TRANSPORT AND TELECOMMUNICATION INSTITUTE

ENGINEERING FACULTY

Career report

Course: **Introduction to Specialty and Digital Skills**

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

Riga
2025

Cybersecurity Professional Career Report

A Roadmap to Security Engineering & Incident Response

Summary

Cybersecurity offers resilient, evolving career opportunities with strong demand, diverse specializations, and meaningful work. This report outlines my career goal as a security engineer specializing in AWS cloud security, detection engineering, and incident response - roles emphasizing technical expertise and written communication over verbal interaction. I detail my skill development plan, academic connections, job market analysis, and 5-year action plan to achieve employability in defensive security.

Career Goal

My goal is to become a security engineer specializing in AWS cloud security, detection engineering, and incident response. Given my speech impairment, I'm targeting roles emphasizing written communication, technical analysis, and automation over verbal interactions.

Target Roles

SOC Analyst (Tier 1-2), Detection Engineer, Security Researcher/Analyst, Digital Forensics Investigator, Penetration Tester, and Bug Bounty Hunter - all emphasizing technical documentation over verbal communication.

Career Progression (Years 1-5+)

SOC Analyst → Detection Engineer/Security Analyst → AWS Cloud Security Specialist → Senior Detection Engineer/AWS Security Architect. These roles leverage technical depth and written documentation while minimizing verbal communication requirements.

Skills & Knowledge Development Plan

Technical Foundations

I will build expertise in: Networking & OS (TCP/IP, DNS, Linux/Windows administration), Security Engineering (IAM, zero-trust, cryptography), AWS Cloud Security (IAM, GuardDuty, Security Hub, CloudTrail), Threat Detection & IR (SIEM, EDR, incident response), MITRE ATT&CK (threat-informed defense), and Application Security (OWASP Top 10, secure coding).

Tools & Platforms

SIEM/SOAR (Splunk, Elastic), EDR/XDR (CrowdStrike, SentinelOne), AWS Security tools (GuardDuty, Security Hub), Network Analysis (Wireshark, Zeek), Vulnerability Management (Nessus, AWS Inspector), Scripting (Python, Bash), and Red-Team tools (Burp Suite, Metasploit).

Certification Roadmap

Year 1-2: Foundation

AWS Cloud Practitioner CompTIA Security+

Year 2-3: AWS Specialization

AWS Certified Security - Specialty

Year 3-4: Incident Response

GIAC GCIH

Year 4-5: Leadership

CISSP

Professional Skills

Excellent written communication, structured reporting, asynchronous collaboration (tickets, Slack/Teams, email), self-directed learning, analytical thinking, and technical documentation - all aligning with remote work and written communication requirements.

Academic Program Connection

I will leverage Computer Science courses directly: Networks/OS for SOC triage and system hardening (building on Red Hat experience), Databases for SIEM queries and threat hunting, Software Engineering for secure coding (using JavaScript/Ruby skills), Cloud Computing for AWS security (extending Oracle Cloud knowledge), and AI/ML for detection systems (applying Generative AI background).

Hands-On Labs: TryHackMe/Hack The Box for SOC skills, AWS free tier for GuardDuty/Security Hub practice, OWASP for application security, and MITRE ATT&CK Navigator for detection mapping. I will focus on remote opportunities with written communication.

Job Market Analysis

Demand & Workforce Gap

The global cybersecurity workforce faces a 4.8 million-person gap. U.S. Information Security Analyst positions are projected to grow 29% (2024-2034) with median salaries of $124,910. Europe expects 500,000+ unfilled positions by 2026.

Key Insights

High Demand: ISC2 2024 reports persistent global shortages despite AI experimentation. European Context: ENISA identifies DDoS and ransomware as top threats targeting public administration and transport. Remote Work: Post-pandemic shift normalizes remote cybersecurity work via Slack/Teams/ticketing—ideal for written communication. Cloud Premium: AWS security skills (GuardDuty, Security Hub) highly valued. Certifications: Security+, AWS Security Specialty, GCIH, and CISSP help cross HR filters and validate expertise.

5-Year Action Plan

Year 1: Foundation

Complete CS programming modules, build AWS home lab (EC2, GuardDuty, CloudTrail), earn AWS Cloud Practitioner and Security+ certifications, complete 15+ TryHackMe labs, update security-focused CV.

Year 2: SOC-Readiness & AWS

Take Cloud Computing and Secure Software courses, build comprehensive AWS security lab with detective controls and Lambda automation, pursue AWS Security Specialty certification, seek SOC internship/part-time role, publish GitHub portfolio with ATT&CK coverage.

Year 3: Security Engineer/IR

Transition to Tier-2 SOC Analyst or Detection Engineer role, earn GIAC GCIH certification, lead detection engineering project, build IR playbook pack, add adversary emulation to labs.

Year 4: Architecture & AWS Mastery

Lead AWS cloud security initiative, demonstrate improvements with metrics, mentor juniors, contribute to security blog, start CISSP preparation, consider AWS Solutions Architect certification.

Year 5: Consolidation & Advancement

Move into Senior Detection Engineer or AWS Security Architect role, achieve full CISSP, publish AWS Security Engineering Playbook compiling baselines, detective controls, IR runbooks, and IaC templates.

European Salary Data & Market Statistics

European cybersecurity professionals earn competitive salaries: Entry-level SOC Analysts €48k, Security Analysts €65k, Senior Engineers €82k. Europe faces a 300k-500k talent shortage with 8-12% annual job growth through 2032. The European market reached €67.79 billion in 2024, projected to grow to €194.43 billion by 2033. Remote work opportunities (approximately one-third of positions) support written/asynchronous communication preferences.

Role-Specific Salaries

SOC Analyst: €45k-68k, Detection Engineer: €60k-85k, Penetration Tester: €50k-80k, Digital Forensics: €60k-95k. All roles emphasize technical documentation over verbal communication.

⚠ Risks & Mitigations

Market Fluctuations: Regional variations exist; hedge with cloud, identity, and detection skills.

Certification Costs: Total investment €2,500-12,000 over 5 years; prioritize cost-effective early certs, delay premium ones until employer-sponsored.

Speech Impairment: Focus on technical specialist roles (SOC, Detection Engineer, Digital Forensics, Bug Bounty) prioritizing written documentation; leverage remote work culture and request interview accommodations.

Certification Investment

My 5-year certification pathway requires strategic investment: CompTIA Security+ (€480-725), AWS Cloud Practitioner (€92), AWS Security Specialty (€138-277 with discount), GIAC GCIH (€920-7,500 depending on SANS training), CISSP (€805-900 initial + €115-125/year maintenance). Total: €2,500-3,200 (minimum self-study), €3,200-4,500 (medium spent), or €8,000-12,000 (premium with SANS).

Strategy: Self-fund foundational certs Years 1-2, seek employer sponsorship for premium certs Years 3-5.

DevOps/DevSecOps Alternative

Given my development experience (Ruby, JavaScript, MuleSoft) and infrastructure skills (Red Hat, Oracle Cloud), DevOps and DevSecOps offer compelling alternatives emphasizing automation, infrastructure-as-code, and CI/CD - primarily code-based with minimal verbal communication.

DevOps Engineer (€50k-85k): Automates delivery, manages cloud infrastructure, implements CI/CD.

Tools: Terraform, Ansible, Docker, Kubernetes, Python.

DevSecOps Engineer (€58k-95k): Integrates security into pipelines, automated testing (SAST/DAST), secrets management.

Tools: Snyk, SonarQube, HashiCorp Vault, OPA.

Career Pathway: DevOps (Years 1-2, €55k-70k) → DevSecOps (Years 2-3, €65k-85k) → Security Engineering (Years 3-5, €75k-100k+).

This progression offers flexibility, comparable compensation, and technical focus with written communication emphasis.

Key Sources

ISC2 Cybersecurity Workforce Study 2024:
https://www.isc2.org/Research/Workforce-Study
- Global workforce gap estimates, skills demand, and hiring trends

U.S. Bureau of Labor Statistics (BLS) - Information Security Analysts:
https://www.bls.gov/ooh/computer-and-information-technology/information-security-analysts.htm
- Job outlook, median salaries, growth projections (29% through 2034)

LinkedIn Talent Insights:
https://business.linkedin.com/talent-solutions/talent-insights
- Job postings, skills demand, and regional hiring trends

Statista Cybersecurity Market Data:
https://www.statista.com/markets/420/topic/484/cybersecurity/
- European and global market size, growth rates, and projections

Glassdoor / Salary.com / PayScale:
https://www.glassdoor.com
- Real-world salary data for cybersecurity roles by country and experience level

Threat Intelligence & Security Landscape

ENISA Threat Landscape 2025:
https://www.enisa.europa.eu/publications/enisa-threat-landscape-2025
- Top threats in Europe, attack vectors, and sector-specific risks

Kroll Cyber Risk Report:
https://www.kroll.com/en/reports/cyber/threat-intelligence-reports/cti-spotlight-trends-report
- Quarterly threat analysis, incident response trends, ransomware data

✓ Conclusion

Cybersecurity offers a technically rewarding, financially viable, and strategically accessible career path with strong market demand, diverse specializations, and increasing support for remote work and written communication. By following my structured 5-year plan - building foundational certifications (Security+, AWS Cloud Practitioner, AWS Security Specialty), developing hands-on detection and incident response skills, and progressing through SOC → Detection Engineering → Security Engineering roles - I can establish a sustainable, meaningful career protecting digital infrastructure. My combination of development experience, system administration skills, cloud knowledge, and written communication positions me to excel in technical specialist roles emphasizing analytical depth over verbal interactions. With strategic certification investments (€2,500-4,500 over five years), consistent hands-on practice, and portfolio development, I can build competitive expertise in one of technology's most resilient career paths.

Full version of this report with visuals available as html file.