THE CYBERSECURIST

The 6 Highest-Paying Tech Learning Paths for 2026

Free resources. Real timelines. No degree required.

Every path starts at zero and ends at six figures.

crownstone.io | @thecybersecurist

Before You Start

The highest-paying skills in tech right now all share something in common: the demand for them is growing faster than the supply. That's not a problem. That's your window.

None of these paths require a four-year degree. They all require curiosity, consistent learning (even 30 minutes a day), building real things, and talking about what you learn.

Each path in this guide gives you a 6-month roadmap with specific resources, milestones, portfolio projects, and realistic salary expectations. Most resources are free. The ones that cost money (certifications) are investments that pay for themselves within weeks of landing the role.

How to use this guide: Find the path that matches your interest. Follow it month by month. Build the projects. Get the certifications. Apply with a portfolio, not just a resume.

If you're not sure which path to pick, start with the one that excites you most. Passion sustains the late nights when motivation runs out.

What's Inside

01

AI/ML Engineering

Salary Range: $180,000 - $250,000

Start free: fast.ai courses, Andrew Ng's ML Specialization on Coursera (audit free)

Month 1-2: Foundations

Build your Python fluency and develop ML intuition before diving into theory.

- → Complete fast.ai Practical Deep Learning for Coders (free at course.fast.ai)
- → Audit Andrew Ng's ML Specialization on Coursera (free to audit)
- → Master Python data tools: NumPy, Pandas, Matplotlib via freeCodeCamp
- → Set up your environment: Anaconda, Jupyter, VS Code, GitHub
- → Build your first image classifier using a pre-trained model and push to GitHub

Month 3: Deep Learning

Move from classical ML into neural networks and transformer architectures.

- → Pick TensorFlow or PyTorch (both free, PyTorch has stronger community momentum)
- → Build: image classifier, text sentiment analyzer using Hugging Face transformers
- → Use Google Colab for free GPU access (colab.research.google.com)
- → Understand transfer learning, fine-tuning, and model evaluation metrics
- → Start a Kaggle profile and submit to at least one competition

Month 4: Production Skills (MLOps)

Most ML engineers can train models. Few can ship them. This is where you stand out.

- → Learn Docker basics for containerizing ML models
- → Build REST APIs with FastAPI to serve predictions
- → Use MLflow for experiment tracking and model versioning
- → Deploy a real model endpoint (AWS Lambda free tier or Hugging Face Spaces)
- → Document your deployment pipeline on GitHub with a clear README

Month 5: AI Security Angle

This is your 2026 differentiator. Companies will pay a $50-100K premium for engineers who understand AI trust and safety.

→ Study adversarial robustness: how models fail under attack
→ Learn model interpretability tools: SHAP and LIME
→ Understand bias detection and fairness metrics
→ Review NIST AI Risk Management Framework (free PDF)
→ Build a project demonstrating responsible AI practices

Month 6: Portfolio + Job Search

Polish 4-5 projects on GitHub, write 2-3 blog posts explaining your work, and start applying.

→ Ensure every project has clean code, documentation, and a demo
→ Write technical blog posts showing your thinking process
→ Practice mock interviews on platforms like interviewing.io (free tier)
→ Target companies investing in AI safety and responsible AI teams
→ Entry salary: $120-150K. Year 2: $160-200K. Year 3: $200-250K+

Key Free Resources: fast.ai (course.fast.ai), Coursera ML Specialization (audit free), Google Colab (free GPU), Kaggle (datasets + competitions), Hugging Face (models + deployment)

Your 2026 Edge: AI security expertise commands a premium. Engineers who understand adversarial attacks, model interpretability, and responsible AI practices are rare and in high demand.

02

Cloud Security

Salary Range: $160,000 - $220,000

Start free: AWS Cloud Practitioner prep (free), Microsoft Learn Azure fundamentals

Month 1-2: Cloud Fundamentals + Security Basics

Get comfortable across all three major clouds. The shared responsibility model is your foundation.

- → AWS Cloud Practitioner Essentials on AWS Skill Builder (free)
- → Azure Fundamentals (AZ-900) on Microsoft Learn (free)
- → Google Cloud Fundamentals: Core Infrastructure on Coursera (free)
- → Set up free tier accounts on AWS, Azure, and GCP
- → Build your first secure VPC in each cloud. Document everything for your portfolio.
- → Download the Cloud Security Alliance CCSK study guide (free PDF)

Month 3: AWS Security Deep Dive

AWS dominates the market. Go deep on IAM, encryption, and network security.

- → Master IAM policies, roles, and least-privilege access design
- → Learn AWS Security Hub, GuardDuty, CloudTrail, and Config
- → Build: a multi-tier VPC with security groups, NACLs, and flow logs
- → Practice: detect and respond to a simulated security event using CloudTrail
- → Study for AWS Certified Cloud Practitioner ($100 exam)

Month 4: Multi-Cloud + Containers

Expand to Azure security services and container security. Multi-cloud expertise is your salary multiplier.

- → Azure Security Center, Sentinel, and Key Vault
- → Container security: Docker image scanning, Kubernetes RBAC, pod security
- → Infrastructure as Code security with Terraform (free, open source)
- → Build: a Kubernetes cluster with proper network policies and RBAC
- → Pass AWS Cloud Practitioner exam

Month 5: Certifications Push

Stack your credentials. Two cloud security certs plus a portfolio gets you hired.

- → Study for AWS Certified Security Specialty ($150 exam)
- → Begin Azure Security Engineer (AZ-500) prep on Microsoft Learn (free)
- → Build incident response playbooks and document them on GitHub
- → Create a cloud security assessment template as a portfolio piece
- → Start networking: join cloud security communities on Discord and LinkedIn

Month 6: Specialize + Job Search

Pick your niche, polish your portfolio, and start applying.

- → Pass AWS Security Specialty and/or AZ-500
- → Choose a specialization: AI workload security, compliance automation, or zero trust
- → Portfolio should have 8-10 projects with diagrams, code, and write-ups
- → Target: Cloud Security Engineer, Cloud Security Architect, SecOps Engineer roles
- → Entry: $140-160K. Year 2: $170-200K. Year 3: $200-220K+

Key Free Resources: AWS Skill Builder (free), Microsoft Learn (free), Google Cloud Skills Boost, Cloud Security Alliance CCSK guide, SANS Cyber Aces (free), Terraform docs

Your 2026 Edge: Most candidates know one cloud. You'll know three. Add AI workload security knowledge and you're commanding top-tier offers in 2026.

03

AI Security / Governance

Salary Range: $170,000 - $230,000

Start free: NIST AI Risk Management Framework, OWASP LLM Top 10

Month 1-2: AI + Security Foundations

Understand both sides: how AI works and how security frameworks apply to it.

→ NIST AI Risk Management Framework (free PDF, nist.gov)
→ OWASP LLM Top 10 (free, owasp.org): the definitive guide to LLM vulnerabilities
→ Fast.ai lesson 1-3 (free): understand how models train and where they break
→ Andrew Ng's AI for Everyone on Coursera (audit free): business context for AI
→ Read: EU AI Act summary and key requirements

Month 3: Adversarial AI + Red Teaming

Learn how AI systems get attacked and how to test their defenses.

→ Study prompt injection, data poisoning, model extraction attacks
→ Learn red teaming methodologies for LLMs (Microsoft/Google published guides)
→ Hands-on: use Garak (free tool) for LLM vulnerability scanning
→ Build: an AI red team assessment report for a sample application
→ Review MITRE ATLAS framework for AI attack taxonomy

Month 4: AI Governance Frameworks

Companies need people who can build AI governance programs, not just find vulnerabilities.

→ Design an AI governance policy template (your key portfolio piece)
→ Study ISO 42001 (AI Management System standard)
→ Learn model cards, data sheets, and AI transparency documentation
→ Understand bias testing, fairness metrics, and responsible AI principles
→ Build: a model risk assessment template for a financial services use case

Month 5: Hands-On Projects

Build the portfolio that proves you can operationalize AI safety.

→ Deploy a simple LLM app and build guardrails around it
→ Create an AI incident response playbook
→ Build a third-party AI vendor risk assessment framework
→ Write a blog post: 'How I Would Audit an AI System'
→ Study for GIAC AI Security Practitioner or similar emerging cert

Month 6: Position + Job Search

This is the hottest niche in security right now. Position yourself as the bridge between AI teams and security teams.

→ Polish portfolio: governance docs, red team reports, risk assessments
→ Target roles: AI Security Engineer, AI Governance Analyst, AI Risk Manager
→ Network in AI safety communities (Partnership on AI, NIST AI forums)
→ Entry: $150-170K. Year 2: $180-210K. Year 3: $210-230K+
→ This field is growing faster than talent can fill it. Move now.

Key Free Resources: NIST AI RMF (free), OWASP LLM Top 10 (free), MITRE ATLAS (free), Garak LLM scanner (free), ISO 42001 overview docs, EU AI Act summaries

Your 2026 Edge: AI security governance is the fastest-growing specialty in tech. Most security teams have zero AI expertise. Most AI teams have zero security expertise. You become the bridge.

04

DevSecOps

Salary Range: $150,000 - $200,000

Start free: GitHub Learning Lab, TryHackMe DevSecOps path (free tier)

Month 1-2: CI/CD + Security Fundamentals

Understand the software development lifecycle and where security fits in.

→ GitHub Learning Lab: intro to GitHub Actions and CI/CD (free)
→ TryHackMe DevSecOps path (free tier rooms)
→ Learn Git workflows, branching strategies, and code review basics
→ Set up a personal CI/CD pipeline with GitHub Actions
→ Understand SAST, DAST, SCA: the three pillars of AppSec testing

Month 3: Application Security Tools

Get hands-on with the tools DevSecOps engineers use daily.

→ SonarQube Community Edition (free): static code analysis
→ OWASP ZAP (free): dynamic application security testing
→ Snyk (free tier): dependency and container vulnerability scanning
→ Trivy (free): container image and IaC scanning
→ Build: a pipeline that runs SAST + SCA + container scan on every commit

Month 4: Infrastructure as Code Security

Modern DevSecOps means securing infrastructure before it deploys.

→ Learn Terraform basics and security best practices
→ Checkov (free): IaC security scanning for Terraform, CloudFormation, K8s
→ Docker security: image hardening, multi-stage builds, rootless containers
→ Kubernetes security: RBAC, network policies, pod security standards
→ Build: a hardened Terraform module with Checkov passing all checks

Month 5: Automation + Monitoring

The best DevSecOps engineers automate everything and build security into the feedback loop.

→ Build security dashboards aggregating findings from multiple tools
→ Learn secrets management: HashiCorp Vault (free), AWS Secrets Manager
→ Implement automated compliance checks in CI/CD pipelines
→ Study for AWS DevOps Engineer Professional or CKS (Certified Kubernetes Security)
→ Create a security metrics dashboard as a portfolio piece

Month 6: Portfolio + Job Search

DevSecOps roles are everywhere. Show you can build secure pipelines, not just talk about them.

→ Portfolio: 6-8 GitHub repos showing secure CI/CD, IaC, container hardening
→ Write a blog post: 'How I Built a Zero-Trust CI/CD Pipeline'
→ Target roles: DevSecOps Engineer, Application Security Engineer, Platform Security
→ Entry: $130-150K. Year 2: $160-180K. Year 3: $180-200K+
→ Bonus: DevSecOps skills transfer directly into cloud security and SRE roles

Key Free Resources: GitHub Learning Lab (free), TryHackMe (free tier), SonarQube Community (free), OWASP ZAP (free), Snyk (free tier), Trivy (free), Checkov (free), Terraform docs

Your 2026 Edge: Every engineering team needs DevSecOps, but few security professionals can actually write code and build pipelines. That combination commands premium pay.

05

GRC / Compliance

Salary Range: $130,000 - $180,000

Start free: ISC2 Certified in Cybersecurity (free cert and training), NIST CSF

Month 1: Build Your Foundation

Learn the GRC ecosystem and start your first certification.

- → ISC2 Certified in Cybersecurity free course (no-cost.isc2.org)
- → Read NIST Cybersecurity Framework 2.0 overview (free PDF from nist.gov)
- → Explore real GRC job descriptions to understand what employers actually need
- → Start building a personal GRC glossary (risk appetite, materiality, control matrix, etc.)
- → Complete the ISC2 CC course by end of month

Month 2: Certifications + Frameworks

Pass your first cert and deepen your compliance framework knowledge.

- → Pass ISC2 CC exam ($199 exam fee, or free if you qualify)
- → Study ISO 27001 controls and SOC 2 Trust Services Criteria
- → Build your first portfolio piece: a compliance gap analysis template
- → Learn the difference between frameworks (NIST, ISO) and regulations (HIPAA, GDPR, PCI-DSS)
- → Start reading SANS whitepapers on risk management (free)

Month 3: Policy Writing + Regulations

GRC pros who can write clear policies are always in demand.

- → Write 2-3 sample policies: Data Classification, Acceptable Use, Incident Response
- → Deep dive HIPAA, GDPR, and PCI-DSS requirements
- → Study third-party risk management processes
- → Start tracking AI governance news: this is your 2026 differentiator
- → Use GDPR.eu and HHS.gov for free regulatory reference material

Month 4: Risk Management + CRISC Prep

Move from compliance checkboxes to strategic risk management.

- → Begin CRISC (Certified in Risk and Information Systems Control) study
- → Create an audit checklist and vendor risk assessment template
- → Learn the COSO framework and how it connects to IT risk
- → Build a risk register with 10-15 realistic organizational risks
- → Practice quantitative risk analysis methods (FAIR framework basics)

Month 5-6: AI Governance + Job Search

Companies need GRC pros who understand generative AI risks. That's your edge.

- → Build an AI risk assessment template (your standout portfolio piece)
- → Create a compliance dashboard or executive summary report sample
- → Pass CRISC exam (or schedule for shortly after month 6)
- → Target roles: Compliance Analyst, Risk Analyst, GRC Specialist, IT Auditor
- → Entry: $130-150K. Year 2: $150-170K. Year 3-5: $180-200K+ (GRC Manager/CISO track)

Key Free Resources: ISC2 CC course (free), NIST CSF 2.0 (free), SANS whitepapers (free), GDPR.eu (free), Practical DevSecOps YouTube, ISACA resources for CRISC prep

Your 2026 Edge: Most GRC candidates have certifications but no work samples. Your portfolio of policies, risk assessments, and AI governance templates will set you apart immediately.

06

Prompt Engineering / AI Integration

Salary Range: $120,000 - $180,000

Start free: OpenAI documentation, Anthropic prompt engineering guide

Month 1-2: Prompt Engineering Foundations

Master the science of communicating with AI systems effectively.

- → Anthropic prompt engineering guide (docs.anthropic.com, free)
- → OpenAI documentation and cookbook (platform.openai.com, free)
- → Learn prompting techniques: chain-of-thought, few-shot, system prompts, structured output
- → Build 10+ prompt templates for different business use cases
- → Understand token economics, context windows, and model selection

Month 3: API Development + Integrations

Go beyond the chat interface. Build real applications with AI APIs.

- → Learn Python + the OpenAI and Anthropic SDKs
- → Build: a customer support bot with retrieval-augmented generation (RAG)
- → Learn vector databases: Pinecone (free tier), Chroma (free, open source)
- → Build: a document Q&A; system using embeddings and RAG
- → Understand API rate limits, cost optimization, and caching strategies

Month 4: Advanced Patterns

Learn the architectures that separate junior prompt engineers from senior AI integration specialists.

- → Multi-agent systems and tool use patterns
- → Function calling and structured outputs for reliable automation
- → Evaluation frameworks: how to measure AI output quality systematically
- → Build: an AI workflow that chains multiple models or tools together
- → Learn LangChain or LlamaIndex basics (both free, open source)

Month 5: Security + Guardrails

The engineers who understand AI security alongside AI capability are the ones companies trust with production systems.

→ Study prompt injection attacks and defenses
→ Implement guardrails: input validation, output filtering, PII detection
→ Learn content moderation APIs and safety classifiers
→ Build: a production-ready AI app with proper security guardrails
→ Review OWASP LLM Top 10 for application-level AI security

Month 6: Portfolio + Job Search

This role barely existed two years ago. The market is wide open.

→ Portfolio: 5-8 projects on GitHub showing RAG, agents, guardrails, eval systems
→ Write case studies showing business impact (cost savings, time saved, accuracy)
→ Target roles: AI Integration Engineer, Prompt Engineer, AI Solutions Architect
→ Entry: $100-130K. Year 2: $140-160K. Year 3: $160-180K+
→ Upside: this role often transitions into AI Product Manager or Head of AI

Key Free Resources: Anthropic docs (free), OpenAI docs + cookbook (free), LangChain docs (free), Pinecone (free tier), Chroma (free), Hugging Face (free), freeCodeCamp Python courses

Your 2026 Edge: Prompt engineering alone won't get you to $180K. Combine it with API development, RAG architectures, and AI security guardrails, and you become an AI Integration Specialist, the role every company needs.

Ready to Go Deeper?

This guide gives you the roadmap. But every career pivot has its own challenges.

If you want personalized guidance on which path fits your background, how to translate your existing experience, or how to stand out in interviews, reach out directly.

DM "CONSULT" on Instagram for a free strategy conversation about your career move.

Follow @thecybersecurist for weekly breakdowns on cybersecurity careers, AI, and what the industry actually needs.

Visit crownstone.io to learn about the Cybersecurist Lens, our strategic framework for building security programs that don't collect dust.

THE CYBERSECURIST

I teach what the industry gatekeeps.