Cybersecurity Professional Career Report

# 🛡️ Cybersecurity Professional Career Report

A Roadmap to Security Engineering & Incident Response

**Author:** Igors Oļeiņikovs

**Course:** Computer Science - 43483 (EN, Distant) **Group:** 4501 BTA

**Date:** November 1, 2025

## 📋 Summary

Cybersecurity represents one of the most resilient, fast-evolving technology careers, with strong long-term demand, diverse specializations, and meaningful work protecting people, organizations, and critical infrastructure. In this report, I present my career goal, outline the skills I plan to develop, connect these competencies to my academic coursework and practical resources, analyze the job market using current data, and detail my 5-year action plan to achieve competence and employability in defensive security, cloud security, and incident response.

## 🎯 Career Goal: Security Engineer & Technical Specialist

My goal is to become a **security engineer and technical specialist with strong AWS (Amazon Web Services) cloud security skills**-capable of engineering secure architectures, developing detection systems, analyzing threats, and implementing technical improvements that reduce risk across hybrid cloud environments. Given my speech impairment, I am strategically targeting roles that emphasize **written communication, technical analysis, and automation** over verbal interactions.

### Ideal Role Characteristics

* **SOC (Security Operations Center) Analyst (Tier 1-2):** Monitoring dashboards, investigating alerts, documenting findings in ticketing systems-primarily written reports
* **Detection Engineer:** Creating and tuning SIEM (Security Information and Event Management) rules, developing automation scripts-technical work with minimal meetings
* **Security Researcher/Analyst:** Threat intelligence analysis, malware analysis, vulnerability research-independent technical work
* **Digital Forensics Investigator:** Analyzing evidence, recovering data, documenting findings in detailed written reports
* **Penetration Tester/Ethical Hacker:** Technical testing, vulnerability identification, comprehensive written reports-limited client interaction
* **Bug Bounty Hunter:** Independent work identifying vulnerabilities, submitting detailed written reports

### Medium-Term Objectives (Years 3-5)

* Progress through roles: SOC Analyst (Tier 1) → Detection Engineer or Security Analyst (Tier 2) → AWS Cloud Security Specialist
* Develop complementary focus on AWS cloud security (EC2, S3, IAM, CloudTrail, GuardDuty, Security Hub) and automation
* Master threat-informed defense using MITRE ATT&CK (Adversarial Tactics, Techniques, and Common Knowledge) framework
* Build expertise in areas requiring deep technical focus rather than frequent verbal communication

### Long-Term Vision (Years 5+)

Advance toward specialized technical roles such as **Senior Detection Engineer, AWS Security Architect, or Cloud Security Specialist**-positions that leverage technical depth and written documentation skills while minimizing requirements for extensive verbal communication.

**Why This Path?**

These roles align with my strengths and personal circumstances. They emphasize technical expertise, analytical thinking, and written communication-skills where I can excel. SOC Analysts primarily work with dashboards and tickets, Detection Engineers focus on code and rules, and Cloud Security Specialists engineer secure AWS infrastructures. These positions require minimal verbal interaction while offering meaningful work protecting digital infrastructure. My existing foundation in Oracle Cloud, Red Hat system administration, and development provides a strong technical base for transitioning into AWS-focused security engineering.

## 🔧 Skills & Knowledge I Plan to Develop

### Technical Foundations I Will Build

#### 🌐 Networking & Operating Systems

I will deepen my understanding of TCP/IP (Transmission Control Protocol/Internet Protocol), routing, DNS (Domain Name System), VPNs (Virtual Private Networks), Windows and Linux administration, logging, and hardening - essential for SOC investigations and engineering secure configurations.

#### 🏗️ Security Engineering

I plan to master identity and access management, segmentation, least privilege, cryptography, secure configuration, and zero-trust design patterns including SASE (Secure Access Service Edge)/SSE (Security Service Edge) concepts.

#### ☁️ Cloud Security (AWS)

I will develop expertise in AWS IAM (Identity and Access Management), EC2 (Elastic Compute Cloud) security, S3 (Simple Storage Service) bucket policies, CloudTrail, GuardDuty, Security Hub, AWS Config, VPC (Virtual Private Cloud) security, KMS (Key Management Service) encryption, and hybrid threat protection across multi-cloud environments.

#### 🔍 Threat Detection & IR (Incident Response)

I aim to build proficiency in SIEM content development, EDR (Endpoint Detection and Response) telemetry, triage, scoping, containment, eradication, recovery, and post-incident improvements.

#### 🎯 Threat-Informed Defense

I will learn to use MITRE ATT&CK to map adversary tactics/techniques to detections and controls, improving coverage and response playbooks.

#### 💻 Application Security

I intend to understand OWASP Top 10 risks, SDLC security touchpoints, basic code review, and DevSecOps practices to reduce exploitable flaws.

### Tools & Platforms I Will Master

* **SIEM/SOAR (Security Orchestration, Automation, and Response):** Splunk, Elastic Stack, AWS Security Lake, Sumo Logic
* **EDR/XDR (Extended Detection and Response):** CrowdStrike Falcon, SentinelOne, Carbon Black
* **Cloud Security:** AWS GuardDuty, Security Hub, CloudTrail, AWS Config, Prowler
* **Network Analysis:** Wireshark, Zeek, tcpdump
* **Vulnerability Management:** AWS Inspector, Nessus, Qualys, OpenVAS
* **Scripting:** Python and Bash for automation and AWS Lambda functions
* **Red-Team Tools:** Burp Suite, Nmap, Metasploit (for adversary mindset)

### My Certification Roadmap

#### ✅ Completed Foundation (2020-2025)

✓ freeCodeCamp Responsive Web Design ✓ JavaScript Algorithms & Data Structures ✓ Microverse Ruby/Databases ✓ Red Hat System Administrator (RH134) ✓ MuleSoft Certified Developer ✓ Oracle Cloud Infrastructure Foundations 2021 ✓ Cisco Introduction to Cybersecurity ✓ ISC2 (International Information System Security Certification Consortium) Candidate ✓ Google Cloud Intro to Generative AI ✓ Data Privacy Fundamentals

**My foundation:** I have established system administration skills (Red Hat), cloud fundamentals (Oracle), development experience (MuleSoft), cybersecurity basics (Cisco), and data privacy knowledge.

#### Year 1-2: Security Foundation & AWS Start

CompTIA Security+ (SY0-701) AWS Certified Cloud Practitioner

I will build on my Oracle cloud foundation to master AWS fundamentals, then validate core security knowledge with Security+. These cover hybrid/cloud, GRC (Governance, Risk, and Compliance), incident response, identity, and threats - widely recognized for entry into SOC roles.

#### Year 2-3: AWS Cloud Security Specialization

AWS Certified Security - Specialty

I plan to deep dive into AWS security engineering: IAM, encryption, monitoring (CloudTrail, GuardDuty), incident response, data protection, and infrastructure security. I will leverage my Oracle certification experience for faster AWS adoption.

#### Year 3-4: Incident Response & Detection

GIAC GCIH (GIAC Certified Incident Handler)

I aim to validate practical incident handling approaches, tooling, and response workflows with proctored, hands-on emphasis. This complements my AWS security skills with defensive response capabilities.

#### Year 4-5+: Advanced Leadership

CISSP (Certified Information Systems Security Professional)

I will pursue this broad governance and architecture credential (requires experience; I can leverage my ISC2 Candidate status and progress to Associate after passing). This validates readiness for senior technical roles.

#### Optional Technical Stretch

OSCP+ or AWS Certified Solutions Architect

I may pursue OSCP+ for deep adversary tradecraft understanding, or AWS Solutions Architect for architectural design skills complementing my security expertise.

### Professional Skills I Will Develop

* **Excellent written communication:** I will develop clear documentation skills for incident reports, technical write-ups, threat analyses, and playbooks
* **Structured reporting:** I will create detailed findings documents, investigation timelines, and root cause analyses
* **Asynchronous collaboration:** I will master ticketing systems, Slack/Teams messages, email, and documentation platforms
* **Self-directed learning:** I will independently follow intelligence sources, advisories, and technology updates
* **Analytical thinking:** I will strengthen my technical analysis and creative problem-solving abilities
* **Technical documentation:** I will learn to create runbooks, detection logic explanations, and security architecture diagrams

**My Accessibility Strategy:** Modern cybersecurity work increasingly supports remote collaboration and written communication. Most technical roles involve primarily written reports, ticketing systems, chat platforms, and documentation - with minimal requirements for phone calls or presentations. SOC environments typically use tickets and chat, while detection engineering and threat analysis are largely independent technical work. This aligns well with my speech impairment accommodation needs.

## 🎓 How I Will Connect My Academic Program

### CS Courses I Will Apply to Cybersecurity

* **Computer Networks / Operating Systems:** I will apply packet flows, sockets, process models, filesystems, authentication knowledge directly to SOC triage, EDR telemetry, and system hardening. I will build on my Red Hat system administration experience.
* **Databases & Data Modeling:** I will use log storage, SIEM data schemas, building detections with joins and regex, and threat hunting queries. I will leverage my Microverse database module knowledge.
* **Software Engineering / Secure Coding:** I will apply threat modeling, input validation, authentication/authorization patterns using OWASP guidance. I will use my JavaScript and Ruby development experience.
* **Cloud Computing (elective):** I will study identity, network security, encryption key management, and security benchmarks in AWS. I will build on my Oracle Cloud Infrastructure Foundations certification.
* **AI/ML (elective):** I will apply machine learning to detection (anomaly scoring) and understand adversarial ML risks valued by modern SOCs. I will leverage my Introduction to Generative AI knowledge.
* **Information Security / Cryptography:** I will study governance, risk, crypto, IAM-aligning with Security+ and CISSP domains. I will connect this with my Data Privacy Fundamentals certification.

### Hands-On Labs & Platforms I Will Use

#### TryHackMe & Hack The Box

I will complete guided and challenge-style labs for SOC, web, and red-team skills. I will build a portfolio of completed rooms/boxes.

#### Microsoft Learn / AWS

I will build a personal lab with AWS free tier: GuardDuty, Security Hub, CloudTrail to author detective controls, Lambda automation, and CloudWatch monitoring. I will leverage my Oracle Cloud experience for faster AWS adoption.

#### OWASP Projects

I will integrate OWASP into my coursework and capstones for secure app design and code review checklists.

#### MITRE ATT&CK Navigator

I will map detections to techniques and produce an "ATT&CK coverage" heatmap as a capstone deliverable.

### Resources I Will Leverage

* **Career Center & Internships:** I will target placements in SOCs, MSP/MSSPs, or IT security teams and request roles emphasizing technical analysis and written documentation
* **CTFs & Hackathons:** I will participate in regular competitions to reinforce practical skills through technical challenges requiring minimal verbal communication
* **Security Clubs:** I will engage in hands-on activities and technical workshops
* **Study Communities:** I will join Security+ and AWS online study groups using official modules and forums
* **Remote Work Opportunities:** I will focus on cybersecurity roles that support remote work with primarily written/asynchronous communication

## 📊 Job Market Analysis (2025)

### Demand & Workforce Gap

4.8M

Global Workforce Gap

29%

U.S. Growth Rate (2024-2034)

$124,910

U.S. Median Salary (2024)

500K+

Unfilled EU Jobs by 2026

### Key Market Insights

* **Global Workforce Gap:** ISC2 2024 Study estimates roughly 4.8 million-person gap worldwide with resource strain, even as teams experiment with AI
* **U.S. Labor Outlook:** Bureau of Labor Statistics projects 29% growth (2024-2034) for Information Security Analysts, median pay $124,910
* **Regional Variations:** While some markets cooled YoY, Germany, Spain, Brazil, and Poland saw increases, emphasizing skills-first hiring
* **European Context:** ENISA Threat Landscape 2024 highlights DDoS and ransomware as top threats, with public administration and transport heavily targeted

### Current Threat Landscape

Understanding prevalent threats drives control priorities and skill development:

* **Phishing/BEC:** Dominant initial access vector requiring identity protection and credential misuse detection
* **Ransomware:** Steady impact requiring resilience skills and incident response capability
* **DDoS:** Availability attacks targeting critical infrastructure and services
* **Supply Chain Attacks:** Increasing sophistication requiring broader security awareness

### Role & Skill Implications

* **Technical-Focused Roles in High Demand:** SOC Analysts, Detection Engineers, and Security Researchers are sought after for their technical expertise, with work primarily conducted through written reports and documentation
* **Remote Work Growth:** Post-pandemic shift has normalized remote cybersecurity work with asynchronous communication via Slack, Teams, and ticketing systems - ideal for professionals who prefer written communication
* **Cloud Security Skills Premium:** AWS security skills (GuardDuty, Security Hub, CloudTrail) are highly valued as organizations migrate to cloud-first architectures
* **Zero-Trust & Cloud-Native Security:** Enterprises shifting to zero-trust access models and cloud-native security controls; engineers with AWS-centric designs and automation skills are in demand
* **Certifications Matter:** Foundations like Security+ help cross HR filters; AWS Security Specialty differentiates cloud expertise; CISSP validates leadership readiness; GCIH proves practitioner depth
* **Automation & Scripting Premium:** Professionals who can automate detection and response through Python and Lambda are highly valued - work requiring minimal verbal communication
* **Bug Bounty & Independent Work:** Growing platforms like HackerOne and Bugcrowd enable fully independent security research with communication primarily through written reports

**Bottom Line:** The broader demand is strong, with local fluctuations. A practical, cloud-aware blue-team skill set aligned to ATT&CK, coupled with recognized certifications and a demonstrable lab/portfolio, places candidates competitively for entry-level SOC roles within 12-24 months and for security engineer/IR roles by years 3-5.

## 📅 My Detailed 5-Year Action Plan

#### Year 1: Building My Foundation

**Technical Learning I Will Pursue:**

* I will complete CS modules in Programming
* I will create a home lab using AWS free tier with EC2, S3, CloudTrail, GuardDuty
* I will document my learning in a lab journal, building on my Red Hat and Oracle Cloud experience
* I will transition my cloud skills from Oracle to AWS ecosystem

**Certifications I Will Earn:**

* I will study and pass AWS Certified Cloud Practitioner (Q1-Q2)
* I will study and pass CompTIA Security+ (SY0-701) by end of year (Q3-Q4)

**Hands-On Practice I Will Complete:**

* I will complete 15+ beginner/intermediate labs on TryHackMe (SOC, blue team, web)
* I will begin one ATT&CK-mapped detection project using AWS services

**Career Assets I Will Build:**

* I will update my security-focused CV highlighting my certifications (Red Hat, Oracle Cloud, Cisco, ISC2 Candidate)
* I will map my skills to NICE (National Initiative for Cybersecurity Education) Work Roles on my LinkedIn profile

#### Year 2: Developing SOC-Readiness & AWS Cloud Security

**Academic & Lab Focus:**

* I will elect Cloud Computing and Secure Software modules
* I will continue OS, networks, databases with security lens (logging, auth, crypto)
* I will build comprehensive AWS security lab: GuardDuty + Security Hub + CloudTrail + Config
* I will create 8-10 detective controls, 3 Lambda automation functions, CloudWatch alerting mapping to 12+ ATT&CK techniques
* I will leverage my Python scripting skills for AWS automation

**Certification Goal:**

* I will prepare for and pass AWS Certified Security - Specialty by end of Year 2 or early Year 3

**Experience I Will Seek:**

* I will pursue summer/term SOC internship or part-time Tier-1 SOC role with MSSP
* When applying, I will emphasize my strong written communication skills and preference for technical analysis roles
* I will request reasonable accommodations for interview process (written responses, extended time for verbal portions)

**Deliverables I Will Create:**

* I will publish GitHub portfolio with AWS security configurations, Python automation scripts, ATT&CK coverage heatmap
* I will create mini "IR runbook" for phishing → credential theft scenario in AWS environment

#### Year 3: Advancing to Security Engineer / Incident Response

**Professional Progression I Plan:**

* I will transition to Tier-2 SOC Analyst or Detection Engineer role (internal or MSSP)
* I will focus on technical specialization: detection engineering, threat intelligence, or digital forensics
* I will lead detection engineering or identity hardening project (conditional access, MFA, least privilege) - primarily technical work
* I will build my reputation for high-quality written documentation and technical analysis

**Certification I Will Pursue:**

* I will study and pass GIAC GCIH (incident handling)
* I will build IR playbook pack (BEC, ransomware, insider misuse) and tabletop exercises

**Advanced Labs I Will Build:**

* I will add adversary emulation: pick 1-2 intrusion sets from ATT&CK
* I will simulate key techniques and ensure my rules detect behaviors (not just IOCs)

**Deliverables I Will Produce:**

* I will write public (sanitized) post-incident "lessons learned" report showing business impact translation

#### Year 4: Developing Architecture Depth & AWS Mastery

**My Stretch Goals:**

* I will lead AWS cloud security posture initiative (AWS Config rules, CloudFormation security templates, Infrastructure-as-Code security)
* I will demonstrate improvements with metrics (risk reduction, MTTD/MTTR in cloud environment)
* I will mentor juniors through written documentation, code reviews, and pairing sessions
* I will contribute to security blog or publish technical write-ups demonstrating my AWS security expertise
* I will consider bug bounty hunting as side project for additional income and skill development

**My Certification Path:**

* I will start CISSP preparation (leverage my ISC2 Candidate status; or take exam and hold Associate status)
* Optional: I may consider AWS Certified Solutions Architect - Professional to complement my security expertise with architectural design skills

#### Year 5: My Consolidation & Career Advancement

**My Role Target:**

* I will move into Senior Detection Engineer, AWS Security Architect, or specialized Cloud Security Researcher role
* I will own a technical domain (AWS detection engineering, cloud threat hunting, or security automation)
* I will focus on deep technical expertise rather than management/leadership roles requiring extensive verbal communication
* I will consider fully remote positions or independent consulting/bug bounty work

**Credentials I Will Achieve:**

* I will achieve full CISSP (experience requirement met through work history)
* If pursued, I will consider OSCP+ for adversary perspective or maintain AWS certifications with continuing education

**My Portfolio Capstone:**

* I will publish "AWS Security Engineering Playbook" compiling:
  + AWS security baselines and best practices (IAM, encryption, monitoring)
  + Detective controls mapped to ATT&CK techniques and ENISA top threats
  + IR runbooks for cloud-specific incidents with KPIs and year-over-year improvements
  + Infrastructure-as-Code security templates (CloudFormation, Terraform)

## 📊 European Cybersecurity Salary & Demand Data (2025)

### Average Annual Salaries Across Europe

€48,000

Europe Avg - Entry SOC Analyst

€65,000

Europe Avg - Security Analyst

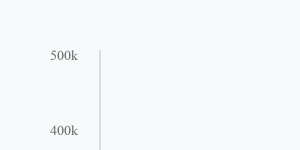
€82,000

Europe Avg - Senior Security Engineer

€52,000-€74,000

Germany - Security Analyst Range

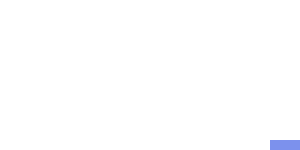
#### Europe Cybersecurity Job Market Growth



### Key Market Statistics (Europe, 2025)

* **Talent Gap:** Europe faces a shortage of approximately 300,000-500,000 cybersecurity professionals, with major markets like Germany (106,000), UK (14,100), and France contributing to this significant gap
* **Market Growth:** The European cybersecurity 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 CAGR of 12.42%
* **Job Growth Rate:** European cybersecurity job markets are expanding at average rates of 8-12% annually through 2032 across major economies
* **Remote Work Opportunities:** Approximately one-third of cybersecurity positions support remote work, facilitating asynchronous, written communication
* **Entry-Level Compensation:** Entry-level roles like SOC Analyst average €45,000-€52,000 annually across Europe, with Junior Penetration Testers earning €50,000-€58,000

### Salary Progression by Experience Level (Europe Average)



### Role-Specific Opportunities for Technical Focus

#### SOC Analyst

**Avg Salary (Europe):** €45k - €68k

**Communication:** Primarily ticketing systems, written reports, and dashboard monitoring

**Demand:** High - critical frontline defense role

#### Detection Engineer

**Avg Salary (Europe):** €60k - €85k

**Communication:** Technical documentation, code reviews, written design docs

**Demand:** Very High - automation focus, minimal verbal interaction

#### Penetration Tester

**Avg Salary (Europe):** €50k - €80k

**Communication:** Comprehensive written reports, technical findings documentation

**Demand:** High - ethical hacking skills in demand

#### Digital Forensics

**Avg Salary (Europe):** €60k - €95k

**Communication:** Detailed forensic reports, evidence documentation

**Demand:** Growing - incident response and legal cases

**Key Takeaway:** Information Security Analysts rank among the top 15 fastest-growing professions globally through 2030, while network and cybersecurity skills are projected to be the second fastest-growing skill category worldwide. The global cybersecurity job market has 3.5 million unfilled positions as of 2025, creating exceptional opportunities for technically focused professionals who excel in written communication and analytical work.

## ⚠️ Risks, Constraints & Mitigations

#### Market Fluctuations

**Risk:** Regional job market variations

**Mitigation:** Hedge with cloud + identity + detection skills, which remain cross-platform and high-value even in cooler markets

#### Certification Costs

**Risk:** Professional certifications can be expensive

**Mitigation:** Prioritize cost-effective early certs (Security+, AWS Cloud Practitioner), delay premium ones (SANS, CISSP) until employer-sponsored.

#### Speech Impairment

**Challenge:** Traditional roles may emphasize verbal communication

**Opportunity:** Focus on technical specialist roles (SOC Analyst, Detection Engineer, Digital Forensics, Bug Bounty Hunter) that prioritize written documentation. Modern remote work culture supports asynchronous, text-based collaboration. Request accommodations during interviews and leverage disability services.

## 💰 Certification Costs in Euros

Understanding the financial investment required for professional certifications is crucial for planning my career development. Below is a detailed breakdown of certification costs in Euros for my recommended pathway.

#### 1. CompTIA Security+

**Exam Cost:** €380-425

**Study Materials (Optional):** €100-300

* Official study guide: €50-70
* Practice exams: €30-50
* Video course (Udemy/Pluralsight): €20-180

**Total Investment:** €480-725

#### 2. AWS Cloud Practitioner

**Exam Cost:** €92

**Study Materials:** Free (AWS Training & Certification portal)

**Total Investment:** €92

#### 3. AWS Security Specialty

**Exam Cost:** €277

**Discounted Exam Cost:** €138 (50% discount after passing another AWS certification)

**Study Materials:** Free (AWS Training, practice labs, whitepapers)

**Total Investment:** €138-277

#### 4. GIAC GCIH

**Standalone Exam:** €920-950

**SANS Training Bundle:** €6,500-7,500

**Note:** The standalone exam tests practical incident handling skills. The SANS training bundle includes comprehensive course materials, labs, and exam attempts but is significantly more expensive. Consider employer sponsorship for SANS training.

**Total Investment:** €920-7,500

#### 5. CISSP

**Exam Cost:** €690-700

**Annual Maintenance (AMF):** €115-125

**Study Materials (Optional):** €100-200

**Requirements:** 5 years of cumulative paid work experience in two or more CISSP domains, or 4 years plus one year waived with relevant degree/certification. Can sit exam and hold Associate status until experience requirement is met.

**Total Investment (First Year):** €805-900

**Ongoing:** €115-125/year

#### 6. OSCP+ (Optional)

**Certification Package:** €1,400-1,600

Includes 90 days lab access, course materials, and exam attempt. Highly technical, hands-on offensive security certification for those seeking deep adversary tradecraft understanding.

**Total Investment:** €1,400-1,600

### 5-Year Total Investment Summary

€2,500-3,200

Minimum (Self-Study Path)

€3,200-4,500

Recommended (Balanced Approach)

€8,000-12,000

Premium (With SANS Training)

#### Investment Strategy

* **Year 1-2:** Self-fund foundational certs (Security+, AWS Cloud Practitioner, AWS Security) = €610-1,094
* **Year 3-4:** Seek employer sponsorship for premium certs (GIAC GCIH with SANS training, or standalone exam) = €920-7,500
* **Year 4-5:** Employer-sponsored or self-funded CISSP after experience requirement met = €805-900 initial + €115-125/year
* **Optional:** OSCP+ or AWS Solutions Architect if pursuing specialized technical path = €1,400-1,600

## 🔄 DevOps/DevSecOps Alternative Paths

Given my existing development experience and cloud infrastructure skills, DevOps and DevSecOps represent compelling alternative or complementary career paths. These roles emphasize technical automation, infrastructure-as-code, and CI/CD (Continuous Integration/Continuous Deployment) pipelines - work that is primarily code-based with minimal verbal communication requirements.

### Why Consider DevOps/DevSecOps

* **Natural Fit:** Leverages my existing Ruby, JavaScript, and MuleSoft development experience plus Red Hat system administration and cloud skills
* **Technical Focus:** Work centers on automation scripts, infrastructure code, CI/CD pipelines, and monitoring - primarily written/code-based communication
* **Career Flexibility:** Provides multiple pathways into security: DevOps → DevSecOps → Security Engineer
* **Market Demand:** Similar talent shortages and salary ranges as cybersecurity roles
* **Remote-Friendly:** High percentage of remote positions with asynchronous collaboration through Git, tickets, and documentation

#### DevOps Engineer

**Role Description:** Automates software delivery, manages cloud infrastructure, implements CI/CD pipelines, monitors systems, and bridges development and operations teams through automation and tooling.

**Good Fit?**

* ✅ Excellent fit for my development + sysadmin background
* ✅ Work is primarily code (Terraform, Ansible, Python, YAML)
* ✅ Communication mainly through Git commits, PRs, tickets, documentation
* ✅ Can transition to DevSecOps or Security Engineering later
* ⚠️ Some roles require team meetings, but much work is independent

**Average Salary (Europe):**

€50,000 - €85,000

* Entry-level: €50,000 - €60,000
* Mid-level: €60,000 - €75,000
* Senior: €75,000 - €85,000+

**Key Skills & Tools:**

* Infrastructure as Code: Terraform, CloudFormation, Ansible
* CI/CD: Jenkins, GitLab CI, GitHub Actions, ArgoCD
* Containers: Docker, Kubernetes, Helm
* Cloud Platforms: AWS, Azure, GCP
* Scripting: Python, Bash, PowerShell
* Monitoring: Prometheus, Grafana, ELK Stack

**Relevant Certifications:**

* AWS Certified DevOps Engineer (€277)
* AWS Solutions Architect - Associate (€138)
* Kubernetes CKA/CKAD (€300-395)
* HashiCorp Terraform Associate (€70)

#### DevSecOps Engineer

**Role Description:** Integrates security into DevOps pipelines, implements automated security testing (SAST, DAST, SCA), manages secrets, enforces security policies as code, and ensures secure software delivery practices.

**Good Fit?**

* ✅ Perfect blend of development, security, and automation
* ✅ Highly technical role focused on security tooling and pipelines
* ✅ Work primarily through code, config files, and automated tests
* ✅ Strong demand with similar salary to security roles
* ✅ Natural progression from DevOps or entry point to security
* ⚠️ May need to explain findings to dev teams, but mostly async/written

**Average Salary (Europe):**

€58,000 - €95,000

* Entry-level: €58,000 - €70,000
* Mid-level: €70,000 - €85,000
* Senior: €85,000 - €95,000+

**Key Skills & Tools:**

* Security Scanning: Snyk, SonarQube, Checkmarx, Veracode
* Container Security: Trivy, Aqua, Twistlock
* Secrets Management: HashiCorp Vault, AWS Secrets Manager
* Policy as Code: Open Policy Agent (OPA), Sentinel
* SAST/DAST Tools: OWASP ZAP, Burp Suite, GitLab Security
* Compliance: CIS Benchmarks, security hardening, audit logging

**Relevant Certifications:**

* AWS Security Specialty (€138-277)
* Certified DevSecOps Professional (€250-300)
* CompTIA Security+ (€380-425)
* GIAC GSEC or GCSA (€920+)

### Strategic Career Pathway

#### DevOps → DevSecOps → Security Engineer Progression

This pathway provides flexibility and fallback options while building toward security specialization:

#### Option 1: Start with DevOps (Years 1-2)

* Easier entry point leveraging existing development + sysadmin skills
* Build cloud infrastructure expertise (AWS, Kubernetes, Terraform)
* Learn CI/CD, automation, and system architecture
* Gradually add security components (vulnerability scanning, compliance checks)
* Target salary: €55,000 - €70,000

#### Option 2: Transition to DevSecOps (Years 2-3)

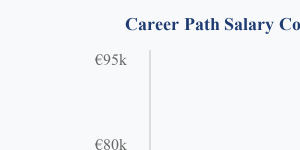
* Add security certifications (Security+, AWS Security Specialty)
* Implement security tooling in CI/CD pipelines
* Focus on container security, secrets management, policy as code
* Build expertise in secure software delivery
* Target salary: €65,000 - €85,000

#### Option 3: Progress to Security Engineering (Years 3-5)

* Deepen security specialization (GCIH, CISSP)
* Focus on cloud security architecture, detection engineering, or IR
* Leverage DevSecOps background for security automation and tooling
* My infrastructure/code skills become differentiators
* Target salary: €75,000 - €100,000+

**Key Advantage:** This progression gives me three career paths that are all in high demand, similarly compensated, and emphasize technical work over verbal communication. I can pivot based on market conditions, personal interests, and opportunities.

### Salary Comparison: All Three Paths (Europe Average)



#### Key Takeaways for Alternative Paths

* **All Three Paths Offer Similar Compensation:** DevOps, DevSecOps, and Security Engineering roles have comparable salary ranges (€50k-95k+ across Europe), making career transitions financially viable
* **Lower Barriers to Entry:** DevOps roles may be easier to secure initially with existing development and system administration experience
* **Technical Communication Focus:** All three paths emphasize written communication through code, documentation, tickets, and Git - minimizing verbal communication requirements
* **High Remote Work Availability:** DevOps and DevSecOps roles frequently offer remote positions with asynchronous collaboration
* **Flexible Career Pivoting:** Skills transfer naturally between paths, allowing adjustments based on interests, market demand, and personal circumstances
* **Existing Skills Leverage:** Ruby, JavaScript, MuleSoft, Red Hat, and Oracle Cloud experience directly applies to DevOps/DevSecOps roles

## 📚 Sources

This report draws on authoritative industry sources, official certification bodies, threat intelligence platforms, and career data resources. Below are organized, clickable references for further exploration.

### Workforce & Job Market Data

* **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/insights/publications/cyber-risk/quarterly-threat-landscape>  
  *Quarterly threat analysis, incident response trends, ransomware data*
* **MITRE ATT&CK Framework:** <https://attack.mitre.org/>  
  *Comprehensive adversary tactics, techniques, and procedures (TTPs) database*
* **OWASP Top 10:** <https://owasp.org/www-project-top-ten/>  
  *Most critical web application security risks and mitigation strategies*
* **Verizon Data Breach Investigations Report (DBIR):** <https://www.verizon.com/business/resources/reports/dbir/>  
  *Annual analysis of real-world data breaches, attack patterns, and trends*

### Certification Information & Official Bodies

* **CompTIA Security+:** <https://www.comptia.org/certifications/security>  
  *Exam objectives, study resources, pricing, and certification details*
* **AWS Certification:** <https://aws.amazon.com/certification/>  
  *Full catalog of AWS certifications, exam guides, pricing, and training paths*
* **AWS Security Specialty:** <https://aws.amazon.com/certification/certified-security-specialty/>  
  *Detailed exam guide, domains, sample questions, and preparation resources*
* **GIAC Certifications (GCIH, GSEC, etc.):** <https://www.giac.org/certifications/>  
  *SANS/GIAC certification catalog, exam formats, pricing, and renewal requirements*
* **ISC2 CISSP:** <https://www.isc2.org/Certifications/CISSP>  
  *CISSP domains, experience requirements, exam details, and maintenance*
* **Offensive Security (OSCP+):** <https://www.offensive-security.com/courses-and-certifications/>  
  *Hands-on penetration testing certifications, lab access, and pricing*

### Training Platforms & Hands-On Practice

* **TryHackMe:** <https://tryhackme.com/>  
  *Guided cybersecurity learning paths, SOC training, and hands-on labs*
* **Hack The Box:** <https://www.hackthebox.com/>  
  *Challenge-based penetration testing labs and CTF competitions*
* **Microsoft Learn:** <https://learn.microsoft.com/en-us/training/>  
  *Free Azure and security training modules aligned with Microsoft certifications*
* **AWS Skill Builder:** <https://skillbuilder.aws/>  
  *Free and paid AWS training courses, labs, and certification prep*
* **Cybrary:** <https://www.cybrary.it/>  
  *Cybersecurity training courses, virtual labs, and certification preparation*
* **SANS Cyber Aces:** <https://www.sans.org/cyberaces/>  
  *Free introductory tutorials on operating systems, networking, and system administration*

### Industry Trends & Analysis

* **Gartner Security & Risk Management:** <https://www.gartner.com/en/information-technology/insights/security>  
  *Strategic insights, technology trends, and market forecasts*
* **Dark Reading:** <https://www.darkreading.com/>  
  *Daily cybersecurity news, threat analysis, and industry commentary*
* **Krebs on Security:** <https://krebsonsecurity.com/>  
  *Investigative security journalism and breach analysis*
* **CSO Online:** <https://www.csoonline.com/>  
  *Security strategy, risk management, and career development resources*
* **The Hacker News:** <https://thehackernews.com/>  
  *Breaking security news, vulnerability disclosures, and threat reports*

## ✅ Conclusion

**Cybersecurity offers me 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, defensive security roles align exceptionally well with my strengths and circumstances.

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.

**Alternative paths through DevOps and DevSecOps** provide me additional flexibility, leveraging my existing development and infrastructure skills while maintaining similar compensation levels and technical focus.

My combination of development experience, system administration skills, cloud knowledge, and written communication positions me to excel in technical specialist roles that emphasize analytical depth over verbal interactions. With strategic certification investments totaling €2,500-4,500 over five years (or more with premium training), combined with consistent hands-on practice and portfolio development, I can build competitive expertise in one of technology's most resilient and impactful career paths.