🔒

CyberSecOp Cybersecurity Consulting and Services

23 sources

This text describes the comprehensive cybersecurity consulting services offered by CyberSecOp, an award-winning firm providing solutions like virtual CISO programs, incident response, risk assessments, and managed security. They cater to various industries and assist with compliance, policy development, and employee training to build cyber resilience. CyberSecOp highlights its recognition from Gartner Peer Insights and positions itself as a trusted advisor for managing and mitigating digital risks through a range of consulting and managed security services.

keepSave to note
copy_all
docsAdd note
audio_magic_eraserAudio Overview
flowchartMind Map

top 5 job rolls in cyber sericuty

Based on the sources provided, there is no explicit list of the "top 5 job roles in cybersecurity" with rankings or comparative salary information for these roles.

However, the sources do mention various roles related to the broader tech, IT, data, and security fields, including some specifically within cybersecurity contexts:

1.

High-Paying Entry-Level Roles (from a source covering various industries): A source discussing high-paying entry-level jobs lists several roles in related fields that offer above-median salaries, some of which intersect with IT and data[1...]. The definition of "high-paying" in this source is a role paying close to or more than the median salary for all U.S. occupations, which was $46,310 per year as of May 2022[3]. Roles mentioned include:

◦

Data scientist: Average entry-level compensation is $86,584[4]. This role involves creating frameworks to analyze large datasets, designing algorithms and statistical models, running tests, and developing data products[4].

◦

Management consultant: Average entry-level compensation is $73,416[5]. This role works with companies to identify problems, develop solutions, and oversee implementation to improve businesses[5].

◦

Software developer (also known as software engineer): Average entry-level compensation is $66,832[6]. These roles are responsible for developing different types of software and are described as problem solvers who work with product managers to design and implement software based on user needs[7].

◦

Business analyst, IT: Average entry-level compensation is $62,390[8]. These analysts analyze a company's IT operations and recommend improvements for efficiency, cost reduction, and productivity[8].

◦

Investment associate: Average entry-level compensation is $53,056[9]. These roles assist portfolio managers with research, developing investment strategies, analyzing financial data, and managing client transactions[9].

◦

Desktop support engineer: Average entry-level compensation is $49,514[10]. These engineers troubleshoot software or hardware issues for an organization[10].

◦

HR associate: Average entry-level compensation is $49,307[11]. These associates support the human resources department with tasks like scheduling interviews, processing payroll, conducting onboarding, and administrative work[11].

◦

Executive assistant: Average entry-level compensation is $46,669[12]. These assistants support executives with day-to-day tasks like booking travel, managing calendars, and scheduling appointments[12].

◦

Marketing associate: Average entry-level compensation is $46,622[13]. These associates support a marketing team on various tasks and projects[13].

◦

Sales development representative (SDR): Average entry-level compensation is $45,332[14]. SDRs generate qualified leads and educate potential customers about a product or service[14]. The source notes that compensation can be driven higher by bonuses and commissions based on performance[15].

◦

Fields offering higher-paying entry-level positions specifically mentioned include STEM fields, IT, data analytics, finance, and consulting[16].

2.

Roles/Areas within Cybersecurity Consulting and Services: A source on cybersecurity consulting mentions several types of professionals or roles involved in delivering security services[17...]. These include:

◦

Cyber security consultants[17...] and IT security consultants[28]: These professionals provide advisory services related to cybersecurity strategy, risk management, compliance, and implementing security programs[17...].

◦

Ethical hackers: Mentioned as performing cyber security penetration testing to simulate attacks and find vulnerabilities[25].

◦

Roles involved in Incident Response[18...]: An Incident Response Team (IRT) can include roles like an Incident Response Manager, individuals responsible for technical remediation and computer forensics, as well as executives overseeing finance, communications, HR, operations, and physical security[36...]. External vendors for security event monitoring or computer forensics may also be involved[39].

◦

Network engineers/consultants: Mentioned as providing network security consulting services[2833].

3.

General Cybersecurity/Security Roles: Other sources mention general roles like "cybersecurity professionals"[40...], "internet security expert"[45...], and "network security professional"[49].

While the sources highlight various roles and fields related to IT, data, and cybersecurity, they do not provide a ranked list of the "top 5 job roles in cybersecurity" or offer a comparative analysis of compensation specifically within ranked cybersecurity positions.

keep_pinSave to note

copy_all

thumb_up

thumb_down

top 5 job rolls in cyber sericuty

Based on the sources provided, there isn't an explicit list ranking the "top 5 job roles" specifically within cybersecurity. However, the sources do identify several significant roles in the field, often discussed in terms of different experience levels and associated salaries.

Here are five prominent job roles in cybersecurity mentioned across the sources, which represent various functions and levels within the industry:

1. Information Security Analyst (also called Cybersecurity Analyst or IT Security Analyst)[1...]:
    - This is often considered among the most common roles on a cybersecurity team and can serve as an entry point into the field, although some positions may require prior IT experience[1...].
    - Responsibilities include monitoring networks for vulnerabilities, investigating and reporting security breaches, researching IT security trends, assisting users with security procedures, and developing security strategies[1].
    - The U.S. Bureau of Labor Statistics projects significant job growth for information security analysts[7].
    - The average annual salary for this role is listed as $113,675[1].
2. Penetration Tester (also called Ethical Hacker or Vulnerability Assessor)[3...]:
    - This is typically a mid-level or advanced cybersecurity job[11]. Ethical hacking is a broader category that includes penetration testing as a specialization[10].
    - Responsibilities involve attempting to breach computer networks with permission to identify security weaknesses before malicious actors do[8]. Tasks include planning and carrying out tests, reporting results and recommendations, and developing automation scripts[9].
    - The average annual salary for this role is listed as $113,518[8].
3. Security Engineer (also called Cybersecurity Engineer or Information Security Engineer)[3...]:
    - A mid-level or advanced role, building upon experience from positions like information security analyst or penetration tester[11][12].
    - Responsibilities focus on designing systems to protect a company's computers, networks, and data[12]. This includes developing security standards, recommending enhancements, ensuring systems are installed correctly, testing solutions, and potentially leading incident response teams or developing tools to automate vulnerability detection[12][13].
    -

The average annual salary for this role is listed as $137,879[12].

4. Cybersecurity Manager (also called Information Security (InfoSec) Manager)[3...]:
    - An advanced cybersecurity leadership position[11].
    - Responsibilities include overseeing the security infrastructure of an organization[14]. This involves managing resources (human and technological), tracking security policies, ensuring compliance, sourcing security tools, and leading risk mitigation efforts[1415].
    - The average annual salary for this role is listed as $153,084[14].
5. Security Architect (also called Cybersecurity Architect or Information Security Architect)[1617]:
    - This is an advanced role, often building on experience as a security engineer or information security analyst[1116].
    - Responsibilities include setting the strategic vision for an organization's security systems[16]. This involves searching for vulnerabilities, developing strategies to strengthen security, building and maintaining security networks, managing budgets, coordinating operations, and conducting security drills[1617].
    - The average annual salary for this role is listed as $164,433[16].

It's worth noting that cybersecurity is a field with high demand[7...] and positions often offer higher-than-average salaries[1821]. Entry into many cybersecurity roles often comes after gaining experience in general IT positions like help desk or systems administration[4...].

keep_pinSave to note

copy_all

thumb_up

thumb_down

how much would i earn a salary off 164,433 if i work 40 hrs a week

Based on the sources, the figure $164,433 is cited as the average annual salary for a Security Architect[1].

The sources do not explicitly state that a standard work week for this role is 40 hours, nor do they provide a formula for converting annual salary to weekly earnings. However, if we assume a standard full-time work week of 40 hours and a typical working year of 52 weeks, we can calculate the approximate weekly salary based on the provided annual figure.

Using the average annual salary of $164,433 for a Security Architect[1] and assuming a 52-week year (standard), the approximate weekly salary would be:

$164,433 / 52 \approx $3,162.17 per week.

It's important to note that the assumption of a 40-hour work week and the conversion using 52 weeks per year are based on common practice for salaried roles and are not figures explicitly provided within the given sources for this specific job title or cybersecurity roles in general.

keep_pinSave to note

copy_all

thumb_up

thumb_down

what are reponsibllities between two entry-level roles for a Security Architect

Based on the sources and our conversation, you're asking about the responsibilities of the two roles that commonly serve as stepping stones towards becoming a Security Architect[1], specifically focusing on what those roles entail and how they differ.

The sources identify the Information Security Analyst and the Security Engineer as feeder roles for a Security Architect position[1]. However, it's important to note that according to the sources, while the Information Security Analyst is often considered an entry point into the field[2,3], the Security Engineer is typically viewed as a mid-level or advanced role that builds upon experience gained in positions like an Information Security Analyst or Penetration Tester[4,5]. Therefore, based *only* on the provided sources, the Security Engineer role is not classified as an entry-level position[4,5].

Nonetheless, I can outline the responsibilities of these two roles, as they are the ones the sources indicate can lead to a Security Architect career:

1.

Information Security Analyst (or Cybersecurity Analyst, IT Security Analyst):

◦

This is described as among the most common roles on a cybersecurity team and an excellent entry point into the world of information security[3].

◦

Their responsibilities primarily involve helping to protect an organization's computer networks and systems[3].

◦

Specific tasks include monitoring networks for data security vulnerabilities[3], investigating, documenting, and reporting security breaches[3], researching IT security trends[3], helping computer users with security products and procedures[3], and developing strategies to help their organization remain secure[3].

- This role often involves reacting to potential threats and ensuring existing security measures are understood and followed[3].

2. Security Engineer (or Cybersecurity Engineer, Information Security Engineer):
   - This role is described as mid-level or advanced[4], typically building on experience from roles like Information Security Analyst[4][5].
   - Their core responsibility is to design the systems to keep a company’s computers, networks, and data safe from cyberattacks and other threats[4]. This includes elements like firewalls and intrusion detection systems[4].
   - Their day-to-day tasks can involve developing security standards and best practices[6], recommending security enhancements to management[6], ensuring new security systems are installed and configured correctly[6], testing security solutions[6], leading incident response teams[6], and potentially developing programs to automate vulnerability detection[6].
   - This role requires deep technical knowledge and hands-on implementation skills, focusing on building and maintaining the security infrastructure itself[5].

Key Differences in Responsibilities Between These Two Feeder Roles:

The primary distinction, based on the sources, is that the Information Security Analyst is more focused on monitoring, analysis, reporting, and supporting users regarding security practices and incidents[3]. They identify issues within the *existing* security framework[3].

In contrast, the Security Engineer is more focused on the design, implementation, testing, and maintenance of the *security systems and infrastructure*[4...]. They build and enhance the defenses that the analyst helps monitor[4...].

These roles then lead to the Security Architect, who sets the overall strategic vision for the company's security systems, combining elements of searching for vulnerabilities, developing broader strategies to strengthen security, building and maintaining comprehensive security networks, and managing budgets and operations[1].

keep_pinSave to note

copy_all

thumb_up

thumb_down

Why is being a Security Architect useful

Based on the sources and our conversation, being a Security Architect is highly useful to an organization primarily because this role is responsible for defining and maintaining the strategic vision and design of the entire security infrastructure[1].

Here's a breakdown of why this role is useful, based on the responsibilities described in the sources:

1.

Setting the Strategic Direction: A Security Architect isn't just reacting to threats or implementing individual security measures. They set the vision for a company’s security systems[1]. This involves looking at the big picture, understanding potential vulnerabilities within networks and systems[1], and developing a comprehensive *strategy* to strengthen overall security[1]. In a constantly evolving threat landscape[23], having a clear, forward-thinking strategy is crucial for proactive defense.

2.

Designing and Building Robust Systems: They are responsible for building and maintaining security networks and systems[4]. While Security Engineers might design specific components or implement security solutions[5], the Architect ensures these elements integrate into a cohesive and effective overall defense framework[14]. This includes combining technical knowledge (programming, threat research) with policy development to keep the organization "a step ahead of threats"[1].

3.

Comprehensive Risk Management: The role involves actively searching for vulnerabilities[1] and determining potential attack vectors. By developing strategies to bolster weak points[1], they directly contribute to minimizing the organization's attack surface and guarding against potential exploits[6]. This is a key aspect of risk management[78].

4.

Coordination and Resource Management: Security Architects may also be involved in preparing budgets and overseeing security expenses[4], as well as coordinating security operations across IT and engineering departments[4]. This ensures that security efforts are adequately funded and integrated throughout the organization, which is vital for effective defense.

5.

Learning and Improvement: Their duties can include improving systems in response to security incidents or vulnerabilities and conducting breach of security drills[4]. This focus on learning from past events and practicing responses helps the organization become more resilient over time[9].

In essence, while other cybersecurity roles might focus on detection, analysis, or specific technical implementations, the Security Architect provides the high-level planning and design expertise needed to build and maintain a strong, integrated security posture[14]. This strategic function is invaluable for protecting an organization's critical assets, data, and reputation in the face of persistent and sophisticated cyber threats[3...]. The role's position as an advanced level job[113] with a high average salary ($164,433)[1] reflects the significant value and responsibility associated with this comprehensive security leadership.

keep_pinSave to note

copy_all

thumb_up

thumb_down

how can i build a project that shows exsprance in a information secrcity anales roll tha focos on suster servios

Based on the sources and our conversation, you're looking for ways to build a project that demonstrates experience in an Information Security Analyst role, with a focus that aligns with ongoing or "sustainer" security services. While the term "sustainer services" isn't explicitly used in the sources, we can interpret this as the continuous, operational aspects of maintaining security, which are key responsibilities of an Information Security Analyst.

An Information Security Analyst is often considered an excellent entry point into information security[1]. Their responsibilities involve protecting an organization's networks and systems[1]. Key tasks that relate to continuous security operations or "sustainer services" include:

- Monitoring networks for data security vulnerabilities[1].
- Investigating, documenting, and reporting security breaches[1].
- Researching IT security trends[1].
- Helping computer users with security products and procedures[1].
- Developing strategies to help their organization remain secure[1].

To demonstrate experience in these areas through a project focusing on ongoing security, consider building a personal lab environment and conducting activities that an analyst performs regularly. Here are a few project ideas drawing on concepts from the sources:

1. Home Network Monitoring and Analysis Project:
    - What it demonstrates: Monitoring networks, identifying unusual activity, using security tools.
    - How to build it: Set up a small, isolated network (this could be a virtual machine environment using tools like VirtualBox or VMware, or even a separate physical network). Install a network monitoring

tool (many open-source options exist, like Security Onion which includes tools like Suricata for intrusion detection and Elastic Stack for logging/analysis, or simply Wireshark for packet capture).

  - Tasks: Monitor network traffic over a period of time. Look for suspicious patterns, unauthorized connection attempts, or unusual data flows. Attempt some basic simulated "attacks" within your isolated lab (e.g., a port scan using Nmap from one VM to another) to generate traffic to analyze.
  - Documentation: Document your setup, the tools used, the types of traffic observed, any suspicious findings, and how you investigated them[1]. Explain what different alerts or logs might indicate. This showcases your ability to monitor and investigate[1].

2. Vulnerability Assessment and Hardening Project:
   - What it demonstrates: Identifying vulnerabilities, researching security weaknesses, applying security best practices.
   - How to build it: Set up a system (again, a VM is ideal) with a vulnerable operating system or application (purposefully insecure VMs are available for practice).
   - Tasks: Use a vulnerability scanning tool (like OpenVAS, or Nessus Essentials which has a free tier for home use) to scan the system for known vulnerabilities[1]. Document the findings, including the severity and potential impact of the vulnerabilities (tying into the idea of prioritizing based on risk, even in a small context)[2]. Research how these vulnerabilities could be exploited and how to fix them. Then, perform security hardening steps on the system[3,4], such as applying patches[5,6], configuring user privileges following the principle of least privilege[7...], removing unnecessary services[10], and configuring firewalls[11].
   - Documentation: Document the initial vulnerabilities found, the research into their impact and remediation, the specific hardening steps taken, and how these steps mitigated the risks. Explain the rationale behind your chosen security controls, referencing concepts like reducing the attack surface[10,12]. This shows your ability to research trends and develop strategies[1].

3. Simulated Incident Response Mini-Project:
   - What it demonstrates: Investigating security breaches, documenting incidents, following a response process.
   -

How to build it: Use your lab environment. Simulate a small security incident (e.g., a failed login attempt followed by suspicious activity, or planting a benign "malicious" file in a specific location).

◦

Tasks: Act as the analyst identifying the suspected incident[13]. Document the initial observation, gather relevant logs or evidence, and describe the steps you would take to investigate and contain the incident[13]. If possible in your lab, simulate quarantine or removal steps[13].

◦

Documentation: Use a structured format, similar to an "Incident Record Form"[14], to log the date/time of events and the details of your actions and findings. Document the type, impact, and potential severity of the simulated incident[15]. Discuss how this process aligns with phases of the Incident Response Life Cycle, such as Identification, Containment, and Analysis[13][16]. Reflect on how this incident might lead to improvements in preparation, as discussed in the post-incident phase[17][18].

For any of these projects, clearly outline the project goals, the setup, the tools used, the steps taken, the findings, and the conclusions. Documenting your process and thought process is crucial for an Information Security Analyst role, as it involves investigating, documenting, and reporting[1]. Highlighting skills like problem-solving and analytical thinking are also beneficial, as mentioned as important skills for preparing for a cybersecurity career[19].

keep_pinSave to note

copy_all

thumb_up

thumb_down

wha tools platforms and programming languages are most commonly expected in entry level job description for this role security architect

Based on the sources and our conversation, the role of a Security Architect is not typically considered an entry-level position[1...]. It is listed as a mid-level to advanced cybersecurity job[12]. The average salary of $164,433[3] is significantly higher than the average for listed entry-level roles like Information Security Analyst ($113,675)[6] or the overall average for entry/junior-level cybersecurity professionals ($86K)[7]. Feeder roles for a Security Architect include positions like Security Engineer and Information Security Analyst[3], suggesting prior experience in other security or IT roles is usually required[4...].

Because the sources indicate that the Security Architect role is not entry-level, they do not provide a description of tools, platforms, or programming languages specifically expected in an *entry-level* job description for this role.

However, drawing from the description of the Security Architect role in the sources, we can identify the types of skills, technologies, and languages associated with the position generally:

Key Responsibilities and Required Knowledge Areas:

- Setting the strategic vision for a company’s security systems[3].
- Searching for vulnerabilities within a company's networks and systems and developing strategies to bolster overall security[3]. This implies knowledge of:
    - Vulnerability assessment[10...].
    - Threat research and understanding of the threat landscape[3...].
- Building and maintaining security networks and systems[18]. This requires familiarity with:
    - Security networks and systems design[3].
    - Protective technologies like firewalls and intrusion detection systems[1920].
    - Network security[15...].
    - Cloud security[14...].
    - System hardening[24...].
- Combining programming, threat research, and policy development[3].
- Improving systems in response to security incidents or vulnerabilities[18]. This relates to knowledge of:
    - Incident response processes[10...].
    - Post-incident analysis and improvements[46...].
- Coordinating security operations across IT and engineering departments[18].
- Developing and maintaining security policies and procedures[3...]. This connects to governance, risk, and compliance (GRC) concepts[10...].
-

Programming (especially scripting) languages[3...] are mentioned as important skills in cybersecurity generally and specifically for Security Architects[3]. Python is explicitly cited as a key skill[7275].

While the sources don't provide a checklist of tools or specific platforms expected for a Security Architect, the responsibilities outlined require a deep understanding of various security technologies and their integration. The emphasis on programming, threat research, and policy development[3] indicates a need for both technical depth and strategic thinking. The certifications listed (CISSP, CISM, CCSK)[18] cover broad domains of information security management, architecture, and cloud security, further illustrating the advanced and comprehensive nature of the role.

keep_pinSave to note

copy_all

thumb_up

thumb_down

what certifications are most often reuired or recommended for these roles how long

Based on the sources, here are the certifications most often required or recommended for the roles of Information Security Analyst and Security Architect:

Information Security Analyst

For an Information Security Analyst, which is described as an excellent entry point into the world of information security[1], common certifications include:

- CompTIA Security+[2]
- GIAC Certified Intrusion Analyst (GCIA)[2]
- GIAC Certified Incident Handler (GCIH)[2]

CompTIA Security+ is mentioned as a foundational certification to consider starting with if you are new to cybersecurity[3]. It is also mentioned as a common starting point for Security Engineers (a potential feeder role to Security Architect)[4].

The sources do not explicitly state the duration or renewal requirements for these specific certifications (Security+, GCIA, GCIH). Generally, industry certifications require periodic renewal, often through continuing education or retaking exams, but the specifics are not detailed in the provided material.

Security Architect

The role of Security Architect is identified as a mid-level to advanced cybersecurity job, not typically entry-level[56]. Feeder roles include Security Engineer and Information Security Analyst[6].

Common certifications for a Security Architect include:

•

- Certified Information Systems Security Professional (CISSP)[7]
- Certified Information Security Manager (CISM)[7]
- CSA Certificate of Cloud Security Knowledge (CCSK)[7]

CISSP is also listed as a common certification for Security Systems Administrators[8] and Security Engineers[9]. CISM is listed for Security Systems Administrators[8] and Cybersecurity Managers[10]. Regarding the duration or path to full certification, the sources mention the ISC2 Associate designation[11]. This allows candidates to take any ISC2 certification exam, including CISSP, before meeting the required work experience[11][12]. If you pass the exam without the necessary experience, you become an ISC2 Associate[12]. The sources state you have up to six years to earn the required experience to become fully certified[12]. This indicates that for ISC2 certifications like CISSP, there is a timeframe within which you must demonstrate relevant professional experience after passing the exam to gain full certification status. The process for maintaining certification after becoming fully certified (e.g., through Continuing Professional Education credits) is not detailed in the provided sources.

keep_pinSave to note

copy_all

thumb_up

thumb_down

write a 1 minute elevator pitch about this role using the data gathered

Okay, here is a 1-minute elevator pitch about the Information Security Analyst role, drawing on the information from the sources:

Looking for a high-demand career where you can make a real impact? Consider the role of an Information Security Analyst. This is an excellent entry point into the cybersecurity field and one of the most common roles on a security team[1]. Information Security Analysts are crucial for protecting an organization's computer networks and systems[1].

They are responsible for monitoring networks for data security vulnerabilities[1], investigating, documenting, and reporting security breaches[1], and researching IT security trends[1]. Information Security Analysts also help develop strategies to keep their organization secure[1]. It's a role that requires skills like problem solving and analytical thinking[2].

With an average salary of over $113,000[1], which is significantly above the average for general entry-level cybersecurity positions[3], and being projected as having the fifth fastest growth among all occupations[4], the demand is high[4]. Common certifications like CompTIA Security+ can be a valuable starting point for this role[5][6]. If you're looking to transition into cybersecurity, perhaps from an IT background, this role offers a solid foundation and crucial hands-on experience in defending against cyber threats[1].

keep_pinSave to note

copy_all

thumb_up

thumb_down

generate a motivation poster quote for someone entering this field using language from my research

Here is a motivation poster quote for someone entering the cybersecurity field, drawing on language from the sources and our conversation:

Cybersecurity: A high-demand field[1...]. Build in-demand skills, defend against cyber threats [24, elevator pitch]. Join the crucial mission to protect networks and systems [3, elevator pitch] and help make the connected world a safer place[4].

keep_pinSave to note

copy_all

thumb_up

thumb_down

based on my current research which role seems like the best match for me and why

Based on the information from the sources and our conversation history, particularly considering your situation as a recent graduate who is currently unemployed[1], the role that seems like the best practical match for starting a career aiming towards cybersecurity is likely one of the general IT feeder roles.

Here's why:

1.

Security Architect is Not Entry-Level: As we've discussed, the Security Architect role is consistently described as a mid-level to advanced position, not an entry-level one[2][3]. It requires prior experience, often gained in roles like Security Engineer or Information Security Analyst[3]. Therefore, this is not a suitable starting point for a recent graduate.

2.

Information Security Analyst as a Target Entry Point: The sources *do* identify Information Security Analyst as an "excellent entry point into the world of information security"[4]. It is listed as one of the four entry-level cybersecurity jobs[5]. The role involves crucial tasks like monitoring networks for vulnerabilities, investigating breaches, and researching trends[4], aligning with foundational security work. We even developed an elevator pitch for this role based on its description [elevator pitch].

3.

The Practical Challenge for Recent Graduates: However, the Reddit source, which includes perspectives from those currently in the field and recent graduates, highlights a significant challenge: finding *true* entry-level cybersecurity jobs (like Security Analyst) that don't require *any* prior IT experience can be very difficult[6...]. Employers often prefer candidates who already have foundational technical skills and experience in IT workflows[6...].

4.

Recommended Feeder Roles: The most frequently recommended path for recent graduates trying to enter the cybersecurity field, as suggested by the Reddit discussion, is to first gain experience in a more general IT role[6...]. Common feeder roles recommended include:

- Help Desk / Technical Support[12...]
- Junior Systems Administrator[13...]
- Network Administrator / Network Analyst[4...]
- IT Support[14...]

5.

These roles allow you to build essential technical skills and understand how systems and networks operate in a real-world environment[13...]. This foundational IT experience is highly valued and makes the transition into a dedicated cybersecurity role significantly easier down the line[6...].

In conclusion, while Information Security Analyst is the identified entry-level *cybersecurity* role, based on the collective insights, starting in a general IT support or administration role appears to be the most commonly advised and practical first step for a recent graduate to build the necessary foundation for a cybersecurity career[6...]. Gaining relevant certifications like the CompTIA Security+ while in such a role is also frequently recommended to enhance your resume for future cybersecurity positions[8...].

keep_pinSave to note

copy_all

thumb_up

thumb_down

what missing from my research that would help someone make a more informed decision about this career path

Based on the sources we've reviewed and our conversation history, you've gathered a good amount of information about cybersecurity roles, demand, salaries, certifications, and the general path into the field, particularly noting that Security Architect is not an entry-level role[1...]. We've also established that Information Security Analyst is an identified entry point[56] and that starting in a general IT feeder role like Help Desk, System Administrator, or Network Administrator is a common and often necessary path for recent graduates to gain experience before moving into dedicated cybersecurity positions[2...].

While the research provides a strong overview, several areas could be further explored to help someone like yourself, a recent graduate considering this career path, make a more informed decision:

1. Detailed Day-to-Day Responsibilities for Entry-Level Roles: The sources describe the *types* of tasks for roles like Information Security Analyst (monitoring networks, investigating breaches, researching trends)[5], IT Auditor (planning/performing audits, documenting findings)[14], and feeder roles like Desktop Support Engineer (troubleshooting hardware/software)[15] or Systems Administrator (monitoring systems, managing accounts)[16]. However, a more granular look at what a typical *day* or *week* actually looks like in these roles is missing. Understanding the specific workflow, common tools used in daily tasks, and the balance between routine work and unexpected challenges would provide a clearer picture of the practical reality of the job[10].
2. Specific Tools and Platforms Commonly Encountered: While the importance of knowing about tools like firewalls, intrusion detection systems, and security software is mentioned[17...], and general categories like SIEM are brought up[1321], the sources don't list specific, commonly used tools and platforms that entry-level professionals or those in feeder IT roles would interact with daily. Knowing the names of prevalent ticketing systems, specific SIEM products, common endpoint protection suites, network monitoring tools, or vulnerability scanners could guide targeted learning and resume building[22].
3. Practical Application of Skills and Knowledge: The research emphasizes building in-demand skills like programming (scripting, especially Python), network security, cloud security, and understanding cyber threats[1...]. It also highlights the value of hands-on learning[25] through things like home labs or CTFs[22...]. What's less detailed is how these specific skills are applied in an entry-level context. For instance, how scripting might be used by an Information Security Analyst, or what level of network troubleshooting is expected from Help Desk personnel looking to transition. More concrete examples of how foundational IT skills translate into security practice would be beneficial.
4. Work Culture and Environment Nuances: The sources mention the high demand and fast-paced nature of cybersecurity[1429]. They also touch on the importance of communication and teamwork, particularly in roles like Incident Response[30...]. However, differences in work environments between different entry points (e.g., the high-alert environment of a Security Operations Center (SOC)[13...]

versus a more process-driven GRC (Governance, Risk, and Compliance) role[36...]) are not fully explored. Understanding these cultural and operational differences could help a job seeker identify the best fit for their personality and working style.

5.

Structured Guidance for Self-Learning and Portfolio Building: The sources recommend gaining experience, getting certifications[9...], and building skills[23]. They mention online programs and courses[7...]. However, for a recent graduate facing unemployment and potentially seeking low-cost ways to gain practical skills, more detailed guidance on structuring self-study, identifying specific free resources (like virtual labs or beginner CTF platforms), and building a portfolio of projects to demonstrate skills beyond coursework or certifications would be very helpful. The Reddit source alludes to "home experience that is relevant to security"[26], but specific actionable steps are limited.

In summary, while the existing research paints a clear picture of the cybersecurity landscape and common entry paths, adding detail on the practical, day-to-day realities of entry-level roles, the specific technologies encountered, explicit links between foundational skills and security tasks, and more granular guidance on self-directed learning and experience building would significantly enhance a beginner's ability to make an informed career decision and prepare effectively for the job market.

keep_pinSave to note

copy_all

thumb_up

thumb_down

rewrite your last response using only whats avalable in the sources i provided

Based on the information from the sources and our previous discussion:

First, the role of Security Architect is consistently described as a more advanced position[1]. It is listed among the mid-level and advanced cybersecurity jobs[1], and its feeder roles include Security Engineer and Information Security Analyst, indicating that prior experience in those roles is typically required[2]. Therefore, Security Architect is not presented as an entry-level role in the provided sources[2].

The role explicitly identified as an "excellent entry point into the world of information security" and listed under "4 entry-level cybersecurity jobs" is Information Security Analyst[3]. This role involves tasks such as monitoring networks for vulnerabilities, investigating security breaches, and researching IT security trends[3]. Other identified entry-level cybersecurity jobs include Information Security Specialist, Digital Forensic Examiner, and IT Auditor[4...].

However, the sources also highlight that finding true entry-level cybersecurity positions often requires some prior experience, particularly in IT[910]. Many cybersecurity professionals enter the field after gaining experience in an entry-level IT role[911].

Feeder roles commonly recommended for those looking to enter cybersecurity and gain necessary experience include:

- Network or Systems Administrator[3...]
- Networking[4]
- IT Support[4...]
- Help Desk / Technical Support[16...]
- Junior Systems Administrator[16][22]
- Network Analyst[16]
- Desktop Support Engineer[23]

Starting in one of these general IT roles allows you to gain familiarity with the "ins and outs of IT related work flows"[16], build fundamental technical skills[9...], and understand how systems and users interact[15][16]. Even roles like Help Desk are seen as a way to gain valuable experience[17...] and can be a "great foundation"[16]. Gaining this technical background by maintaining servers and other devices can help in the long run for a pivot to cybersecurity[21].

While roles like Information Security Analyst are listed as entry-level cybersecurity positions[3][25], the practical reality discussed is that these roles often "request 2 or 4+ years of IT experience"[25] or require a mix of skills and experience, including "entry IT experience (1-2 years - help desk or desktop support for ex)"[10]. Therefore, for a recent graduate without prior IT experience, gaining that foundational experience in a general IT feeder role like Help Desk or Systems Administrator appears to be the most frequently advised and pragmatic first step toward a cybersecurity career, as supported by the sources[9...].

keep_pinSave to note

copy_all

thumb_up

thumb_down

what types of projects could i build to demonstrate my readiness for this role baseed on everything ive researched

Based on the information from the sources and our previous conversation, while the sources don't provide a specific list of "projects" for someone entering the field, they strongly emphasize gaining hands-on experience and building in-demand skills[1...]. The recommended path involves starting in a general IT feeder role like Help Desk, System Administrator, or Network Administrator, with the goal of moving into a dedicated Information Security Analyst position[5...].

Therefore, projects you could build to demonstrate readiness for these roles, drawing on the concepts and skills mentioned in the sources, might fall under the umbrella of Homelabs or Online Labs, which are explicitly mentioned as a form of "home experience that is relevant to security"[4] and where you can apply new skills[3].

Here are types of projects implied by the sources that demonstrate skills needed for IT feeder roles and entry-level cybersecurity positions:

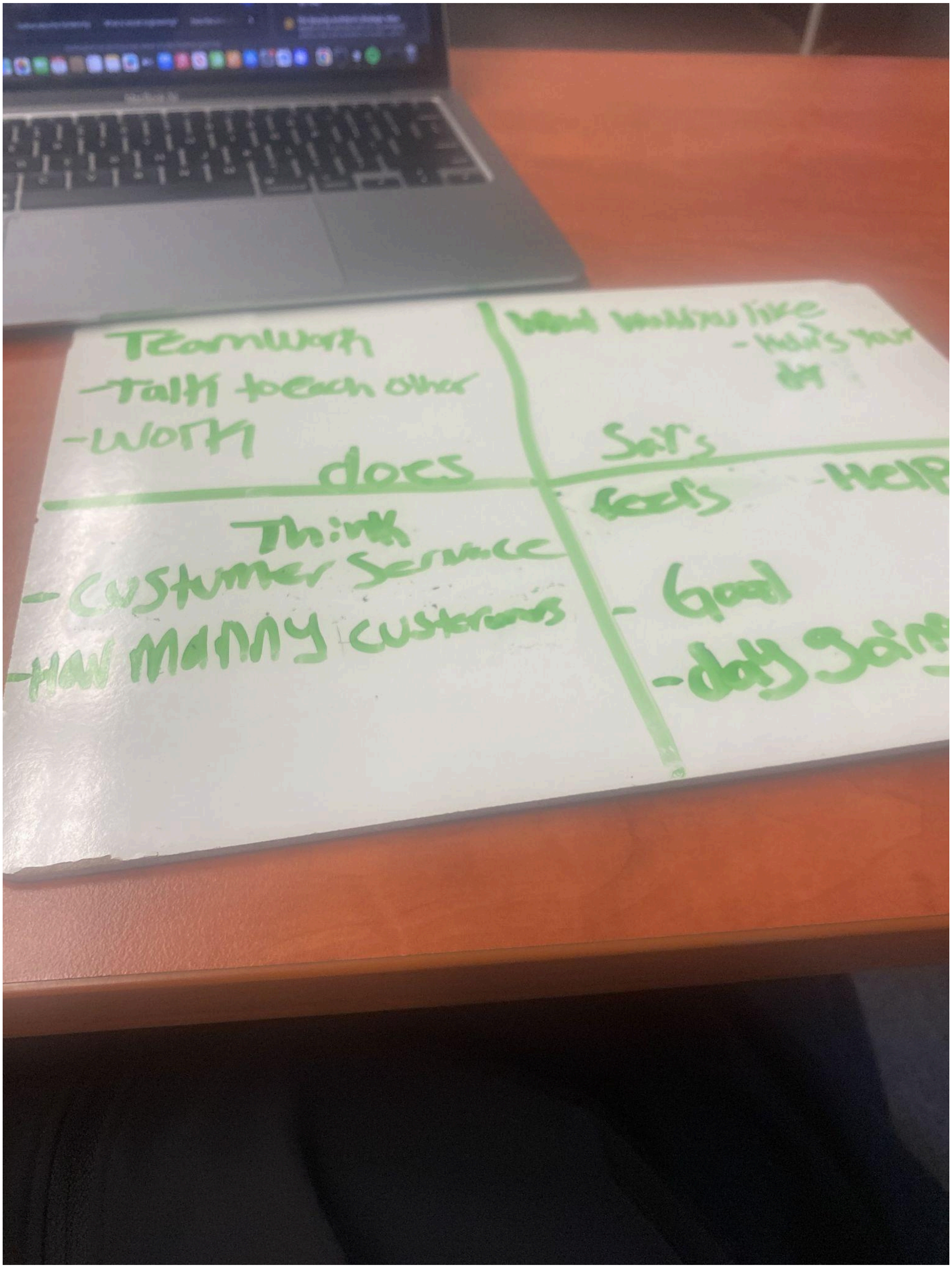
- Implementing Foundational IT/Security Controls: The sources discuss core cybersecurity best practices and standards, which can be simulated in a lab environment. Building a project around setting up and securing a small network or system can demonstrate knowledge of:
    - Access Control and Least Privilege: Configuring user accounts and permissions to adhere to the principle of least privilege[18...]. This aligns with Account Management Standards[21...] and Identity Management concepts[26...].
    - Network Security and Segmentation: Setting up a basic network with a firewall and implementing segmentation to protect different parts[18...]. This relates to Network Security Consulting[31] and Protective Technology Standards[32].
    - Encryption: Demonstrating how to encrypt data at rest (e.g., disk encryption) and data in transit (e.g., setting up a secure connection using SSL/TLS)[23...]. This is a key in-demand skill[2].
    - Patch Management and Updates: Setting up a system to manage software updates and patches[33...].
    - Backup and Recovery: Implementing a backup strategy and practicing recovery processes[34...]. This relates to Recovery Planning[80].
    - Secure Configuration (Hardening): Following best practices to secure an operating system or application[2481]. This is part of Security Hardening[8283].
    - MFA Implementation: Setting up Multi-Factor Authentication on a service or system[34...].
- Scripting and Automation: Programming, especially scripting languages like Python, is listed as an in-demand skill[12]. While sources link automation scripting to more advanced roles like Penetration

Tester[86] or Security Engineer[87], creating basic scripts can demonstrate this foundational skill valuable in many IT and security roles. Projects could involve:

  - Automating simple system administration tasks.
  - Writing scripts to parse logs or identify specific patterns.
  - Creating simple tools to check for common misconfigurations.

- Simulated Incident Response/Threat Analysis: Information Security Analysts investigate security breaches[5]. Practicing the Incident Response lifecycle[20...] in a controlled environment can demonstrate readiness. A project could involve:
  - Setting up a vulnerable system.
  - Simulating a basic attack (e.g., attempting to exploit a known vulnerability, triggering an alert).
  - Using logging/monitoring tools (if available in a lab[25...]) to detect the event[75].
  - Documenting the steps taken to identify, contain, and eradicate the simulated threat[8991]. This aligns with the Incident Response process[20...].
- Participation in Cyber Activities: Engaging in activities like Capture The Flag (CTF) competitions[92] or online labs like those mentioned for certifications[9394] provides practical experience. While not a single "project" to build, documenting the challenges solved, techniques learned, or creating write-ups for specific exercises could serve as demonstrable experience.

By building projects in a lab environment that showcase the implementation of security controls, basic scripting, and understanding of incident response principles, you can demonstrate the practical skills and foundational knowledge valued by employers in both IT feeder roles and entry-level cybersecurity positions like Information Security Analyst, drawing directly from the concepts highlighted across your research.



Teamwork
-Talk to each other
-Work
does

What would you like
-How's your day
Says

Think
-Custumer Service
-How manny custeroms

feels
-Help
- Good
-day goin

Jobe role: System Architect

Project:

Scripting and Automation: Programming, especially scripting languages like Python, is listed as an in-demand skill[12]. While sources link automation scripting to more advanced roles like Penetration Tester[86] or Security Engineer[87], creating basic scripts can demonstrate this foundational skill valuable in many IT and security roles. Projects could involve:

- Automating simple system administration tasks.
- Writing scripts to parse logs or identify specific patterns.
- Creating simple tools to check for common misconfigurations.