💰

Cybersecurity Salaries Across the United States

10 sources

The provided texts explore the landscape of cybersecurity from various angles. One source offers a step-by-step guide to building a cybersecurity portfolio for professionals at any level, emphasizing real-world examples and strategic formatting for recruiters. Another provides free cybersecurity training and resources from the SANS Institute, highlighting fundamental learning, course demos, and career pathways. A discussion on Reddit offers advice for those considering a cybersecurity career, often recommending foundational IT roles before specializing. Lastly, an introduction to cybersecurity by DHET explains the necessity of cybersecurity, common threats and attacks, methods for data protection, and organizational security measures.

list all 10 sources

Here is a list of all 10 sources you provided:

- Excerpts from "15 Essential Skills for Cybersecurity Analysts in 2025 - Coursera"
- Excerpts from "8 cybersecurity career paths worth considering in 2025 - IMD Business School"
- Excerpts from "A Step-by-Step Guide to Building a Cybersecurity Portfolio | Cyber Security District"
- Excerpts from "Free Cyber Security Training & Resources - SANS Institute"
- Excerpts from "How I Would Start a Cybersecurity Career in 2025 (If I Were Starting from Scratch)"
- Excerpts from "How to Make a Career Change to Cybersecurity - Coursera"

-

Excerpts from "Introduction to Cybersecurity - DHET"

-

Excerpts from the transcript of the video "the hacker’s roadmap (how to get started in IT in 2025)" uploaded on the YouTube channel "NetworkChuck"

-

Excerpts from "To anyone considering a career in cybersecurity - Reddit"

-

Implicitly, a second source from Reddit is included within the provided Reddit excerpts, as there are multiple distinct posts and usernames present, suggesting a forum discussion rather than a single authored piece. For example, posts from users like `geewizzzie12`, `KiloTWE`, `mapplejax`, `ComfortableProperty9`, `admiralspark`, `AdPristine9059`, `MindGoblinThis`, `Recludere`, `hunduk`, `crabapplesteam`, `PC509`, `Chris_Shtein`, `driftwooddreams`, `tdedu75`, `v202099`, `Key-Calligrapher-209`, `dans_cafe`, `Rsubs33`, `ElethaVaric`, and `[deleted]` are all part of this broader discussion on Reddit.

with all you know 3 projects idea I can do for cybersecurity in a 2 weeks time

Here are three cybersecurity project ideas you can likely accomplish within two weeks, drawing from the information in the sources:

1.

Develop a Basic Network Scanner with Python: Source 3 highlights that knowing how to build tools and automate repetitive tasks with languages like Python empowers you to become a more efficient analyst and that Python ranks among the most prevalent languages in cybersecurity and is relatively easy to learn. Source 3 also mentions that you can start scripting with Python in as little as one month. Furthermore, source 10 specifically suggests that in "phase two," you should challenge yourself to build some kind of thing, a project, and provides the idea to build a simple network scanner, scan your network and look for open ports using Python. This project will give you hands-on experience with Python, a key technical skill, and introduce you to network concepts. You can focus on using libraries like `socket` or `nmap` to scan for active hosts and open ports on your local network.

2.

Simulate a Phishing Awareness Campaign: Source 3 suggests that if you're new to cybersecurity, you can create mock projects to demonstrate your skills. For example, simulate a phishing attack scenario. This project involves creating a realistic-looking phishing email and a corresponding landing page (for educational purposes only, without attempting to capture real credentials). You can then create a brief educational document or presentation explaining what phishing is, how to identify phishing emails, and the potential consequences. This project will help you understand social engineering tactics from an attacker's perspective and allow you to practice communication skills by explaining the risks and mitigation strategies. Understanding attack vectors like phishing is also a core security concept.

3.

Set Up a Basic Home Lab with Virtualization to Explore Operating System Security: Source 7 suggests setting up a home lab using virtual machines to practice security concepts. Source 3 emphasizes the importance of operating systems knowledge, including MacOS, Windows, Linux, as well as their command-line interfaces. For this project, you can use free virtualization software like VirtualBox or VMware Player to install a couple of different operating systems (e.g., a Linux distribution and a Windows evaluation version). Within this isolated environment, you can experiment with basic security configurations like firewall settings, user account controls, and explore command-line tools for system monitoring. Source 10 also recommends getting your own Linux server & secure it, spin up a cloud vm, and starting with the basics of IT and cyber skills. This hands-on experience will build your familiarity with different operating systems and their security mechanisms.

What are the top 5 entry-level job titles in my chosen field and their average starting salaries across different regions?

Based on the information in the sources, here are 5 commonly discussed entry-level job titles relevant to a cybersecurity career, along with salary information where available:

1.

IT Help Desk / Technical Support: This is frequently mentioned as a starting point for gaining foundational IT knowledge necessary for cybersecurity. Source 11 specifically recommends applying for these roles immediately. While the sources don't provide specific starting salaries for these roles within the cybersecurity context, Source 6 lists a Systems Administrator with an average annual US base salary of $92,589, and Source 8 mentions that some advanced technicians in schools or businesses can make $40-50 an hour, suggesting that entry-level IT support roles can vary significantly in pay depending on the employer and location.

2.

Security Operations Center (SOC) Analyst: Several sources identify this as a common entry point into cybersecurity. These roles typically involve monitoring and analyzing security events. Source 8 notes that some companies run structured training programs to develop SOC analysts. Source 11 mentions that private sector SOC analyst roles often want SIEM tool experience and knowledge of basic log types. While specific entry-level SOC analyst salaries across regions aren't detailed, Source 11 mentions that Tier 1 SOC analyst roles at smaller companies may pay around $75,000+.

3.

Information Security Analyst: This is a core cybersecurity role focused on assessing vulnerabilities and responding to security incidents. Source 2 reports the median annual wage for Information Security Analysts is $120,360 according to BLS, and Source 9 corroborates this with a median annual salary of $120,360 as of 2023. Source 2 provides an estimated salary breakdown with entry-level roles ranging from $70,000 – $105,000. Source 9 further breaks this down by state, showing significant regional variations. For example, in 2023, the median salary for Information Security Analysts ranged from $84,860 in Vermont to $142,940 in Washington.

4.

Junior Penetration Tester: Source 6 lists this as an entry-level position with an average annual US base salary of $98,583. Penetration testers, also known as ethical hackers, search for and exploit security vulnerabilities. Source 2 suggests that many professionals start in SOC roles before specializing in areas like incident handling or forensics, which could eventually lead to penetration testing.

5.

Security Auditor: Source 6 includes Security Auditor as an entry-level role with an average annual US base salary of $98,487. Auditors are involved in ensuring security measures are in place and effective. Source 8 mentions auditing teams that ensure clients have security measures like network segmentation and IAM in place.

It's important to note that salary figures can vary significantly based on location, the specific company, required skills, and the candidate's prior experience and certifications. The salary ranges provided should be considered as general estimates.

How much would I earn per hour if my annual salary is $62,000 and I work 40 hours per week?

To calculate your hourly wage, we can use the following formula:

Hourly Wage = Annual Salary / (Number of Working Weeks in a Year * Hours Worked Per Week)

Given your annual salary is $62,000 and you work 40 hours per week, we can calculate it as follows:

- Number of working weeks in a year = 52 weeks
- Total hours worked per year = 52 weeks * 40 hours/week = 2080 hours

Now, we can calculate your hourly wage:

Hourly Wage = $62,000 / 2080 hours ≈ $29.81 per hour

Therefore, if your annual salary is $62,000 and you work 40 hours per week, you would earn approximately $29.81 per hour.

This calculation is based on standard working year assumptions and does not directly relate to the information provided in the sources regarding cybersecurity careers, skills, or salaries or our previous discussion about cybersecurity project ideas and entry-level job titles.

Compare responsibilities between two entry-level roles in my field (e.g., Information Security Analyst vs. Security Operations Center) — include what skills are unique to each.

Based on the sources, let's compare the responsibilities of two entry-level cybersecurity roles: Information Security Analyst and Security Operations Center (SOC) Analyst.

Information Security Analyst:

A Cybersecurity Analyst uses a combination of technical and workplace skills to assess vulnerabilities and respond to security incidents. If you have a background in information technology (IT), you may already possess some of the necessary technical skills. The role can involve researching IT security trends and suggesting security enhancements. According to one source, the median annual wage for Information Security Analysts was $120,360 as of 2023, with entry-level roles ranging from $70,000 to $105,000.

Security Operations Center (SOC) Analyst:

A significant part of a cybersecurity analyst's job involves monitoring network activity for possible intrusions. Knowing how to use intrusion detection software—security information and event management (SIEM) products, intrusion detection systems (IDS), and intrusion prevention systems (IPS)—enables you to quickly identify suspicious activity or security violations. Network specialists can transition to security operations roles by applying their deep knowledge of network protocols and architecture to monitor traffic patterns, detect anomalies, and investigate potential breaches within a security operations center. Many professionals in incident response start in security operations center (SOC) roles. Tier 1 SOC analyst roles may involve following a playbook. Private sector SOC analyst roles often want SIEM tool experience and knowledge of basic log types.

Unique Skills:

While both roles fall under the umbrella of cybersecurity analysis, some skills are more emphasized or unique to each at the entry level:

- Information Security Analyst:
  - A stronger emphasis on the ability to assess vulnerabilities. This might involve a broader understanding of different types of weaknesses across systems and applications.
  - The role might require more research into IT security trends to proactively suggest improvements.
- Security Operations Center (SOC) Analyst:

  - Proficiency in using security monitoring tools like SIEM systems, IDS, and IPS is crucial for identifying and triaging alerts.
  - A strong focus on real-time monitoring of network activity and logs to detect anomalies and potential threats.
  - Skills in the initial stages of incident response, such as containment and escalation, following established procedures or playbooks.
  - Familiarity with basic log types (OS, PCAP) and the ability to read and understand them is a significant advantage.

In essence, while both roles aim to protect an organization, entry-level Information Security Analysts may have a broader focus on identifying and understanding vulnerabilities and suggesting improvements, while entry-level SOC Analysts are more focused on the continuous monitoring and immediate response to security events as they occur. However, career paths can evolve, and experience gained in a SOC can often lead to more specialized roles like incident response.

What tools, platforms, and programming languages are most commonly expected in entry-level job descriptions for this role?

Drawing on the sources and our previous discussion, here are some of the tools, platforms, and programming languages that are commonly expected in entry-level job descriptions for roles like Information Security Analyst and Security Operations Center (SOC) Analyst:

Programming/Scripting Languages:

- Python: This language is highlighted as one of the most prevalent in cybersecurity and is considered relatively easy to learn. Knowing Python empowers analysts to build tools and automate repetitive tasks, making them more efficient. You can start scripting with Python in as little as one month. Building a simple network scanner using Python is even suggested as a project to showcase skills.
- PowerShell: This is another scripting language mentioned as beneficial for automation.

- Bash: Familiarity with Bash scripting is also listed as a programming basic.

The ability to read and understand code in these languages is crucial for analyzing potential threats and automating security tasks.

Operating Systems:

- Windows, Linux, and macOS: A deep familiarity with these operating systems, as well as their command-line interfaces, is essential for security analysts. Understanding their security mechanisms and potential weaknesses is also important.

Security Tools and Platforms:

- SIEM (Security Information and Event Management) products: Knowing how to use SIEM software is crucial for monitoring network activity and identifying suspicious activity or security violations. Private sector SOC analyst roles often specifically look for SIEM tool experience. Examples of SIEM tools are Splunk and Elastic Stack. Being able to build queries in tools like Splunk or Kusto is also beneficial.
- IDS/IPS (Intrusion Detection Systems/Intrusion Prevention Systems): Understanding and knowing how to use these systems for intrusion detection is a key skill for cybersecurity analysts, particularly SOC analysts.
- Network monitoring tools: Tools like Wireshark are important for analyzing network traffic.
- Vulnerability scanning tools: While not always explicitly named for entry-level, the concept of identifying vulnerabilities implies familiarity with scanning tools.
- Endpoint Protection solutions: Experience with setting up and maintaining these solutions is relevant.
- Cloud platforms (AWS, Azure, Google Cloud): As more businesses move to the cloud, familiarity with major cloud providers and their native security tools is increasingly important. Cloud security is a fast-growing specialization.
-

Virtualization software: Platforms like VirtualBox or VMware are useful for setting up home labs and practicing security concepts in virtual machines.
Frameworks and Controls:

- Familiarity with common cybersecurity frameworks like NIST, ISO, CIS, and SOC 2 is helpful for understanding best practices and security protocols. Understanding what security controls are and how they are used to protect against vulnerabilities is also important.

Key Concepts:

- Networking fundamentals: A solid understanding of how computer networks function, including protocols and architecture, is foundational for any cybersecurity role. Understanding the OSI model can also be beneficial.
- Security concepts: Familiarity with core principles like defense-in-depth, least privilege, and encryption basics is expected.
- Threat knowledge: Keeping up-to-date on the threat landscape, including understanding common attack vectors and resources like the OWASP Top 10, is important.
- Incident response basics: Understanding the fundamentals of responding to security incidents is often expected.

It's worth noting that while many entry-level roles might not require deep programming skills initially, a basic understanding of scripting, especially in Python, is increasingly valued for automation and tool development. Furthermore, gaining hands-on experience with these tools and platforms through personal projects and home labs is highly recommended to stand out to employers. Many employers prioritize practical skills and the ability to demonstrate them.

What certifications are most often required or recommended for these roles, and how long does each take to earn?

For entry-level roles like Information Security Analyst and Security Operations Center (SOC) Analyst, several certifications are often required or highly recommended. These certifications demonstrate a foundational understanding of key cybersecurity concepts and practices.

Here are some of the most commonly discussed certifications and the general timeframes associated with earning them, based on the sources:

- CompTIA Security+: This is frequently mentioned as an entry-level certification covering fundamental security concepts and best practices. It is often seen as a baseline certification that helps get past HR filters and is even a requirement for some government jobs as it satisfies the DOD 8570 directive. One source suggests dedicating roughly two to three months to study for this certification.
- CompTIA Network+: Understanding networking is considered crucial for cybersecurity roles, and the Network+ certification validates these foundational skills. While not always a direct cybersecurity certification, the knowledge gained is invaluable. The time to earn this can vary depending on individual learning pace.
- Cisco CCNA: The Cisco Certified Network Associate (CCNA) is often considered a highly valuable networking certification and even a "gold standard". Some hiring managers prefer a candidate with a CCNA who understands networking over those with only cybersecurity certifications lacking networking knowledge. While it is noted to be harder and may take more study time than the CompTIA Network+, it is often seen as more valuable by employers. The timeframe to achieve this depends on study intensity and prior networking knowledge.
- Microsoft SC-900 Certification: This certification is part of the Microsoft Cybersecurity Analyst Professional Certificate program, which aims to get individuals job-ready in as little as six months through hands-on experience and preparation for the exam.
- Certified Ethical Hacker (CEH): While more focused on offensive security and penetration testing, the CEH can be beneficial for understanding attack methodologies, which is valuable for security analysts. The time to earn this depends on the chosen study method and individual learning speed.
- GIAC Security Essentials Certification (GSEC): This is another recognized cybersecurity certification that can demonstrate foundational knowledge.

The SANS Institute, which offers GIAC certifications, also provides free training resources. The length of their courses can vary, with introductory ones potentially taking 1-4 weeks.

It's important to note that the time it takes to earn a certification is highly individual and depends on factors like prior experience, study habits, and the chosen learning resources. Some individuals may choose to study independently using free resources like Professor Messer, while others may opt for paid courses or boot camps that offer a more structured learning environment.

Additionally, while certifications can be valuable for proving knowledge to potential employers, gaining hands-on experience through home labs, contributing to open-source projects, participating in Capture The Flag (CTF) competitions, and pursuing internships is also crucial for landing an entry-level cybersecurity role. Some employers prioritize demonstrated skills over just certifications.

Write a 1-minute elevator pitch about this role using the data I've gathered.

"Are you looking for someone to help protect your organization from the ever-increasing threat of cyberattacks? As an aspiring entry-level cybersecurity analyst, I am eager to apply my growing knowledge and skills to safeguard your valuable data and systems. The demand for cybersecurity specialists is rapidly increasing, and I am committed to building a strong foundation in this critical field.

My understanding encompasses the importance of assessing vulnerabilities and responding to security incidents, as well as the crucial role of monitoring network activity for potential intrusions [SOC Analyst definition from previous turn]. I am actively learning essential technical skills, including scripting with Python, and gaining familiarity with security tools and platforms like SIEM systems [SOC Analyst definition from previous turn, 20]. Furthermore, I understand the significance of cybersecurity frameworks and controls in maintaining a secure environment.

Beyond technical aptitude, I recognize the importance of workplace skills such as communication, collaboration, and critical thinking to effectively contribute to a security team and communicate technical concepts to various stakeholders. I am a lifelong learner dedicated to staying ahead of evolving cyber threats. While I am at the beginning of my career, my enthusiasm and commitment to mastering these essential skills make me a valuable asset ready to contribute to your security operations and protect your organization's digital assets."

Generate a motivational poster quote for someone entering this field using language from my research.

"Embrace the cybersecurity journey: Learn the fundamentals, apply your skills through projects, and remember that experience is king. The demand is high, and with persistence and a willingness to learn, you can become a Masterful Defender in this ever-changing field."

Give me the summary of all the what we talked with detais

Here is a detailed summary of our conversation, drawing on the provided sources:

We began by discussing the tools, platforms, and programming languages commonly expected in entry-level job descriptions for roles like Information Security Analyst and Security Operations Center (SOC) Analyst. We identified several key areas [Based on previous turns]:

- Programming/Scripting Languages: Python was highlighted as a prevalent and relatively easy-to-learn language essential for building tools and automation [Based on previous turns]. You can start scripting with Python in as little as one month. PowerShell and Bash were also mentioned as beneficial for automation, and familiarity with these was considered a programming basic [Based on previous turns]. The ability to read and understand code in these languages is crucial for analyzing threats and automating tasks [Based on previous turns].
- Operating Systems: Deep familiarity with Windows, Linux, and macOS, including their command-line interfaces and security mechanisms, was deemed essential [Based on previous turns].
- Security Tools and Platforms:

○

SIEM (Security Information and Event Management) products like Splunk and Elastic Stack are crucial for monitoring network activity and identifying suspicious behavior [Based on previous turns]. Being able to build queries in tools like Splunk or Kusto is beneficial [Based on previous turns, 137].

  - Understanding and knowing how to use IDS/IPS (Intrusion Detection Systems/Intrusion Prevention Systems) is a key skill [Based on previous turns, 42].
  - Network monitoring tools such as Wireshark are important for analyzing network traffic [Based on previous turns, 12].
  - Familiarity with vulnerability scanning tools was implied [Based on previous turns].
  - Experience with endpoint protection solutions is relevant [Based on previous turns].
  - Familiarity with cloud platforms (AWS, Azure, Google Cloud) and their native security tools is increasingly important [Based on previous turns, 2]. Cloud security skills can come with a salary premium.
  - Virtualization software like VirtualBox or VMware is useful for home labs and practicing security concepts [Based on previous turns, 165].
- Frameworks and Controls: Familiarity with cybersecurity frameworks like NIST, ISO, CIS, and SOC 2 is helpful [Based on previous turns, 1]. A framework provides best practices, policies, tools, and security protocols. A control is a measure used to protect against vulnerabilities. Understanding what security controls are and how they are used is important [Based on previous turns].
- Key Concepts: A solid understanding of networking fundamentals, core security concepts (defense-in-depth, least privilege, encryption), threat knowledge (attack vectors, OWASP Top 10), and incident response basics is expected [Based on previous turns, 6]. Incident response professionals are frontline defenders during security breaches, identifying, containing, eradicating, and recovering from incidents. Effective incident handling requires familiarity with an organization's incident response plan.

Next, we discussed certifications commonly required or recommended for these roles and their estimated timelines [Based on previous turns]:

- CompTIA Security+: Frequently mentioned as an entry-level certification covering fundamental security concepts and best practices, often required for government jobs [Based on previous turns, 107]. Studying can take roughly two to three months [Based on previous turns, 166].
- CompTIA Network+: Validates foundational networking skills, crucial for cybersecurity roles [Based on previous turns, 107]. Time to earn varies.
- Cisco CCNA: A highly valuable networking certification, sometimes preferred over cybersecurity certifications lacking networking knowledge [Based on previous turns, 175, 148]. It is noted to be harder and may take more study time [Based on previous turns, 115].
- Microsoft SC-900 Certification: Part of a program aiming to get individuals job-ready in as little as six months [Based on previous turns].
- Certified Ethical Hacker (CEH): Focuses on offensive security and can be beneficial for understanding attack methodologies [Based on previous turns]. Time to earn depends on the study method.
- GIAC Security Essentials Certification (GSEC): Demonstrates foundational cybersecurity knowledge [Based on previous turns]. Introductory courses can take 1-4 weeks [Based on previous turns].

We also noted that hands-on experience is crucial, gained through home labs, open-source contributions, CTFs, and internships [Based on previous turns, 165].

Following this, I generated a 1-minute elevator pitch about the role, highlighting the increasing demand for cybersecurity specialists and the essential skills being learned [Based on previous turn]. This included vulnerability assessment, incident response, network monitoring, scripting with Python, familiarity with SIEM systems, and understanding cybersecurity frameworks and controls [Based on previous turn]. The pitch also emphasized workplace skills like communication and collaboration [Based on previous turn, 3, 4].

Finally, I created a motivational poster quote encouraging individuals entering the field to embrace the cybersecurity journey, learn fundamentals, apply skills, and recognize the high demand and potential to become a "Masterful Defender" [Based on previous turn, 33]. Throughout our discussion, the importance of foundational IT skills, particularly in networking and operating systems, was emphasized as beneficial for a career in cybersecurity. Starting in roles like system administration or IT support can provide invaluable experience. Building a cybersecurity portfolio to showcase technical projects, including documenting the overview, tools used (like Metasploit, Wireshark, Splunk, PowerShell), and outcomes, was highlighted as essential for establishing credibility. The portfolio should also include an introduction, resume, certifications, and case studies demonstrating problem-solving approaches. Communication and collaboration are crucial workplace skills for cybersecurity analysts. Familiarity with cybersecurity frameworks and controls is also important for securing an organization’s data and operations. The demand for cybersecurity specialists is increasing rapidly.