Hidden Heroes in Cybersecurity

Explore the industry's more enigmatic roles

The current cybersecurity workforce gap is estimated to be 4 million professionals.[1]

Bridging the Cybersecurity Workforce Gap is imperative to fortify global cybersecurity resilience. This gap increases over time and is a concern for organizations worldwide.

Two key challenges are:

1. A lack of broad understanding and visibility into the breadth of cybersecurity roles and career paths.
2. Misalignment in education, where colleges are not in step with the rapidly evolving needs of the cybersecurity industry, creating an absence of clear curriculum recommended to attain cybersecurity roles. Learn more here.

Fun fact:
Cybersecurity roles are not all about hacking, and they are not only present in tech companies. Healthcare, banking, education, government, and utility industries all need cybersecurity experts.

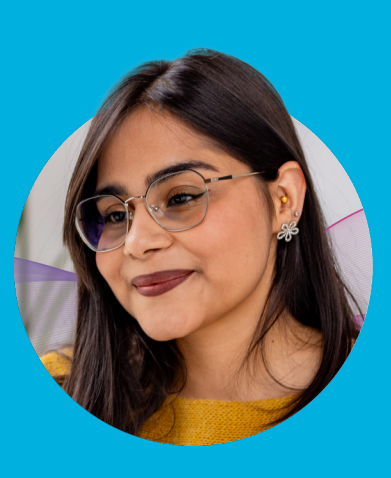
You don't know what you don't know! Discover the possibilities.

Let's check out some obscure roles in Cybersecurity. What are the responsibilities? Which skills are required? How do I attain them? Journey down potential career paths and get a glimpse into a "Day in the Life" perspective from real people in these roles.

Deception Engineer: The Strategist

Digital Forensics Specialist: The Cyber Sleuth

Malware Reverse Engineer: The Protector



Security Automation Engineer: The Innovator

Deception Engineer: The Strategist

A deception engineer specializes in the creation and deployment of deceptive technologies and strategies to mislead cyber attackers.

The Skills: What you need and how to get it

Technical Proficiency
Deep understanding of network architectures, operating systems, and cybersecurity principles.
Learn How
Degree programs in cybersecurity or computer science

Knowledge of Deceptive Technologies
Familiarity with tools like honeypots, decoys, and intrusion detection systems.
Learn how
Training courses and hands-on practice with these tools

Understanding Attack Vectors
Insight on how cyber attacks are carried out and how to design deception strategies.
Learn how
Cybersecurity competitions or capture-the-flag events

Analytical Skills
Ability to interpret data from deception systems and provide actionable insights.
Learn how
Practice with real-world scenarios

Career Opportunities
- Senior Deception Engineer
- Threat Intelligence Analyst
- Security Architect
- Research and Development Specialist
- Consulting and Advisory Roles

Traits for Success
- Creativity and innovation
- Attention to detail
- Problem-solving skills
- Adaptability
- Collaboration skills

A Day in the Life of a Deception Engineer

Interested in what the day-to-day looks like? Here's an overview:
- Review security logs and assess current deception measures.
- Monitor and analyze interactions with deceptive elements.
- Design new deceptive strategies.
- Work with security teams to keep company's infrastructure safe.

Digital Forensics Specialist: The Cyber Sleuth

A digital forensics specialist uses their sleuthing skills to work alongside cybersecurity experts and law enforcement to recover and investigate material found in digital devices.

The Skills: What you need and how to get it

Technical Proficiency
Strong understanding of computer systems, operating systems, and network protocols.
Learn How
Computer science or cybersecurity degrees

Familiarity with Technical Tools
Proficiency in forensic tools such as EnCase, FTK, and Cellebrite.
Learn How
Most tools offer courses and certifications for newcomers

Understanding of Legal Standings
Knowledge of legal procedures and standards for evidence collection and handling.
Learn How
Courses in cyber law or digital forensics workshops

Attention to Detail
Ability to identify and analyze subtle details in digital data.
Learn How
Practice and real-world case studies

Continuous Learning and Certifications
Keep up with the latest learnings and certifications.
Learn How
Start with certifications like a Certified Computer Forensics Examiner or Certified Forensic Computer Examiner

Career Opportunities
- Senior Forensics Analyst
- Cybercrime Investigator
- Incident Response Coordinator
- Research and Development Specialist
- Consulting and Advisor Roles

Traits for Success
- Analytical thinking
- Integrity and ethics
- Patience and persistence
- Communications skills

A Day in the Life of a Digital Forensics Specialist

Interested in what the day-to-day looks like? Here's an overview:
- Review case files and set priorities for ongoing investigations.
- Collect and analyze digital evidence.
- Collaborate with law enforcement, legal teams, and security experts on cases.
- Document investigative processes and results.
- Stay up to date on the latest forensic techniques.

Malware Reverse Engineer: The Protector

A malware reverse engineer analyzes malicious software to understand its behavior, origin, and impact and uses this information to protect its organization from future attacks.

The Skills: What you need and how to get it

Programming Skills
Proficiency in programming languages such as C, C++, Python.
Learn How
Online courses, workshops, and coding bootcamps

Understanding Operating Systems
Deep understanding of operating systems like Windows and Linux.
Learn How
Improve familiarity with system internals and architecture

Knowledge of Assembly Language
Understanding of assembly language to help detect malware samples.
Learn How
Online tutorials, textbooks, and practice with disassemblers

Experience with Analysis Tools
Proficiency with IDA Pro, Ghidra, Binary Ninja, and Radare2.
Learn How
Most tools offer documentation and tutorials for newcomers

Networking and Protocols
Strong understanding of network protocols and how malware communicates over them.
Learn How
Networking courses or hands-on experience with network analysis tools

Rules and Signature Development
Using tools like YARA to develop rules to detect malware samples and variants.
Learn How
Hunting for additional samples on platforms like VirusTotal

Continuous Learning and Certifications
Proficiency with IDA Pro, Ghidra, Binary Ninja, and Radare2.
Learn How
Start with certifications like a Certified Reverse Engineering Analyst or Offensive Security Certified Professional

Career Opportunities
- Senior Reverse Engineer
- Threat Intelligence Analyst
- Security Architect
- Research and Development Specialist
- Consulting and Advisor Roles

Traits for Success
- Curiosity and problem-solving skills
- Attention to detail
- Persistence and patience
- Technical aptitude
- Communications skills

A Day in the Life of a Reverse Malware Engineer

Interested in what the day-to-day looks like? Here's an overview:
- Meet with teams to discuss investigations, threats, and priorities.
- Analyze new malware samples.
- Share findings with other cybersecurity experts to develop security strategies.
- Recommend mitigation strategies based on malware characteristics.
- Learn the latest changes to the threat landscape.

Security Automation Engineer: The Innovator

A security automation engineer develops and implements innovative automated systems to streamline security processes, enhance efficiency, and improve security threat response.

The Skills: What you need and how to get it

Programming and Scripting Skills
Proficiency in Python, JavaScript, or Bash.
Learn How
Online courses, coding workshops, or self-study

Knowledge of Security Tools and Platforms
Familiarity with security tools like SEIM, SOAR, and endpoint detection and response (EDR) systems.
Learn How
Internships or lab simulations

Understanding of Network and System Security
Strong grasp of network protocols, system architectures, and security principles.
Learn How
Networking courses and certifications

Experience with Automation Frameworks
Proficiency in using automation frameworks like Ansible, Puppet, or Chef.
Learn How
Documentation and community support to aid learning

Continuous Learning and Certifications
Keeping up with the latest developments is essential.
Learn How
Start with certifications like Certified Information Systems Security Professional or Certified Automation Professional

Career Opportunities
- Lead Automation Engineer
- Security Architect
- DevSecOps Specialist
- Research and Development Specialist
- Consulting and Advisory Roles

Traits for Success
- Innovation and creativity
- Attention to detail
- Problem-solving skills
- Adaptability
- Collaboration skills

A Day in the Life of a Security Automation Engineer

Interested in what the day-to-day looks like? Here's an overview:
- Review system performance and address any issues in automated processes.
- Collaborate with security teams to identify repetitive tasks that can be automated.
- Find ways to improve security strategies through automation.
- Learn about new automation tools, techniques, and cybersecurity threats.

While career paths are great for reference, the threat landscape's rapid evolution is constantly challenging skillsets and defense tactics. Expanding your skillset can serve as a powerful catalyst, unlocking opportunities that may not yet exist and empowering you to embrace a 'choose your own adventure' career mindset. Boost your career and strengthen your company by regularly upgrading your cybersecurity skills.

23% of organizations recruit outside of traditional cybersecurity degrees or credentials[1]

Listen to this episode of "Beers with Talos" podcast to hear real supporting examples.

How you can get started

To close this gap, Cisco Networking Academy offers free online Cybersecurity courses ranging from Beginner to Immediate skill levels. These offerings are designed to help you gain skills to secure your own digital life and defend an organization from threats.

It is not too late to start—up-skilling and re-skilling are an asset and a well-recognized strategy.

1. Bridging the Cyber Skills Gap