TRANSPORT AND TELECOMMUNICATION INSTITUTE

Career report

Course: Introduction to Specialty and Digital Skills

Student: Igors Oļeiņikovs
Student code: 93642
Group: 4501BTA

Riga
2025

TABLE OF CONTENTS

1. Introduction

Cybersecurity represents one of the most resilient and fast-evolving technology careers, with strong long-term demand, diverse specializations, and meaningful work protecting people, organizations, and critical infrastructure. This report presents a career development plan in cybersecurity, specifically focusing on defensive security, cloud security, and incident response. The document outlines a career vision for the next 5-10 years, identifies the technical and professional skills required, analyzes the current job market for cybersecurity professionals, explains how academic coursework will support career development, and presents a detailed 5-year action plan with specific milestones and deliverables.

2. Career Vision (5-10 Years)

The target career role is **security engineer and technical specialist with strong AWS cloud security skills**, capable of engineering secure architectures, developing detection systems, analyzing threats, and implementing technical improvements that reduce risk across hybrid cloud environments. Role selection prioritizes positions emphasizing written communication, technical analysis, and automation over verbal interactions.

Target roles include SOC Analyst (Tier 1-2), Detection Engineer, Security Researcher/ Analyst, Digital Forensics Investigator, and Penetration Tester. These positions share common characteristics: they primarily involve monitoring dashboards, investigating alerts, creating detection rules, analyzing threats, and documenting findings in ticketing systems and written reports, with minimal requirements for verbal presentations or client-facing communication.

Medium-term objectives (Years 3-5) include progressing through the following career path: SOC Analyst (Tier 1) → Detection Engineer or Security Analyst (Tier 2) → AWS Cloud Security Specialist. During this progression, expertise development will focus on AWS cloud security services including EC2, S3, IAM, CloudTrail, GuardDuty, and Security Hub, combined with threat-informed defense capabilities using the MITRE ATT&CK framework (MITRE Corporation, 2025).

Long-term vision (Years 5+) is to advance toward specialized technical roles such as Senior Detection Engineer, AWS Security Architect, or Cloud Security Specialist. These positions leverage technical depth and written documentation skills while minimizing requirements for extensive verbal communication. This career path aligns with technical analysis strengths, systematic thinking, and written communication abilities, while providing meaningful work protecting digital infrastructure and data.

Career Choice Rationale: The cybersecurity field offers alignment with professional strengths and circumstances. Target roles emphasize technical expertise, analytical thinking, and written communication. SOC Analysts primarily work with dashboards and tickets,

Detection Engineers focus on code and detection rules, and Cloud Security Specialists engineer secure AWS infrastructures. These positions require minimal verbal interaction while offering intellectually challenging work with strong job security. The existing foundation in Oracle Cloud Infrastructure, Red Hat system administration, and development (Ruby, JavaScript, MuleSoft) provides a strong technical base for transitioning into AWS-focused security engineering (Bureau of Labor Statistics, 2025).

3. Required Knowledge and Skills

3.1. Technical Foundations

Comprehensive technical expertise across multiple cybersecurity domains is required. **Networking and operating systems** knowledge encompasses TCP/IP protocols, routing, DNS, VPNs, Windows and Linux administration, system logging, and security hardening—all essential for SOC investigations and engineering secure configurations.

Security engineering principles include identity and access management (IAM), network segmentation, least privilege principles, cryptography, secure configuration management, and zero-trust design patterns including SASE and SSE concepts (ENISA, 2025).

AWS cloud security expertise encompasses AWS IAM, EC2 security, S3 bucket policies, CloudTrail logging, GuardDuty threat detection, Security Hub, AWS Config, VPC security, KMS encryption, and hybrid threat protection across multi-cloud environments. This specialization differentiates candidates in the job market as organizations continue migrating to cloud-first architectures (AWS, 2025).

Threat detection and incident response competencies include SIEM content development, EDR telemetry analysis, alert triage, incident scoping, containment strategies, eradication procedures, recovery processes, and post-incident improvements. **Threat-informed defense** capability using MITRE ATT&CK enables mapping of adversary tactics and techniques to detection controls, improving coverage and response playbooks.

Application security fundamentals encompass OWASP Top 10 risks, SDLC security touchpoints, basic code review techniques, and DevSecOps practices to reduce exploitable vulnerabilities in software systems (OWASP, 2025).

3.2. Tools and Platforms

Industry-standard security tools across multiple categories are required. SIEM and SOAR platforms include Splunk, Elastic Stack, AWS Security Lake, and Sumo Logic. Endpoint and extended detection and response tools include CrowdStrike Falcon, SentinelOne, and Carbon Black. AWS cloud security tools include GuardDuty, Security Hub, CloudTrail, AWS Config, and Prowler. Network analysis tools include Wireshark and tcpdump. Vulnerability management tools include AWS Inspector, Nessus, Qualys, and OpenVAS. Scripting capabilities in Python and Bash for automation and AWS Lambda functions are required. Red-team tools including Burp Suite, Nmap, and Metasploit support development of adversary perspective essential for defensive work.

3.3. Certification Roadmap

Certification strategy balances foundational credentials with specialized expertise. Previously

completed relevant certifications include freeCodeCamp Responsive Web Design and JavaScript Algorithms, Microverse Ruby and Databases modules, Red Hat System Administrator (RH134), MuleSoft Certified Developer, Oracle Cloud Infrastructure Foundations 2021, Cisco Introduction to Cybersecurity, ISC² Candidate status, and Google Cloud Introduction to Generative AI.

In Years 1-2, AWS Certified Cloud Practitioner (Q1-Q2) and CompTIA Security+ SY0-701 (Q3-Q4) are pursued to establish security foundation and AWS cloud fundamentals. These certifications cover hybrid/cloud environments, governance, risk, compliance, incident response, identity management, and threats—widely recognized credentials for entry into SOC roles (CompTIA, 2025).

In Years 2-3, AWS Certified Security - Specialty is pursued, diving deep into AWS security engineering including IAM, encryption, monitoring with CloudTrail and GuardDuty, incident response, data protection, and infrastructure security. This certification leverages Oracle Cloud Infrastructure experience for faster AWS adoption.

In Years 3-4, GIAC GCIH (GIAC Certified Incident Handler) is earned to validate practical incident handling approaches, tooling, and response workflows with hands-on emphasis, complementing AWS security skills with defensive response capabilities (GIAC, 2025).

In Years 4-5+, CISSP (Certified Information Systems Security Professional) is pursued, a broad governance and architecture credential requiring professional experience. ISC² Candidate status can be leveraged to progress to Associate status after passing the exam, with full CISSP certification upon meeting the experience requirement. Optional credentials include OSCP+ for deep adversary tradecraft understanding or AWS Certified Solutions Architect for architectural design skills.

3.4. Professional Skills

Professional skills required for effective cybersecurity practice include strong written communication for incident reports, technical write-ups, threat analyses, and security playbooks. Structured reporting skills encompassing detailed findings documents, investigation timelines, and root cause analyses are essential. Asynchronous collaboration through ticketing systems, Slack and Teams messages, email, and documentation platforms enables effective distributed team contribution. Self-directed learning supporting independent engagement with threat intelligence sources, security advisories, and technology updates is required. Analytical thinking and problem-solving capabilities enable effective threat assessment and response. Technical documentation skills for creating runbooks, detection logic explanations, and security architecture diagrams support knowledge transfer and institutional learning.

Modern cybersecurity work emphasizes remote collaboration and written communication. Technical security roles primarily involve written reports, ticketing systems, chat platforms,

and documentation—with minimal requirements for phone calls or presentations. SOC environments typically use tickets and chat for communication, while detection engineering and threat analysis are largely independent technical work. This operational reality aligns with professional communication preferences and accessibility needs.

4. Job Market Analysis

4.1. Workforce Demand and Gap

The global cybersecurity workforce faces a significant talent shortage. According to the ISC² Cybersecurity Workforce Study 2025, there is an estimated global gap of approximately 4.8 million cybersecurity professionals, creating substantial opportunities for qualified candidates. In the United States, the Bureau of Labor Statistics projects 29% growth for Information Security Analysts from 2024 to 2034, significantly faster than the average for all occupations, with a median annual salary of $124,910 in May 2024. In Europe, ENISA estimates approximately 300,000-500,000 unfilled cybersecurity positions, with major markets like Germany, UK, and France contributing significantly to this gap (ISC², 2025; Bureau of Labor Statistics, 2025).

4.2. European Market Trends

The European cybersecurity market demonstrates strong growth trajectories. The market was valued at $67.79 billion in 2024 and is projected to reach $76.21 billion in 2025, expanding to $194.43 billion by 2033 at a compound annual growth rate of 12.42%. Average annual salaries across Europe reflect this demand: entry-level SOC Analysts earn €45,000-€52,000, mid-level Security Analysts earn €60,000-€70,000, and senior Security Engineers earn €75,000-€90,000+. The ENISA Threat Landscape 2025 report, analyzing 4,875 incidents from July 2024 to June 2025, identifies seven prime threats: threats against availability, ransomware, threats against data, malware, social engineering, information manipulation and interference, and supply chain attacks. The report highlights trends including zero-day exploits, complex DDoS attacks, expanding hacktivism, AI-enabled disinformation, and ongoing regional conflicts shaping the cybersecurity landscape (ENISA, 2025; Statista, 2025).

Table 1 below summarizes the European cybersecurity salary ranges by experience level:

Table 1: European Cybersecurity Salaries by Experience Level (2025)

Experience Level	Role Examples	Annual Salary (EUR)
Entry-Level (0-2 years)	Junior SOC Analyst, Security Analyst	€45,000 - €52,000
Mid-Level (3-5 years)	SOC Analyst Tier 2, Detection Engineer	€60,000 - €75,000
Senior (5-8 years)	Senior Security Engineer, Security Architect	€75,000 - €90,000
Expert (8+ years)	Lead Security Architect, Principal Engineer	€90,000 - €120,000+

Source: Compiled from Glassdoor, Salary.com, and industry reports (2025)

Figure 1: Salary Progression by Experience Level (Europe Average)

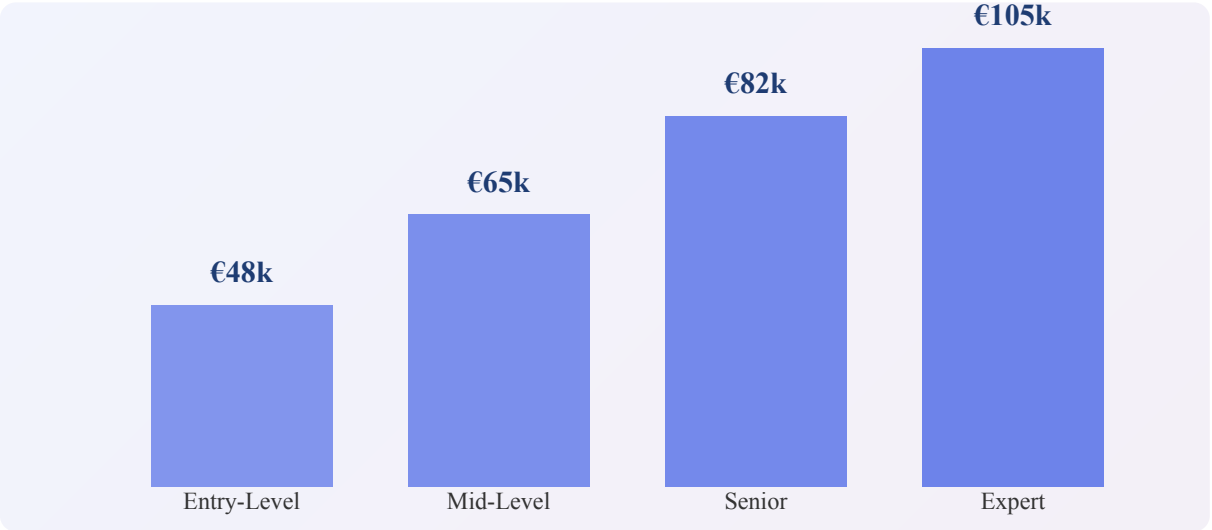
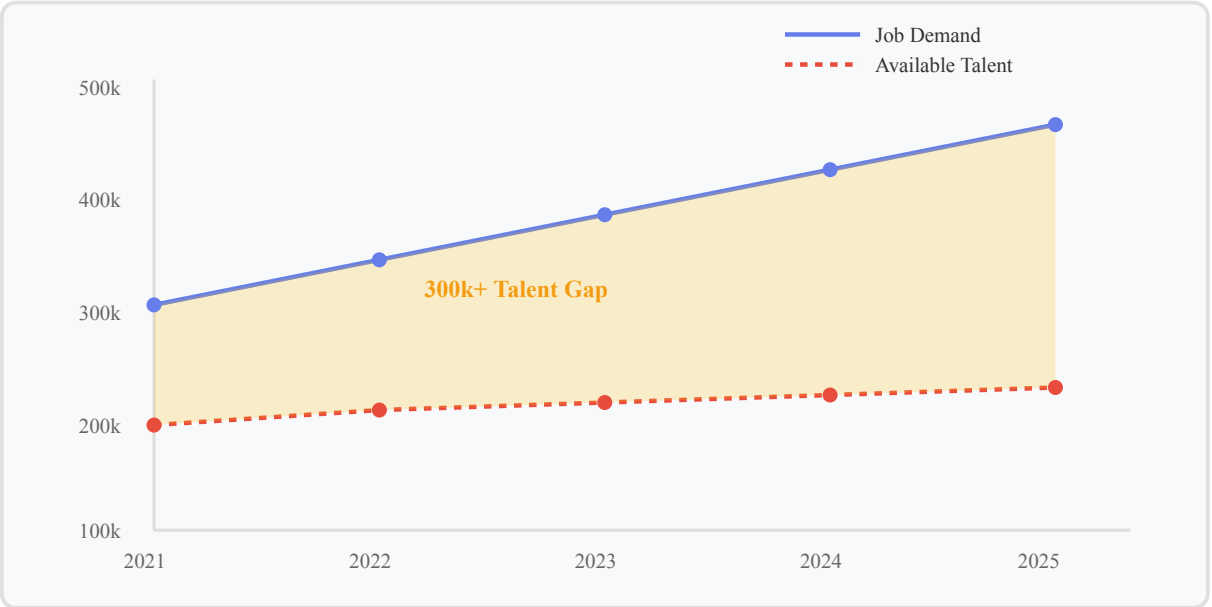


Figure 2: Europe Cybersecurity Job Market Growth (2021-2025)



4.3. Role and Skill Implications

Current market analysis reveals several critical trends for my career planning. First, technical-focused roles such as SOC Analysts, Detection Engineers, and Security Researchers are in high demand for their expertise, with work primarily conducted through written reports and documentation. Second, the post-pandemic shift has normalized remote cybersecurity work with asynchronous communication via Slack, Teams, and ticketing systems - ideal for professionals who prefer written communication. Third, AWS security skills including GuardDuty, Security Hub, and CloudTrail command a salary premium as organizations migrate to cloud-first architectures. Fourth, enterprises shifting to zero-trust access models and cloud-native security controls create strong demand for engineers with AWS-centric designs and automation skills. Fifth, foundational certifications like Security+ help candidates pass HR filters, AWS Security Specialty differentiates cloud expertise, CISSP validates leadership readiness, and GCIH proves practitioner depth. Sixth, professionals who can automate detection and response through Python and Lambda earn premium compensation for work requiring minimal verbal communication. Finally, growing bug bounty platforms like HackerOne and Bugcrowd enable fully independent security research with communication primarily through written reports.

The broader demand remains strong despite local market fluctuations. A practical, cloud-aware blue-team skill set aligned to MITRE ATT&CK, coupled with recognized certifications and a demonstrable lab portfolio, positions candidates competitively for entry-level SOC roles within 12-24 months and for security engineer or incident response roles by years 3-5 (Kroll, 2025).

5. Academic Plan

5.1. Computer Science Courses

My academic program in Computer Science provides essential foundations for cybersecurity work. Computer Networks and Operating Systems courses will teach packet flows, sockets, process models, filesystems, and authentication - knowledge I will apply directly to SOC triage, EDR telemetry analysis, and system hardening, building on my Red Hat system administration experience. Databases and Data Modeling courses will enable me to work with log storage, SIEM data schemas, detection queries with joins and regex, and threat hunting, leveraging my Microverse database module knowledge. Software Engineering and Secure Coding courses will teach threat modeling, input validation, and authentication/authorization patterns using OWASP guidance, utilizing my JavaScript and Ruby development experience. Cloud Computing electives will cover identity management, network security, encryption key management, and security benchmarks in AWS, building on my Oracle Cloud Infrastructure Foundations certification. AI and Machine Learning electives will introduce anomaly detection scoring and adversarial ML risks valued by modern SOCs, leveraging my

Introduction to Generative AI knowledge. Finally, Information Security and Cryptography courses will teach governance, risk management, cryptography, and IAM - aligning with Security+ and CISSP domains and connecting with my Data Privacy Fundamentals certification.

5.2. Hands-On Labs and Resources

Beyond formal coursework, I will utilize multiple hands-on learning platforms. On TryHackMe and Hack The Box, I will complete guided and challenge-style labs for SOC, web security, and red-team skills, building a portfolio of completed rooms and boxes. Using AWS free tier services, I will build a personal lab environment with EC2, S3, CloudTrail, GuardDuty, and Security Hub to author detective controls, Lambda automation functions, and CloudWatch monitoring, leveraging my Oracle Cloud experience for faster AWS adoption. I will integrate OWASP projects into my coursework and capstone projects for secure application design and code review checklists. Using MITRE ATT&CK Navigator, I will map detection rules to adversary techniques and produce an "ATT&CK coverage" heatmap as a capstone deliverable demonstrating threat-informed defense capabilities.

Additional resources I will leverage include university career center services for internship placements in SOCs, MSSPs, or IT security teams, specifically requesting roles emphasizing technical analysis and written documentation. I will participate in CTF competitions and hackathons to reinforce practical skills through technical challenges requiring minimal verbal communication. I will join security clubs for hands-on activities and technical workshops. I will engage with Security+ and AWS online study groups using official modules and forums. Finally, I will focus on remote work opportunities in cybersecurity roles that support primarily written and asynchronous communication.

6. Action Plan for the Next 5 Years

My action plan for the next five years prioritizes completing my Computer Science degree with strong academic performance while actively pursuing cybersecurity-focused internships and part-time work opportunities. I will develop technical expertise through coursework, hands-on labs, capstone projects, and industry certifications pursued in parallel with my studies. This strategic combination of academic rigor, practical experience, and certifications will position me for seamless transition into full-time cybersecurity roles upon graduation.

Year 1 (Current - Semesters 1-2): Foundation in Mathematics and Programming. Coursework in this year includes Higher Mathematics (both semesters), Programming (both semesters), Computer Systems Structure (Semester 2), Programming Languages Concepts (Semester 2), and supporting courses in Labour Safety and Foreign Languages. The focus is on mastering core mathematical concepts and programming fundamentals that underpin advanced cybersecurity work. Additionally, AWS Certified Cloud Practitioner certification

will be pursued using online resources, leveraging Oracle Cloud Infrastructure knowledge to support AWS adoption.

Year 2 (Semesters 3-4): Database Design, Mathematics, and Software Engineering. Coursework in this year includes Database Design Concepts (Semester 4), Discrete Mathematics (Semester 3-4), Probability Theory and Mathematical Statistics (Semester 4), and Software Project Management (Semester 4). Data Structures and Algorithms and Object-Oriented Programming were completed at a previous institution and provide foundational knowledge applicable to detection engineering and security tool development. This year involves internship opportunities in IT support, systems administration, or entry-level security operations roles. CompTIA Security+ (SY0-701) certification will be completed by end of Year 2.

Year 3 (Semesters 5-6): Operating Systems, Databases, and Networks. Coursework includes Operating Systems and System Programming (Semester 5), enabling deep understanding of process models, memory management, and system calls applicable to SOC investigations and EDR telemetry analysis. Database Processing (Semester 5) provides proficiency in querying security logs and performing threat hunting. Computer Networks (Semester 6) covers TCP/IP protocols, routing, DNS, VPNs, and network security architectures. Additional courses include Applied Numerical Methods (Semester 6), Data Science Fundamentals (Semester 6), and Software Engineering (Semester 6). Internship opportunities in SOC environments, security operations centers, or MSSPs are pursued. Hands-on security labs on TryHackMe and HackTheBox supplement coursework. A network security analysis project using Wireshark and tcpdump is developed for portfolio documentation.

Year 4 (Semesters 7-8): Software Engineering, Cloud Computing, and Advanced Systems. Coursework includes advanced Software Engineering topics (Semester 7), Web Programming, and UX Design (Semester 7). Cloud Computing and Internet of Things (Semester 8) provides foundation in cloud architecture, security configurations, and multi-tenant security models. System Analysis and Modelling (Semester 8) supports threat modelling capabilities, and Introduction to Intelligence Systems (Semester 8) covers AI/ML applications in security. AWS Certified Security - Specialty certification is pursued. Part-time or internship roles in detection engineering, cloud security, or incident response are sought. A comprehensive AWS security lab project mapping MITRE ATT&CK techniques to AWS detective controls in GuardDuty, Security Hub, and CloudTrail is developed and documented.

Year 5 (Semesters 9-10): Cybersecurity, Integration, and Bachelor's Thesis. Coursework includes the dedicated Cybersecurity course (Semester 9) integrating knowledge from operating systems, networks, software engineering, and data science. Blockchain Technologies and complementary electives are selected. The Bachelor's Thesis (Semester 10) focuses on a cybersecurity topic such as "Detection Engineering for Cloud-Native

Architectures" or "Threat-Informed Defense Using MITRE ATT&CK and AWS Security Services," integrating systems programming knowledge, database query optimization, network analysis, statistical methods, and software engineering practices. "English for Career Management" (Semester 10) supports professional documentation skills. Part-time security work or internship rotations in detection engineering, cloud security, or incident response are pursued. Upon degree completion, a comprehensive portfolio of cybersecurity projects, lab configurations, technical documentation, practical internship experience, and relevant certifications (Security+, AWS certifications) is established.

Parallel Learning and Work Strategy. Throughout the five-year study program, industry certifications are pursued aligned with each year's coursework and job market requirements. Years 1-2 include AWS Certified Cloud Practitioner and CompTIA Security+ using online resources and practice exams. Year 3 includes security-specific labs on TryHackMe and HackTheBox concurrent with cybersecurity internship opportunities. Year 4 includes AWS Certified Security - Specialty certification. A GitHub portfolio is maintained with lab configurations, scripts, project documentation, and internship project evidence. Cybersecurity-related work opportunities are prioritized to build practical skills, professional networks, and portfolio documentation.

7. Conclusion

Cybersecurity represents a professionally rewarding and financially viable career path well-aligned with technical strengths and personal circumstances. Strong market demand evidenced by the global shortage of 4.8 million cybersecurity professionals, diverse technical specializations, and support for remote work and written communication support this career trajectory in defensive security roles including SOC analysis, detection engineering, and cloud security.

The five-year Computer Science degree program provides a comprehensive foundation for cybersecurity specialization. Academic coursework in operating systems, networks, databases, software engineering, and system design forms the technical bedrock for professional cybersecurity practice. Dedicated courses in Cloud Computing and Cybersecurity enable development of domain-specific expertise. Concurrent pursuit of industry certifications (Security+, AWS certifications), internship experience in security environments, and portfolio development through academic projects and professional work contribute to preparation for cybersecurity roles upon graduation.

The Bachelor's degree in Computer Science, combined with prior practical experience (Red Hat System Administration, Oracle Cloud Infrastructure, development in Ruby and JavaScript) and strategic internship placements in cybersecurity environments, provides credibility and technical foundation for entry into SOC Analyst, Detection Engineer, or Security Operations positions. Alignment between academic coursework, hands-on

cybersecurity projects, internship experience, industry certifications, and career objectives creates a coherent pathway to professional cybersecurity practice. Upon degree completion, completion of specialized knowledge, professional networks, work experience, portfolio documentation, and professional credentials enables launch of a cybersecurity career focused on technical specialization and analytical depth—characteristics of modern remote-capable security roles.

> ***Note:*** *A full interactive HTML version of this career report with enhanced visualizations and detailed content is available at: https://github.com/st93642/Career-report/releases/download/1.0.0/career_report_93642.html*

References

AWS. (2025). *AWS Certified Security - Specialty.* Retrieved from https://aws.amazon.com/certification/certified-security-specialty/

Bureau of Labor Statistics. (2025). *Occupational Outlook Handbook: Information Security Analysts.* U.S. Department of Labor. Retrieved from https://www.bls.gov/ooh/computer-and-information-technology/information-security-analysts.htm

CompTIA. (2025). *CompTIA Security+ Certification.* Retrieved from https://www.comptia.org/certifications/security

ENISA. (2025). *ENISA Threat Landscape 2025.* European Union Agency for Cybersecurity. Retrieved from https://www.enisa.europa.eu/publications/enisa-threat-landscape-2025

GIAC. (2025). *GIAC Certified Incident Handler (GCIH).* Global Information Assurance Certification. Retrieved from https://www.giac.org/certifications/certified-incident-handler-gcih/

ISC². (2025). *Cybersecurity Workforce Study.* International Information System Security Certification Consortium. Retrieved from https://www.isc2.org/Research

Kroll. (2025). *Cyber Risk Insights and Publications.* Retrieved from https://www.kroll.com/en/insights

MITRE Corporation. (2025). *MITRE ATT&CK Framework.* Retrieved from https://attack.mitre.org/

OWASP. (2025). *OWASP Top 10 - 2025.* Open Web Application Security Project. Retrieved from https://owasp.org/www-project-top-ten/

Statista. (2025). *Cybersecurity Market Data.* Retrieved from https://www.statista.com/markets/420/topic/484/cybersecurity/