



Cybersecurity Career Roadmap

2026

Your Complete Guide to Breaking Into Cybersecurity

Contents

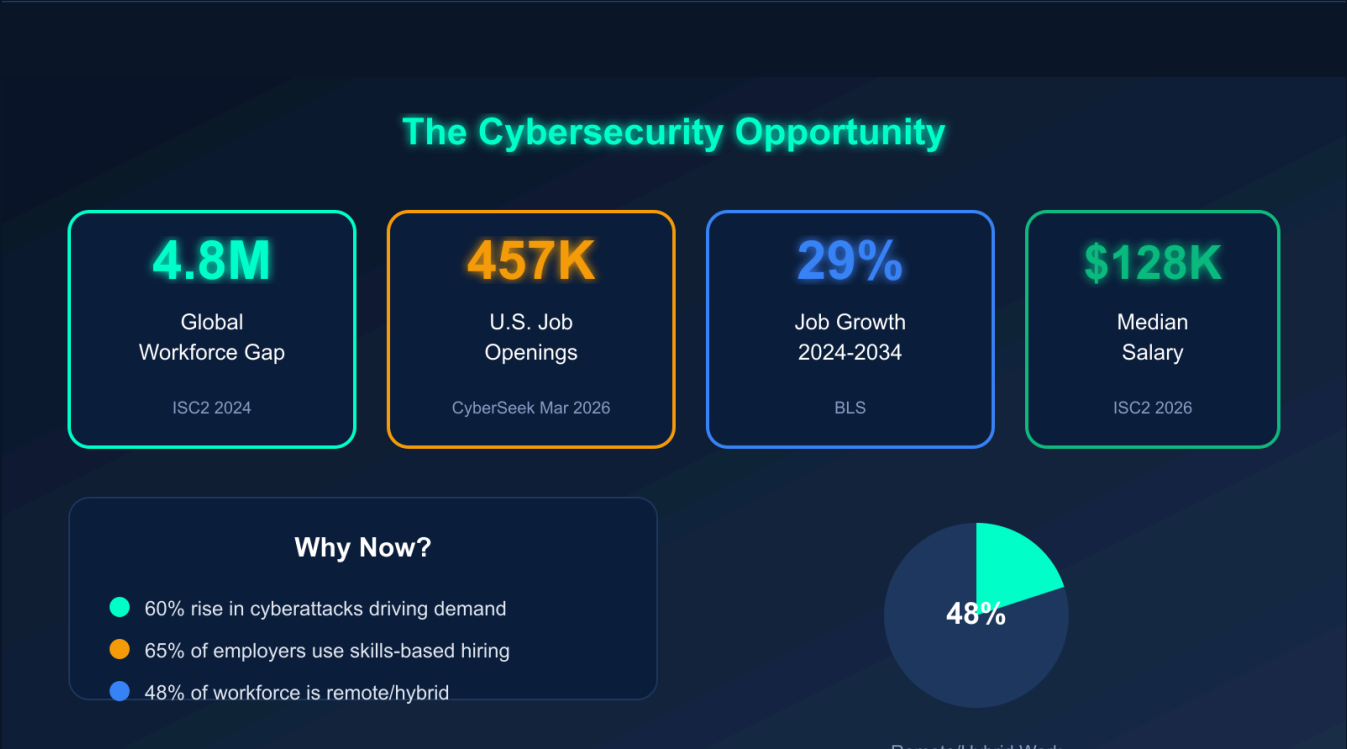
01	The Opportunity	3
02	Career Paths Comparison	4
03	AI + Cybersecurity: The New Frontier	5
04	Certification Roadmap	9
05	Skills Gap Assessment	10
06	30-Day Action Plan	11
07	Free & Low-Cost Resources	12
08	Industry-Specific Paths	13
09	Remote Work Reality	14
10	Getting Hired Without Experience	15
11	Next Steps	16

About This Guide

This roadmap provides actionable career guidance backed by 2024-2026 industry data from ISC2, Bureau of Labor Statistics, CyberSeek, and leading industry analysts. All salary figures, certification costs, and market statistics are sourced and current as of publication.

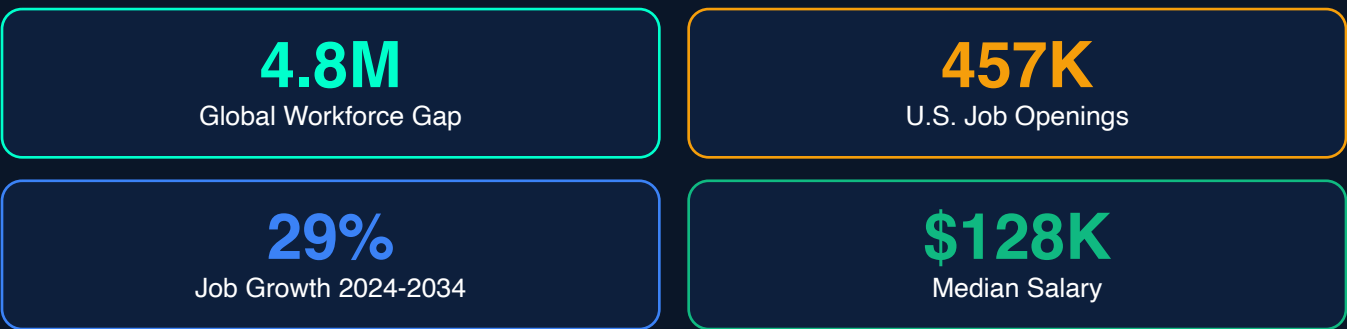
Version 1.0 | February 2026

The Opportunity



Why Cybersecurity, Why Now?

The cybersecurity industry faces an unprecedented talent shortage, creating one of the most compelling career opportunities of the decade.



The Timing Has Never Been Better

Demand is Exploding

Cyberattacks have risen **60% year-over-year**. Every breach that makes headlines creates more budget and more job openings.

Skills-Based Hiring

65% of employers now use skills evaluations over degree requirements. What you can demonstrate matters more than credentials.

No Degree Required

Many entry-level roles—SOC Analyst, Security Analyst, Help Desk with security focus—don't require a four-year degree.

Remote Work is Standard

48% of the global cybersecurity workforce works remotely or hybrid. Geographic barriers are disappearing.

Career Paths Comparison

Choose your path based on your interests, skills, and career goals.



Career Paths at a Glance

Career Path	Entry	Senior	Best For
SOC Analyst	50-80K	85-130K	Problem-solvers
Penetration Tester	80-105K	140K+	Creative hackers
Security Engineer	70-100K	158-173K	Builders
GRC Analyst	65-90K	120K+	Process-driven
Cloud Security	100K+	128-170K	Cloud enthusiasts
Incident Responder	85K	145K	Crisis handlers
Security Architect	130K	200K+	Big-picture thinkers
CISO	150K	400K+	Strategic leaders

Emerging Roles 2026-2026

AI Security Engineer

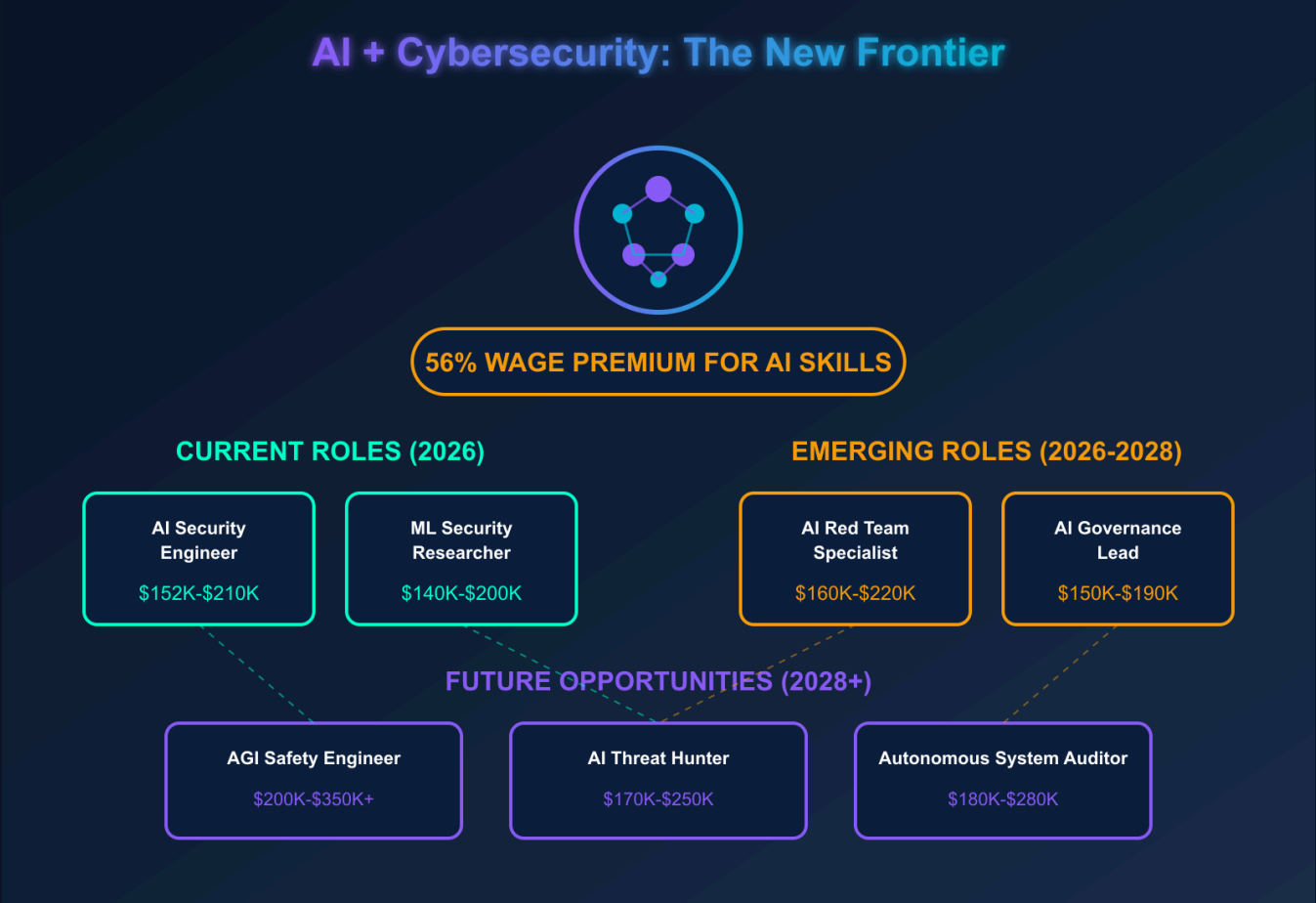
- Salary: \$152K-\$210K
- 56% wage premium for AI skills

AI Governance Specialist

- High demand, low supply
- ML + policy expertise

AI + Cybersecurity: The New Frontier

The intersection of AI and cybersecurity is creating the most lucrative and fastest-growing career opportunities in tech.



Why AI Security Matters Now

The Threat Landscape

- AI-powered attacks are here:**
- Deepfake social engineering
 - Automated vulnerability discovery
 - AI-generated phishing at scale
 - Adversarial ML attacks on models
 - AI-assisted malware evasion

The Defense Opportunity

- AI-powered defense is critical:**
- Behavioral anomaly detection
 - Automated threat hunting
 - Real-time incident response
 - Predictive security analytics
 - AI model security & alignment

56% Wage Premium for professionals with AI + Security skills

AI Security Roles: Current & Future

Current Roles (Hiring Now - 2026)

AI Security Engineer **\$152K-\$210K**

What you do: Secure AI/ML systems, implement model access controls, detect adversarial inputs, ensure training data integrity.

Skills needed: Python, ML frameworks (PyTorch, TensorFlow), security fundamentals, API security, cloud platforms.

Who's hiring: OpenAI, Anthropic, Google, Microsoft, Meta, NVIDIA, AI startups.

ML Security Researcher **\$140K-\$200K**

What you do: Research adversarial ML, model vulnerabilities, jailbreaks, data poisoning attacks, publish findings.

Skills needed: Deep ML knowledge, Python, research methodology, academic writing, red team mindset.

Who's hiring: AI labs, universities, DARPA, big tech research teams.

LLM Red Team Specialist **\$145K-\$195K**

What you do: Test LLMs for jailbreaks, prompt injection, harmful outputs, safety bypasses. Break AI systems before attackers do.

Skills needed: Prompt engineering, creative attack thinking, NLP understanding, documentation skills.

Who's hiring: Anthropic, OpenAI, Scale AI, AI safety orgs, consulting firms.

AI Governance Analyst **\$120K-\$160K**

What you do: Develop AI policies, ensure regulatory compliance (EU AI Act), risk assessments, ethics frameworks.

Skills needed: Policy writing, regulatory knowledge, risk management, communication, some technical literacy.

Who's hiring: Enterprises adopting AI, consulting firms, government, AI companies.

AI Security Roles: Emerging & Future

Emerging Roles (2026-2028)

AI Threat Intelligence Analyst \$130K-\$175K

What you do: Track AI-powered threat actors, analyze AI-generated malware, monitor adversarial ML trends.

Why emerging: As attackers adopt AI, defenders need specialists who understand both domains.

Autonomous Systems Auditor \$150K-\$200K

What you do: Audit AI agents, autonomous vehicles, robotics for security and safety compliance.

Why emerging: Regulations are coming. Companies need auditors before deployment.

AI Supply Chain Security \$140K-\$185K

What you do: Secure model pipelines, verify training data provenance, audit third-party models, detect backdoors.

Why emerging: Model supply chain attacks are the next SolarWinds.

Deepfake Detection Engineer \$135K-\$180K

What you do: Build systems to detect AI-generated media, voice clones, synthetic identities.

Why emerging: Deepfakes are becoming indistinguishable. Detection is critical infrastructure.

Future Opportunities (2028+)

The Horizon

AGI Safety Engineer \$200K-\$350K+

Alignment research, containment protocols, safety testing for advanced AI systems.

AI-Human Trust Architect \$170K-\$250K

Design verification systems for human-AI interaction, prevent manipulation.

Synthetic Media Forensics \$150K-\$220K

Legal-grade analysis of AI-generated content for courts and investigations.

Breaking Into AI Security

Path 1: Security Professional → AI Security

If you have security experience

Add these skills:

- Python for ML (start with scikit-learn, then PyTorch)
- Fundamentals of neural networks and LLMs
- Hugging Face ecosystem
- Prompt engineering and LLM APIs

Projects to build:

- Build a simple classifier, then try to fool it with adversarial examples
- Create a prompt injection test suite for an open-source LLM
- Document AI attack techniques on your blog

Timeline: 3-6 months to become hireable

Path 2: AI/ML Engineer → AI Security

If you have ML experience

Add these skills:

- Security fundamentals (Security+ or equivalent knowledge)
- Threat modeling and attack trees
- Secure software development practices
- Red team/adversarial mindset

Projects to build:

- Red team your own models for jailbreaks
- Implement model access controls and audit logging
- Contribute to AI safety research papers

Timeline: 2-4 months to become hireable

Resources for AI Security

Learning

Courses:

- NVIDIA AI Red Team Training
- Coursera ML Security Specialization
- SANS SEC595: Applied Data Science

Research:

- MITRE ATLAS (AI attack framework)
- Anthropic safety research papers
- OpenAI red teaming reports

Practice

Hands-on:

- Gandalf (prompt injection game)
- AI CTF challenges
- HuggingFace model security labs

Community:

- AI Village (DEF CON)
- MLSecOps Community
- AI safety Discord servers

Certification Roadmap

Certifications serve two purposes: they get you past HR filters, and they validate your knowledge.

Certification Roadmap by Year

YEAR 1: Foundation

Security+
\$404

Google
Cybersecurity
Free

ISC2 CC
Free



YEARS 2-3: Specialization

BLUE TEAM
CySA+ | BTL1
GCIH

RED TEAM
CEH | PNPT
eJPT

CLOUD
AWS Security
AZ-500

GRC
CISA | CRISC
CGRC



YEARS 4-5: Advanced / Leadership

CISSP
\$749 | 15-25% raise

OSCP
\$1,749+ | Elite

CISM
\$760 | Management

CCSP
\$599 | Cloud Lead

Year 1: Foundation

Start here regardless of your target role.

Certification	Cost	Details
CompTIA Security+	\$404	DoD 8140 approved, 700K+ holders
Google Cybersecurity	Free	Available on Coursera, great for career changers
ISC2 CC	Free	No experience required, stepping stone

Certification ROI

37%

Higher Salary
(Certified vs Non)

91%

Employers Prefer
Certifications

\$151K

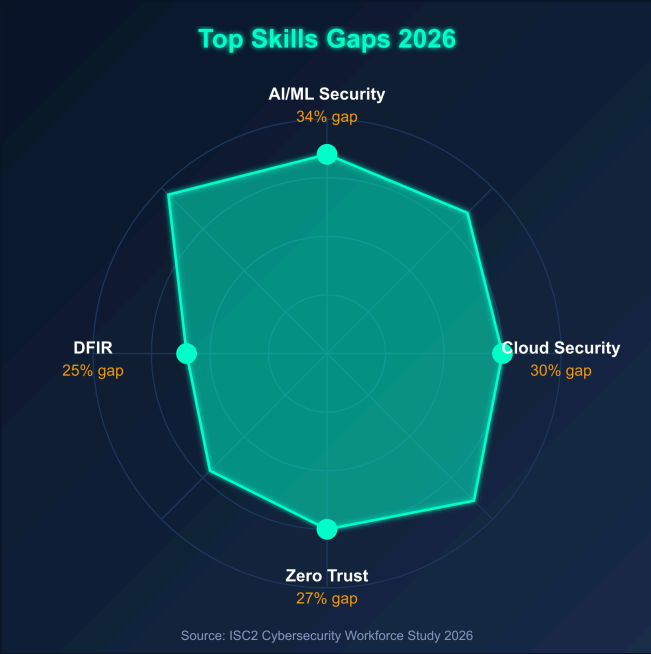
Average OSCP
Holder Salary

Government/DoD Path

DoD 8140 replaced 8570 in 2026. Compliance deadline: February 15, 2026 (cyber roles), February 15, 2026 (all cyber workforce). Security+ satisfies multiple 8140 work role requirements.

Skills Gap Assessment

Understanding the skills gaps helps you position yourself strategically.



Top Skills Gaps 2026

Organizations are struggling to find talent in these areas:

1. AI/ML Security

Securing AI systems and models

34%

2. Cloud Security

AWS, Azure, GCP security

30%

3. Zero Trust

Implementation & architecture

27%

4. DFIR

Digital forensics & incident response

25%

Self-Assessment Checklist

Rate your current proficiency in each area:

Networking

- TCP/IP model and protocols
- DNS, DHCP, routing
- Firewall concepts
- VPNs and segmentation

Operating Systems

- Linux command line
- Windows administration
- File permissions
- Log analysis

Scripting

- Python basics
- Bash fundamentals
- PowerShell basics
- API interaction

Security Concepts

- CIA triad
- Authentication vs Authorization
- Encryption types
- Common attack types

30-Day Action Plan

Your first month in cybersecurity. Assumes 2-3 hours per day.



Week 1: Foundation

Days 1-2: Set up home lab

- Download VirtualBox (free)
- Install Kali Linux VM
- Document the process

Days 3-4: Start learning

- Create TryHackMe account
- Complete "Pre-Security" path

Days 5-7: Begin cert study

- Watch Professor Messer Sec+ videos
- Create flashcards

Week 2: Hands-On

Days 8-10: Continue CTFs

- Complete "Intro to Cybersecurity"
- Start "Complete Beginner" path

Days 11-12: Linux skills

- Learn essential commands
- Practice navigation

Days 13-14: Network analysis

- Install Wireshark
- Capture your first packets

Week 3: Build Brand

Days 15-16: LinkedIn

- Update headline
- Add security skills
- Write transition story

Days 17-18: Community

- Join r/cybersecurity
- Find Discord servers
- Follow security pros

Days 19-21: Documentation

- Create GitHub account
- Start a blog or GitHub Pages
- Write first post

Week 4: Career Prep

Days 22-23: Research

- Search LinkedIn jobs
- Note common requirements
- Identify target companies

Days 24-25: Resume

- Lead with certs & projects
- Quantify learning
- Add GitHub/blog links

Days 26-30: Action

- Apply to 3-5 positions
- Schedule Sec+ exam date
- Set 90-day goals

Free & Low-Cost Resources

The best resources in cybersecurity are often free.

Free Training Platforms

Platform	Focus	URL
TryHackMe	Guided learning, CTF-style	tryhackme.com
Hack The Box Academy	Structured courses	academy.hackthebox.com
SANS Cyber Aces	Foundational skills	cyberaces.org
Fortinet NSE	Network security, free certs	training.fortinet.com
PortSwigger Academy	Web application security	portswigger.net
LetsDefend	SOC analyst training	letsdefend.io
CyberDefenders	Blue team challenges	cyberdefenders.org

Free Certification Prep

Security+

Professor Messer

Free YouTube videos
Complete SY0-701 course

CISSP

FRSecure Mentor

Live webinars + recordings
Community-driven prep

Google Cert

Coursera Audit

Free access to materials
Pay only for certificate

Essential Free Tools

Offensive Tools

Kali Linux - Complete pentesting distro
Nmap - Network scanning
Burp Suite Community - Web testing
Metasploit Framework - Exploitation
Gobuster - Directory enumeration

Defensive Tools

Wireshark - Packet analysis
Security Onion - Network monitoring
Ghidra - Reverse engineering (NSA)
YARA - Malware detection rules
CyberChef - Data analysis (GCHQ)

Industry-Specific Paths

Certain industries pay premiums for cybersecurity talent.

Healthcare

Why it pays: HIPAA violations cost \$100-\$50,000 per incident. Healthcare data sells for 10x financial data.

Key compliance: HIPAA, HITECH

Recommended cert: HCISPP (ISC2)

Focus areas:

- Patient data protection
- Medical device security
- EHR systems

Premium: \$140K+ for specialists

Financial Services

Why it pays: Banks face constant attacks and heavy regulation. They pay for the best.

Key compliance: PCI-DSS, SOX, GLBA

Focus areas:

- Fraud prevention
- Transaction security
- API security

Premium: \$140K+ for elite testers

Government & Defense

Why it pays: Stable employment, excellent benefits, mission-driven work.

Key requirement: DoD 8140 certification

Security clearance: Required for most roles

Top employers: NSA, CISA, FBI, DoD, contractors

Benefit: Job security + pension

AI & Technology

Why it pays: AI security is the new frontier. Few people have both skillsets.

Focus areas:

- ML model security
- AI governance
- Prompt injection defense

Top employers: OpenAI, Anthropic, Google

Premium: 56% wage premium for AI skills

Remote Work Reality

The pandemic permanently changed cybersecurity work.

2026-2026 Remote Statistics

48%

Remote/
Hybrid

75%

Companies
Hybrid

76%

Would Quit
W/O Remote

\$55–80K

Entry Remote
Salaries

Remote-Friendly Roles

Highly Remote

- ✓ SOC Analyst (Tier 1-3)
- ✓ Security Analyst
- ✓ GRC/Compliance Analyst
- ✓ Threat Intelligence
- ✓ Penetration Tester

Hybrid Preferred

Security Engineer
Incident Responder
Security Architect
Red Team Lead
Security Manager

Usually On-Site

- × Physical Security
- × OT/ICS Security
- × Classified Gov Work
- × Data Center Security
- × Hardware Security

Top Companies Hiring Remotely

Technology

Google
Amazon
Microsoft
NVIDIA

Finance

JPMorgan
Goldman Sachs
Visa
Mastercard

Defense

Northrop
Leidos
BAE Systems
Booz Allen

Consulting

Deloitte
KPMG
Accenture
Mandiant

Getting Hired Without Experience

“How do I get experience without a job, and a job without experience?”

The Five-Step Formula

1 Get Certified

Security+ clears HR filters. Period. It's the minimum bar for most entry-level positions.

2 Build Labs

Create a home lab and document it. Write detailed walkthroughs on GitHub or a blog. This IS experience.

3 Practice CTFs

TryHackMe and Hack The Box. Track progress publicly. “Completed 100+ CTF challenges” is a resume line.

4 Network

LinkedIn outreach, informational interviews. Local meetups: ISSA, OWASP, BSides conferences.

5 Contribute to Open Source

Find security tools on GitHub. Start with documentation or small fixes. Work up to code contributions. This demonstrates real-world collaboration.

Alternative Entry Points

Path	Why It Works
MSP/MSSP	Higher turnover = lower hiring bar. Great experience.
IT Helpdesk → Security	Internal transfers are easier. Learn the company first.
Internships	Many pay well. Direct path to full-time.
Non-profit volunteer	Gain experience while doing good.

Resume Tips

Lead with certifications: CompTIA Security+ (2026) | Google Cybersecurity Certificate

Quantify your learning: “Completed 50+ TryHackMe rooms” | “Ranked top 5% globally”

Include links: GitHub portfolio | Blog | LinkedIn

Next Steps

You've read the roadmap. Now it's time to move.

Take the Career Quiz

Not sure which path fits? Our assessment matches your skills and interests to specific cybersecurity roles.

remnantsecurity.com

Join the Waitlist

Get early access to structured courses, mentorship, and our community of security professionals.

remnantsecurity.com

Start Day 1

Go back to the 30-Day Action Plan. Today is Day 1. Download VirtualBox. Create your TryHackMe account. Begin.

About Remnant Security

Remnant Security provides actionable cybersecurity career guidance backed by current industry data. We cut through the noise to give you practical steps for breaking into and advancing in cybersecurity.

hello@remnantsecurity.com

This guide was compiled using data from ISC2, Bureau of Labor Statistics, CyberSeek, Robert Half, ISACA, and direct industry research. All figures reflect 2024-2026 data as of publication.

Version 1.0 | February 2026

Copyright 2026 Remnant Security. All rights reserved.