifications

- CISSP
- CISM (Certified Information Security Manager)
- CISA (Certified Information Systems Auditor

Career roadmap

- Years of Experience: 2-6 years
- Previous roles: Security Analyst, Cybersecurity Consultant
- University degrees: Bachelor's in Computer Science, Information Technology, or Cybersecurity

ENTRY	MID-LEVEL	SENIOR
1-3 years of exp.	3-5 years of exp.	5+ years of exp.
≈ €67,719	≈ €96,249	≈ €119,291

SALARIES 2025

GOVERNANCE, RISK & COMPLIANCE

Technical ISO

The TISO focuses on the technical aspects of an organization’s information security program. This includes implementing and managing technical controls, conducting vulnerability assessments, and ensuring the security of IT infrastructure.

Relevant certifications

- CISSP
- CEH
- OSCP (Offensive Security Certified Professional)

Career roadmap

- Years of Experience: 2-6 years
- Previous roles: Security Engineer, Penetration Tester, ISO or Cybersecurity Consultant
- University degrees: Bachelor's in Computer Science, Information Technology, or Cybersecurity

ENTRY	MID-LEVEL	SENIOR
0-2 years of exp.	2-5 years of exp.	5+ years of exp.
€40,000 - €55,000	€55,000 - €70,000	€70,000 - €85,000

SALARIES 2025

GOVERNANCE, RISK & COMPLIANCE

Data Protection Officer

Data Protection Officers (DPOs) are responsible for ensuring that an organization complies with data protection laws and regulations. They oversee data protection strategies, implement policies to protect personal data, and act as a point of contact for regulatory authorities and individuals whose data is processed by the organization.

Relevant certifications

- CIPP (Certified Information Privacy Professional)
- CIPM (Certified Information Privacy Manager)
- CISSP

Career roadmap

- Years of Experience: 2-5 years
- Previous roles: Privacy Officer, Compliance Officer, or Legal Advisor
- University degrees: Bachelor's in Law, Information Systems, or related fields; Master's in Privacy Law or Data Protection

ENTRY	MID-LEVEL	SENIOR
1-3 years of exp.	3-5 years of exp.	5+ years of exp.
≈ €41,208	≈ €57,246	≈ €70,485

SALARIES 2025

GOVERNANCE, RISK & COMPLIANCE

Chief Information Security Officer

The CISO is a senior executive responsible for developing and implementing an organization's information security strategy, overseeing the cybersecurity team, and ensuring compliance with regulatory requirements.

Relevant certifications

- CISSP
- CISM
- CGEIT (Certified in the Governance of Enterprise IT)

Career roadmap

- Years of Experience: 10+ years
- Previous roles: Security Manager, IT Director or Security Architect
- University degrees: Bachelor's in Computer Science, Information Technology, or Cybersecurity; Master's in Business Administration (MBA) or Information Security

SENIOR
10+ years of exp.

€118,847 - €180,000

SALARIES 2025

THREAT DOMAIN

Cyber Threat Intelligence Specialist

Cyber Threat Intelligence Specialists gather, analyze, and interpret data on cyber threats. They provide actionable intelligence to help organizations anticipate and defend against cyber attacks, staying ahead of emerging threats.

Relevant certifications

- GCTI (GIAC Cyber Threat Intelligence)
- CISSP
- CEH

Career roadmap

- Years of Experience: 3-7 years
- Previous roles: Security Analyst or Incident Responder
- University degrees: Bachelor's in Computer Science, Information Technology, or Cybersecurity

ENTRY	MID-LEVEL	SENIOR
1-2 years of exp.	2-5 years of exp.	5+ years of exp.
≈ €47,130	≈ €88,990	€95,622 - €108,568

SALARIES 2025

THREAT DOMAIN

Threat Hunter

Threat Hunters proactively search for hidden threats and potential security breaches within an organization's network. They analyze system logs, network traffic, and other data sources to detect and respond to advanced threats.

Relevant certifications

- GCIH (GIAC Certified Incident Handler)
- CEH
- CISSP

Career roadmap

- Years of Experience: 2-5 years
- Previous roles: Security Analyst or Incident Responder
- University degrees: Bachelor's in Computer Science, Information Technology, or Cybersecurity

MID-LEVEL
3-5 years of exp.

€70,000 - €90,000

SENIOR
6+ years of exp.

€90,000 - €130,000

SALARIES 2025

SALES DOMAIN

Cyber Security Sales

Cyber Security Sales professionals are responsible for selling cybersecurity products and services to businesses and organizations. They identify customer needs, present suitable solutions, and manage the sales process from prospecting to closing deals.

Relevant certifications

- CISSP
- CISM (Certified Information Security Manager)

Career roadmap

- Years of Experience: 2-5 years
- Previous roles: Sales Representative or Account Manager
- University degrees: Bachelor's in Business Administration, Marketing, or related fields

ENTRY	MID-LEVEL	SENIOR
0-2 years of exp.	2-5 years of exp.	5+ years of exp.
€40,000 - €55,000	€55,000 - €70,000	€70,000 - €85,000

SALARIES 2025

SALES DOMAIN

Pre Sales

Pre Sales professionals work closely with the sales team to provide technical expertise during the sales process. They demonstrate the features and benefits of cybersecurity products, answer technical questions, and help tailor solutions to meet customer requirements.

Relevant certifications

- CISSP
- CEH
- CCSP (Certified Cloud Security Professional)

Career roadmap

- Years of Experience: 3-7 years
- Previous roles: Technical Support Engineer or Security Engineer
- University degrees: Bachelor's in Computer Science, Information Technology, or Cybersecurity

JUNIOR	MID-LEVEL	SENIOR
1-3 years of exp.	3-5 years of exp.	6+ years of exp.
€55,000 - €70,000	€70,000 - €90,000	€90,000 - €130,000

Secondary benefits are crucial for attracting and retaining top cybersecurity talent, demonstrating an employer's commitment to their well-being and professional growth.

Cyber Security District

SECONDARY BENEFITS

Flexible Working

Cybersecurity professionals value flexibility in their work arrangements, including remote work options, hybrid models, and adaptable hours that support work-life balance and personal commitments.

Pension Plan

They seek organizations that contribute to pension schemes, ensuring long-term financial security and stability.

13th Salary

They appreciate employers that offer a 13th-month salary as an additional annual bonus, providing extra financial support and recognition for their work.

Paid Vacation Days

Most professionals prioritize offers that include at least 25 vacation days, paid parental leave, and sabbatical options, allowing them to rest, recharge, and manage personal responsibilities effectively.

Travel and Education Allowance

Value offers that provide allowances for travel expenses, or a company car, along with education funding for certifications (e.g., CISSP, CEH, CISM), conferences, and workshops.

READY TO FIND YOUR NEXT ROLE OR NEW HIRE?

WE CAN HELP.

Contact us

info@cybersecuritydistrict.com
+31 (0)20 21 01 608

Visit our office

Keizersgracht 209, 1016 DT Amsterdam, The Netherlands

CYBER
SECURITY
DISTRICT